BAN CƠ YẾU CHÍNH PHỦ

BÁO CÁO ĐỀ TÀI NHÁNH

"NGHIÊN CỨU, XÂY DỰNG GIẢI PHÁP BẢO MẬT THÔNG TIN TRONG THƯƠNG MẠI ĐIỆN TỬ"

Thuộc đề tài : "*Nghiên cứu một số vấn đề kỹ thuật, công nghệ chủ yếu trong thương mại điện tử và triển khai thử nghiệm - mã số KC.01.05*"

5095-1
14/9/2006

Hà nội, tháng 9 năm 2004

NỘI DUNG

Chương 1: Các hiểm hoạ đối với an toàn thương mại điện tử 4
1.1 Giới thiệu 4
1.2 Các hiểm hoạ đối với sở hữu trí tuệ 7
1.3 Các hiểm hoạ đối với thương mại điện tử 8

Chương 2: Thực thi an toàn cho thương mại điện tử 20
2.1 Bảo vệ các tài sản thương mại điện tử 20
2.2 Bảo vệ sở hữu trí tuệ 21
2.3 Bảo vệ các máy khách 22
2.4 Bảo vệ các kênh thương mại điện tử 27
2.5 Đảm bảo tính toàn vẹn giao dịch 36
2.6 Bảo vệ máy chủ thương mại 39
2.7 Tóm tắt 41

Chương 3: Một số kỹ thuật an toàn áp dụng cho thương mại điện 43
3.1 Mật mã đối xứng 43
3.2 Mật mã khoá công khai 45
3.3 Xác thực thông báo và các hàm băm 60
3.4 Chữ ký số 71

Chương 4: Chứng chỉ điện tử **79**
4.1 Giới thiệu về các chứng chỉ khoá công khai 79
4.2 Quản lý cặp khoá công khai và khoá riêng 85
4.3 Phát hành các chứng chỉ 89
4.4 Phân phối chứng chỉ 92
4.5 Khuôn dạng chứng chỉ X.509 94
4.6 Việc thu hồi chứng chỉ 107
4.7 CRL theo X.509 114
4.8 Cặp khoá và thời hạn hợp lệ của chứng chỉ 121
4.9 Chứng thực thông tin uỷ quyền 123
4.10 Tóm tắt 128

Chương 5: Cơ sở Hạ tầng khoá công khai 131
5.1 Các yêu cầu 131
5.2 Các cấu trúc quan hệ của CA 132
5.3 Các chính sách của chứng chỉ X.509 145
5.4 Các ràng buộc tên X.509 150
5.5 Tìm các đường dẫn chứng thực và phê chuẩn 152
5.6 Các giao thức quản lý chứng chỉ 154
5.7 Ban hành luật 155

Chữ ký điện tử trong hoạt động thương mại điện tử 156
Phần A: Cơ sở công nghệ cho chữ ký số 170
Phần B: Cơ sở pháp lý cho chữ ký số 195

CÁC VẤN ĐỀ LÝ THUYẾT

Trong phần này trình bầy những vấn đề lý thuyết cơ bản phục vụ cho việc xây dựng các giải pháp an toàn TMĐT sẽ trình bầy trong phần 2.

Chương 1:

CÁC HIỂM HOẠ ĐỐI VỚI AN TOÀN THƯƠNG MẠI ĐIỆN TỬ

1.1 Giới thiệu

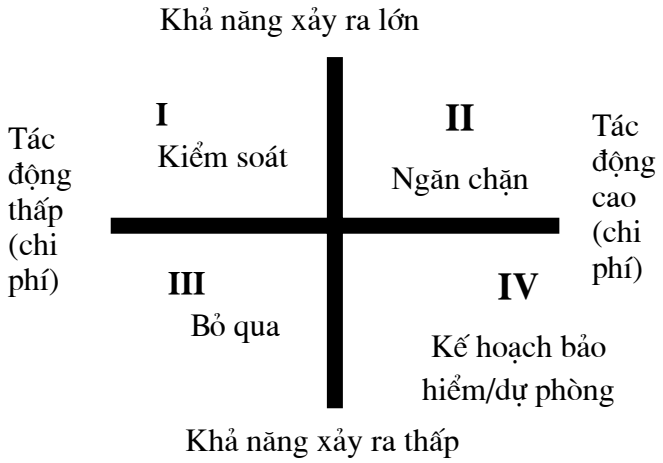
Khi Internet mới ra đời, thư tín điện tử là một trong những ứng dụng phổ biến nhất của Internet. Từ khi có thư tín điện tử, người ta thường lo lắng và đặt vấn đề nghi ngờ, các thư điện tử có thể bị một đối tượng nào đó (chẳng hạn, một đối thủ cạnh tranh) chặn đọc và tấn công ngược trở lại hay không?

Ngày nay, các mối hiểm hoạ còn lớn hơn. Internet càng ngày càng phát triển và các cách mà chúng ta có thể sử dụng nó cũng thay đổi theo. Khi một đối thủ cạnh tranh có thể truy nhập trái phép vào các thông báo và các thông tin số, hậu quả sẽ nghiêm trọng hơn rất nhiều so với trước đây. Trong thương mại điện tử thì các mối quan tâm về an toàn thông tin luôn phải được đặt lên hàng đầu.

Một quan tâm điển hình của những người tham gia mua bán trên Web là số thẻ tín dụng của họ có khả năng bị lộ khi được chuyển trên mạng hay không. Từ 30 năm trước đây cũng xảy ra điều tương tự khi mua bán sử dụng thẻ tín dụng thông qua điện thoại: "Tôi có thể tin cậy người đang ghi lại số thẻ tín dụng của tôi ở đầu dây bên kia hay không?". Ngày nay, các khách hàng thường đưa số thẻ tín dụng và các thông tin khác của họ thông qua điện thoại cho những người xa lạ, nhưng nhiều người trong số họ lại e ngại khi làm như vậy qua máy tính. Trong phần này, chúng ta sẽ xem xét vấn đề an toàn trong phạm vi thương mại điện tử và đưa ra một cái nhìn tổng quan nó cũng như các giải pháp hiện thời.

An toàn máy tính: Chính là việc bảo vệ các tài sản không bị truy nhập, sử dụng, hoặc phá huỷ trái phép. Ở đây có hai kiểu an toàn chung: vật lý và logic. An toàn vật lý bao gồm việc bảo vệ thiết bị (ví dụ như báo động, người canh giữ, cửa chống cháy, hàng rào an toàn, tủ sắt hoặc hầm bí mật và các toà nhà chống bom). Việc bảo vệ các tài sản không sử dụng các biện pháp bảo vệ vật lý thì gọi là an toàn logic. Bất kỳ hoạt động hoặc đối tượng gây nguy hiểm cho các tài sản của máy tính đều được coi như một "hiểm hoạ".

Biện pháp đối phó: Đây là tên gọi chung cho thủ tục (có thể là vật lý hoặc logic) phát hiện, giảm bớt hoặc loại trừ một hiểm hoạ. Các biện pháp đối phó thường biến đổi, phụ thuộc vào tầm quan trọng của tài sản trong rủi ro. Các hiểm hoạ bị coi là rủi ro thấp và hiếm khi xảy ra có thể được bỏ qua, khi chi phí cho việc bảo vệ chống lại hiểm hoạ này vượt quá giá trị của tài sản cần được bảo vệ. Ví dụ, có thể tiến hành bảo vệ một mạng máy tính khi xảy ra các trận bão ở thành phố Okalahoma, đây là nơi thường xuyên xảy ra các trận bão, nhưng không cần phải bảo vệ một mạng máy tính như vậy tại Los Angeles, nơi hiếm khi xảy ra các trận bão. Mô hình quản lý rủi ro được trình bày trong hình 1.3, có 4 hoạt động chung mà bạn có thể tiến hành, phụ thuộc vào chi phí và khả năng xảy ra của các hiểm hoạ vật lý. Trong mô hình này, trận bão ở Kansas hoặc Okalahoma nằm ở góc phần tư thứ 2, còn trận bão ở nam California nằm ở góc phần tư thứ 3 hoặc 4.



Hình 1.3 Mô hình quản lý rủi ro

Kiểu mô hình quản lý rủi ro tương tự sẽ áp dụng cho bảo vệ Internet và các tài sản thương mại điện tử khỏi bị các hiểm hoạ vật lý và điện tử. Ví dụ, đối tượng mạo danh, nghe trộm, ăn cắp. Đối tượng nghe trộm là người hoặc thiết bị có khả năng nghe trộm và sao chép các cuộc truyền trên Internet. Để có một lược đồ an toàn tốt, bạn phải xác định rủi ro, quyết định nên bảo vệ tài sản nào và tính toán chi phí cần sử dụng để bảo vệ tài sản đó. Trong các phần sau, chúng ta tập trung vào việc bảo vệ, quản lý rủi ro chứ không tập trung vào các chi phí bảo vệ hoặc giá trị của các tài sản. Chúng ta tập trung vào các vấn đề như xác định các hiểm hoạ và đưa ra các cách nhằm bảo vệ các tài sản khỏi bị hiểm hoạ đó.

Phân loại an toàn máy tính

Các chuyên gia trong lĩnh vực an toàn máy tính đều nhất trí rằng cần phân loại an toàn máy tính thành 3 loại: loại đảm bảo tính bí mật (***secrecy)***, loại đảm bảo tính toàn vẹn (***integrity***) và loại bảo đảm tính sẵn sàng (***necessity***). Trong đó:

- Tính bí mật ngăn chặn việc khám phá trái phép dữ liệu và đảm bảo xác thực nguồn gốc dữ liệu.
- Tính toàn vẹn ngăn chặn sửa đổi trái phép dữ liệu.
- Tính sẵn sàng ngăn chặn, không cho phép làm trễ dữ liệu và chống chối bỏ.

Giữ bí mật là một trong các biện pháp an toàn máy tính được biết đến nhiều nhất. Hàng tháng, các tờ báo đưa ra rất nhiều bài viết nói về các vụ tấn công ngân hàng hoặc sử dụng trái phép các số thẻ tín dụng bị đánh cắp để lấy hàng hoá và dịch vụ. Các hiểm hoạ về tính toàn vẹn không được đưa ra thường xuyên như trên, nên nó ít quen thuộc với mọi người. Ví dụ về một tấn công toàn vẹn, chẳng hạn như nội dung của một thông báo thư điện tử bị thay đổi, có thể khác hẳn với nội dung ban đầu. Ở đây có một vài ví dụ về hiểm hoạ đối với tính sẵn sàng, xảy ra khá thường xuyên. Việc làm trễ một thông báo hoặc phá huỷ hoàn toàn

thông báo có thể gây ra các hậu quả khó lường. Ví dụ, bạn gửi thông báo thư tín điện tử lúc 10 giờ sáng tới E*Trade, đây là một công ty giao dịch chứng khoán trực tuyến, đề nghị họ mua 1.000 cổ phiếu của IBM trên thị trường. Nhưng sau đó, người môi giới mua bán cổ phiếu thông báo rằng anh ta chỉ nhận được thông báo của bạn sau 2 giờ 30 phút chiều (một đối thủ cạnh tranh nào đó đã làm trễ thông báo) và giá cổ phiếu lúc này đã tăng lên 15% trong thời gian chuyển tiếp.

Bản quyền và sở hữu trí tuệ

Quyền đối với bản quyền và bảo vệ sở hữu trí tuệ cũng là các vấn đề cần đến an toàn, mặc dù chúng được bảo vệ thông qua các biện pháp khác nhau. Bản quyền là việc bảo vệ sở hữu trí tuệ của một thực thể nào đó trong mọi lĩnh vực. Sở hữu trí tuệ là chủ sở hữu của các ý tưởng và kiểm soát việc biểu diễn các ý tưởng này dưới dạng ảo hoặc thực. Cũng giống với xâm phạm an toàn máy tính, xâm phạm bản quyền gây ra các thiệt hại. Tuy nhiên, nó không giống với các lỗ hổng trong an toàn máy tính. Tại Mỹ, luật bản quyền đã ra đời từ năm 1976 và hiện nay có rất nhiều các trang Web đưa ra các thông tin bản quyền.

Chính sách an toàn và an toàn tích hợp

Để bảo vệ các tài sản thương mại điện tử của mình, một tổ chức cần có các chính sách an toàn phù hợp. Một chính sách an toàn là một tài liệu công bố những tài sản cần được bảo vệ và tại sao phải bảo vệ chúng, người nào phải chịu trách nhiệm cho việc bảo vệ này, hoạt động nào được chấp nhận và hoạt động nào không được chấp nhận. Phần lớn các chính sách an toàn đòi hỏi an toàn vật lý, an toàn mạng, quyền truy nhập, bảo vệ chống lại virus và khôi phục sau thảm hoạ. Chính sách phải được phát triển thường xuyên và nó là một tài liệu sống, công ty hoặc văn phòng an toàn phải tra cứu và cập nhật thường xuyên hay định kỳ, thông qua nó.

Để tạo ra một chính sách an toàn, phải bắt đầu từ việc xác định các đối tượng cần phải bảo vệ (ví dụ, bảo vệ các thẻ tín dụng khỏi bị những đối tượng nghe trộm). Sau đó, xác định người nào có quyền truy nhập vào các phần của hệ thống. Tiếp theo, xác định tài nguyên nào có khả năng bảo vệ các tài sản đã xác định trước. Đưa ra các thông tin mà nhóm phát triển chính sách an toàn đòi hỏi. Cuối cùng, uỷ thác các tài nguyên phần mềm và phần cứng tự tạo ra hoặc mua lại, các rào cản vật lý nhằm thực hiện chính sách an toàn.Ví dụ, nếu chính sách an toàn chỉ ra rằng, không một ai được phép truy nhập trái phép vào thông tin khách hàng và các thông tin như số thẻ tín dụng, khái lược của tín dụng, chúng ta phải viết phần mềm đảm bảo bí mật từ đầu này tới đầu kia (end to end) cho các khách hàng thương mại điện tử hoặc mua phần mềm (các chương trình hoặc các giao thức) tuân theo chính sách an toàn này. Để đảm bảo an toàn tuyệt đối là rất khó, thậm chí là không thể, chỉ có thể tạo ra các rào cản đủ để ngăn chặn các xâm phạm.

An toàn tích hợp là việc kết hợp tất cả các biện pháp với nhau nhằm ngăn chặn việc khám phá, phá huỷ hoặc sửa đổi trái phép các tài sản. Các yếu tố đặc trưng của một chính sách an toàn gồm:

- Xác thực: Ai là người đang cố gắng truy nhập vào site thương mại điện tử?
- Kiểm soát truy nhập: Ai là người được phép đăng nhập vào site thương mại điện tử và truy nhập vào nó?
- Bí mật: Ai là người được phép xem các thông tin có chọn lọc?
- Toàn vẹn dữ liệu: Ai là người được phép thay đổi dữ liệu và ai là người không được phép thay đổi dữ liệu?
- Kiểm toán: Ai là người gây ra các biến cố, chúng là biến cố như thế nào và xảy ra khi nào?

Trong phần này, chúng ta tập trung vào các vấn đề áp dụng các chính sách an toàn vào thương mại điện tử như thế nào. Tiếp theo, chúng ta sẽ tìm hiểu về các hiểm hoạ đối với thông tin số, đầu tiên là các hiểm hoạ đối với sở hữu trí tuệ.

1.2 Các hiểm hoạ đối với sở hữu trí tuệ

Các hiểm hoạ đối với sở hữu trí tuệ là một vấn đề lớn và chúng đã tồn tại trước khi Internet được sử dụng rộng rãi. Việc sử dụng tài liệu có sẵn trên Internet mà không cần sự cho phép của chủ nhân rất dễ dàng. Thiệt hại từ việc xâm phạm bản quyền rất khó ước tính so với các thiệt hại do xâm phạm an toàn lên tính bí mật, toàn vẹn hay sẵn sàng (như đã trình bày ở trên). Tuy nhiên, thiệt hại này không phải là nhỏ. Internet có mục tiêu riêng hấp dẫn với hai lý do. Thứ nhất, có thể dễ dàng sao chép hoặc có được một bản sao của bất cứ thứ gì tìm thấy trên Internet, không cần quan tâm đến các ràng buộc bản quyền. Thứ hai, rất nhiều người không biết hoặc không có ý thức về các ràng buộc bản quyền, chính các ràng buộc bản quyền này bảo vệ sở hữu trí tuệ. Các ví dụ về việc không có ý thức và cố tình xâm phạm bản quyền xảy ra hàng ngày trên Internet. Hầu hết các chuyên gia đều nhất trí rằng, sở dĩ các xâm phạm bản quyền trên Web xảy ra là do người ta không biết những gì không được sao chép. Hầu hết mọi người không chủ tâm sao chép một sản phẩm đã được bảo vệ và gửi nó trên Web.

Mặc dù luật bản quyền đã được ban bố trước khi Internet hình thành, Internet đã làm rắc rối các ràng buộc bản quyền của nhà xuất bản. Nhận ra việc sao chép trái phép một văn bản khá dễ dàng, còn không cho phép sử dụng trái phép một bức tranh trên một trang Web là một việc rất khó khăn. Trung tâm Berkman về Internet và xã hội tại trường luật Harvard mới đây đã giới thiệu một khoá học có tiêu đề "Sở hữu trí tuệ trong không gian máy tính". The Copyright Website giải quyết các vấn đề về bản quyền, gửi các nhóm tin và sử dụng không gian lận. Sử dụng không gian lận cho phép sử dụng giới hạn các tài liệu bản quyền sau khi thoả mãn một số điều kiện nào đó.

Trong một vài năm trở lại đây, xảy ra sự tranh chấp về quyền sở hữu trí tuệ và các tên miền của Internet. Các toà án đã phải giải quyết rất nhiều trường hợp xoay quanh hoạt động Cybersquatting. Cybersquatting là một hoạt động đăng ký tên miền, đúng hơn là đăng ký

nhãn hiệu của một cá nhân hay công ty khác và người chủ sở hữu sẽ trả một số lượng lớn đôla để có được địa chỉ URL.

1.3 Các hiểm hoạ đối với thương mại điện tử

Có thể nghiên cứu các yêu cầu an toàn thương mại điện tử bằng cách kiểm tra toàn bộ quy trình, bắt đầu với khách hàng và kết thúc với máy chủ thương mại. Khi cần xem xét từng liên kết logic trong "dây chuyền thương mại", các tài sản phải được bảo vệ nhằm đảm bảo thương mại điện tử an toàn, bao gồm các máy khách, các thông báo được truyền đi trên các kênh truyền thông, các máy chủ Web và máy chủ thương mại, gồm cả phần cứng gắn với các máy chủ. Khi viễn thông là một trong các tài sản chính cần được bảo vệ, các liên kết viễn thông không chỉ là mối quan tâm trong an toàn máy tính và an toàn thương mại điện tử. Ví dụ, nếu các liên kết viễn thông được thiết lập an toàn nhưng không có biện pháp an toàn nào cho các máy khách hoặc các máy chủ Web, máy chủ thương mại, thì chắc chắn không tồn tại an toàn truyền thông. Một ví dụ khác, nếu máy khách bị nhiễm virus thì các thông tin bị nhiễm virus có thể được chuyển cho một máy chủ thương mại hoặc máy chủ Web. Trong trường hợp này, các giao dịch thương mại chỉ có thể an toàn chừng nào yếu tố cuối cùng an toàn, đó chính là máy khách.

Các mục tiếp theo trình bày bảo vệ các máy khách, bảo vệ truyền thông trên Internet và bảo vệ các máy chủ thương mại điện tử. Trước hết chúng ta xem xét các hiểm hoạ đối với các máy khách.

Các mối hiểm hoạ đối với máy khách

Cho đến khi biểu diễn được nội dung Web, các trang Web chủ yếu ở trạng thái tĩnh. Thông qua ngôn ngữ biểu diễn siêu văn bản HTML (ngôn ngữ mô tả trang Web chuẩn), các trang tĩnh cũng ở dạng động một phần chứ không đơn thuần chỉ hiển thị nội dung và cung cấp liên kết các trang Web với các thông tin bổ xung. Việc sử dụng rộng rãi các nội dung động (active content) đã dẫn đến điều này.

Khi nói đến active content, người ta muốn nói đến các chương trình được nhúng vào các trang Web một cách trong suốt và tạo ra các hoạt động. Active content có thể hiển thị hình ảnh động, tải về và phát lại âm thanh, hoặc thực hiện các chương trình bảng tính dựa vào Web. Active content được sử dụng trong thương mại điện tử để đặt các khoản mục mà chúng ta muốn mua trong một thẻ mua hàng và tính toán tổng số hoá đơn, bao gồm thuế bán hàng, các chi phí vận chuyển bằng đường thuỷ và chi phí xử lý. Các nhà phát triển nắm lấy active content vì nó tận dụng tối đa chức năng của HTML và bổ xung thêm sự sống động cho các trang Web. Nó cũng giảm bớt gánh nặng cho các máy chủ khi phải xử lý nhiều dữ liệu và gánh nặng này được chuyển bớt sang cho các máy khách nhàn rỗi của người sử dụng.

Active content được cung cấp theo một số dạng. Các dạng active content được biết đến nhiều nhất là applets, ActiveX controls, JavaScript và VBScript.

JavaScript và VBScript cho các script (tập các chỉ lệnh) hoặc các lệnh có thể thực hiện được, chúng còn được gọi là các ngôn ngữ kịch bản. VBScript là một tập con của ngôn ngữ lập trình Visual Basic của Microsoft, đây là một công cụ biên dịch nhanh gọn và mềm dẻo khi sử dụng trong các trình duyệt Web và các ứng dụng khác có sử dụng Java applets hoặc ActiveX controls của Microsoft.

Applet là một chương trình nhỏ chạy trong các chương trình khác và không chạy trực tiếp trên một máy tính. Điển hình là các applet chạy trên trình duyệt Web.

Còn có các cách khác để cung cấp active content, nhưng chúng không phổ biến với nhiều người, chẳng hạn như các trình Graphics và các trình duyệt Web plug-ins. Các tệp Graphics có thể chứa các chỉ lệnh ẩn được nhúng kèm. Các chỉ lệnh này được thực hiện trên máy khách khi chúng được tải về. Các chương trình hoặc các công cụ biên dịch thực hiện các chỉ lệnh được tìm thấy trong chương trình Graphics, một số khuôn dạng khác có thể tạo ra các chỉ lệnh không có lợi (ẩn trong các chỉ lệnh graphics) và chúng cũng được thực hiện. Plug-ins là các chương trình biên dịch hoặc thực hiện các chỉ lệnh, được nhúng vào trong các hình ảnh tải về, âm thanh và các đối tượng khác.

Active content cho các trang Web khả năng thực hiện các hoạt động. Ví dụ, các nút nhấn có thể kích hoạt các các chương trình được nhúng kèm để tính toán và hiển thị thông tin hoặc gửi dữ liệu từ một máy khách sang một máy chủ Web. Active content mang lại sự sống động cho các trang Web tĩnh.

Active content được khởi chạy như thế nào? Đơn giản, bạn chỉ cần sử dụng trình duyệt Web của mình và xem một trang Web có chứa active content. Applet tự động tải về, song song với trang mà bạn đang xem và bắt đầu chạy trên máy tính của bạn. Điều này làm nảy sinh vấn đề. Do các mođun active content được nhúng vào trong các trang Web, chúng có thể trong suốt hoàn toàn đối với bất kỳ người nào xem duyệt trang Web chứa chúng. Bất kỳ ai cố tình gây hại cho một máy khách đều có thể nhúng một active content gây hại vào các trang Web. Kỹ thuật lan truyền này được gọi là con ngựa thành Tơroa, nó thực hiện và gây ra các hoạt động bất lợi. Con ngựa thành Tơroa là một chương trình ẩn trong các chương trình khác hoặc trong các trang Web. Con ngựa thành Tơroa có thể thâm nhập vào máy tính của bạn và gửi các thông tin bí mật ngược trở lại cho một máy chủ Web cộng tác (một hình thức xâm phạm tính bí mật). Nguy hiểm hơn, chương trình có thể sửa đổi và xoá bỏ thông tin trên một máy khách (một hình thức xâm phạm tính toàn vẹn).

Việc đưa active content vào các trang Web thương mại điện tử gây ra một số rủi ro. Các chương trình gây hại được phát tán thông qua các trang Web, có thể phát hiện ra số thẻ tín dụng, tên người dùng và mật khẩu. Những thông tin này thường được lưu giữ trong các file đặc biệt, các file này được gọi là cookie. Các cookie được sử dụng để nhớ các thông tin yêu cầu của khách hàng, hoặc tên người dùng và mật khẩu. Nhiều active content gây hại có thể lan truyền thông qua các cookie, chúng có thể phát hiện được nội dung của các file phía máy khách, hoặc thậm chí có thể huỷ bỏ các file được lưu giữ trong các máy khách. Ví dụ,

một virus máy tính đã phát hiện được danh sách các địa chỉ thư tín điện tử của người sử dụng và gửi danh sách này cho những người khác trên Internet. Trong trường hợp này, chương trình gây hại giành được đầu vào (entry) thông qua thư tín điện tử được truy nhập từ một Web trình duyệt. Cũng có nhiều người không thích lưu giữ các cookie trên các máy tính của họ. Trên máy tính cá nhân có lưu một số lượng lớn các cookie giống như trên Internet và một số các cookie có thể chứa các thông tin nhạy cảm và mang tính chất cá nhân. Có rất nhiều chương trình phần mềm miễn phí có thể giúp nhận dạng, quản lý, hiển thị hoặc loại bỏ các cookie.Ví dụ, Cookie Crusher (kiểm soát các cookie trước khi chúng được lưu giữ trên ổ cứng của máy tính) và Cookie Pal.

Các mối hiểm hoạ đối với kênh truyền thông

Internet đóng vai trò kết nối một khách hàng với một tài nguyên thương mại điện tử (máy tính dịch vụ thương mại). Chúng ta đã xem xét các hiểm hoạ đối với các máy khách, các tài nguyên tiếp theo chính là kênh truyền thông, các kênh này được sử dụng để kết nối các máy khách và máy chủ.

Internet không phải đã an toàn. Ban đầu nó chỉ là một mạng dùng trong quân sự. Mạng DARPA được xây dựng để cung cấp các truyền thông không an toàn khi một hoặc nhiều đường truyền thông bị cắt. Nói cách khác, mục đích ban đầu của nó là cung cấp một số đường dẫn luân phiên để gửi các thông tin quân sự thiết yếu. Dự tính, các thông tin nhạy cảm được gửi đi theo một dạng đã được mã hoá, do đó các thông báo chuyển trên mạng được giữ bí mật và chống lấy trộm. Độ an toàn của các thông báo chuyển trên mạng có được thông qua phần mềm chuyển đổi các thông báo sang dạng chuỗi ký tự khó hiểu và người ta gọi chúng là các văn bản mã.

Ngày nay, tình trạng không an toàn của Internet vẫn tồn tại. Các thông báo trên Internet được gửi đi theo một đường dẫn ngẫu nhiên, từ nút nguồn tới nút đích. Các thông báo đi qua một số máy tính trung gian trên mạng trước khi tới đích cuối cùng và mỗi lần đi, chúng có thể đi theo những tuyến đường khác nhau. Không có gì đảm bảo rằng tất cả các máy tính mà thông báo đi qua trên Internet đều tin cậy, an toàn và không thù địch. Bạn biết rằng, một thông báo được gửi đi từ Manchester, England tới Cairo, Egypt cho một thương gia có thể đi qua máy tính của một đối tượng cạnh tranh, chẳng hạn ở Beirut, Lebanon. Vì chúng ta không thể kiểm soát được đường dẫn và không biết được các gói của thông báo đang ở đâu, những đối tượng trung gian có thể đọc các thông báo của bạn, sửa đổi, hoặc thậm chí có thể loại bỏ hoàn toàn các thông báo của chúng ta ra khỏi Internet. Do vậy, các thông báo được gửi đi trên mạng là đối tượng có khả năng bị xâm phạm đến tính an toàn, tính toàn vẹn và tính sẵn sàng. Chúng ta sẽ xem xét chi tiết các mối hiểm hoạ đối với an toàn kênh trên Internet dựa vào sự phân loại này.

Các mối hiểm hoạ đối với tính bí mật

Đe doạ tính bí mật là một trong những mối hiểm hoạ hàng đầu và rất phổ biến. Kế tiếp theo tính bí mật là tính riêng tư. Tính bí mật và tính riêng tư là hai vấn đề khác nhau. Đảm

bảo bí mật là ngăn chặn khám phá trái phép thông tin. Đảm bảo tính riêng tư là bảo vệ các quyền cá nhân trong việc chống khám phá. Đảm bảo bí mật là vấn đề mang tính kỹ thuật, đòi hỏi sự kết hợp của các cơ chế vật lý và logic, trong khi đó luật pháp sẵn sàng bảo vệ tính riêng tư. Một ví dụ điển hình về sự khác nhau giữa tính bí mật và tính riêng tư, đó chính là thư tín điện tử. Các thông báo thư tín điện tử của một công ty có thể được bảo vệ chống lại các xâm phạm tính bí mật, bằng cách sử dụng kỹ thuật mã hoá. Trong mã hoá, thông báo ban đầu được mã thành một dạng khó hiểu và chỉ có người nhận hợp lệ mới có thể giải mã trở về dạng thông báo ban đầu. Các vấn đề riêng tư trong thư tín điện tử thường xoay quanh việc có nên cho những người giám sát của công ty đọc thông báo của những người làm công một cách tuỳ tiện hay không. Các tranh cãi xoay quanh, ai là người chủ sở hữu các thông báo thư tín điện tử, công ty hay là người làm công (người đã gửi các thông báo thư tín điện tử). Trọng tâm của mục này là tính bí mật, ngăn chặn không cho các đối tượng xấu đọc thông tin trái phép.

Chúng ta đã đề cập đến việc một đối tượng nguy hiểm có thể lấy cắp các thông tin nhạy cảm và mang tính cá nhân, bao gồm số thẻ tín dụng, tên, địa chỉ và các sở thích cá nhân. Điều này có thể xảy ra bất cứ lúc nào, khi có người nào đó đưa các thông tin thẻ tín dụng lên Internet, một đối tượng có chủ tâm xấu có thể ghi lại các gói thông tin (xâm phạm tính bí mật) không mấy khó khăn. Vấn đề này cũng xảy ra tương tự trong các cuộc truyền thư tín điện tử. Một phần mềm đặc biệt, được gọi là chương trình đánh hơi (sniffer) đưa ra các cách móc nối vào Internet và ghi lại các thông tin đi qua một máy tính đặc biệt (thiết bị định tuyến- router) trên đường đi từ nguồn tới đích. Chương trình sniffer gần giống với việc móc nối vào một đường điện thoại và ghi lại cuộc hội thoại. Các chương trình sniffer có thể đọc các thông báo thư tín điện tử cũng như các thông tin thương mại điện tử. Tình trạng lấy cắp số thẻ tín dụng là một vấn đề đã quá rõ ràng, nhưng các thông tin sản phẩm độc quyền của hãng, hoặc các trang dữ liệu phát hành được gửi đi cho các chi nhánh của hãng có thể bị chặn xem một cách dễ dàng. Thông thường, các thông tin bí mật của hãng còn có giá trị hơn nhiều so với một số thẻ tín dụng (các thẻ tín dụng thường có giới hạn về số lượng tiền), trong khi đó các thông tin bị lấy cắp của hãng có thể trị giá tới hàng triệu đôla.

Để tránh không bị xâm phạm tính bí mật là việc rất khó. Sau đây là một ví dụ về việc bạn có thể làm lộ các thông tin bí mật, qua đó đối tượng nghe trộm hoặc một máy chủ Web (Web site server) khác có thể lấy được các thông tin này. Giả sử bạn đăng nhập vào một Web site, ví dụ *www.anybiz.com* và Web site này có nhiều hộp hội thoại như tên, địa chỉ và địa chỉ thư tín điện tử của bạn. Khi bạn điền vào các hộp hội thoại và nhấn vào nút chấp nhận, các thông tin sẽ được gửi đến máy chủ Web để xử lý. Một cách thông dụng để truyền dữ liệu của bạn tới một máy chủ Web là tập hợp các đáp ứng của hộp hội thoại, đồng thời đặt chúng vào cuối URL của máy chủ đích (địa chỉ). Sau đó, dữ liệu này được gửi đi cùng với yêu cầu HTTP chuyển dữ liệu tới máy chủ. Cho đến lúc này không có xâm phạm nào xảy ra. Giả sử rằng, bạn thay đổi ý kiến và quyết định không chờ đáp ứng từ máy chủ anybiz.com (sau khi đã gửi thông tin đến máy chủ này) và chuyển sang Web site khác, chẳng hạn *www.somecompany.com*. Máy chủ Somecompany.com có thể chọn để thu thập

các trang Web đề mô, ghi vào nhật ký các URL mà bạn vừa đến. Điều này giúp cho người quản lý site xác định được luồng thông tin thương mại điện tử đã tới site. Bằng cách ghi lại địa chỉ URL anybiz.com, Somecompany.com đã vi phạm tính bí mật, vì đã ghi lại các thông tin bí mật mà bạn vừa mới nhập vào. Điều này không thường xuyên xảy ra, nhưng chúng ta không được chủ quan, nó vẫn "có thể" xảy ra.

Bạn đã tự làm lộ thông tin khi sử dụng Web. Các thông tin này có cả địa chỉ IP (địa chỉ Internet) và trình duyệt mà bạn đang sử dụng. Đây là một ví dụ về việc xâm phạm tính bí mật. Ít nhất có một Web site có thể đưa ra dịch vụ "trình duyệt ẩn danh", dịch vụ này che dấu các thông tin cá nhân, không cho các site mà bạn đến được biết. Web site có tên là Anonymizer, nó đóng vai trò như một bức tường lửa và các lưới chắn che dấu thông tin cá nhân. Nó tránh làm lộ thông tin bằng cách đặt địa chỉ Anonymizer vào phần trước của các địa chỉ URL bất kỳ, nơi mà bạn đến. Lưới chắn này chỉ cho phép các site khác biết thông tin về Web site mang tên là Anonymizer, chứ không cho biết thông tin gì về bạn. Ví dụ, nếu bạn truy nhập vào Amazon.com, Anonymizer sẽ đưa ra URL như sau: *http://www.anonymizer.com:8080/http:// www.amazon.com*

Các hiểm hoạ đối với tính toàn vẹn

Mối hiểm hoạ đối với tính toàn vẹn tồn tại khi một thành viên trái phép có thể sửa đổi các thông tin trong một thông báo. Các giao dịch ngân hàng không được bảo vệ, ví dụ tổng số tiền gửi được chuyển đi trên Internet, là chủ thể của xâm phạm tính toàn vẹn. Tất nhiên, xâm phạm tính toàn vẹn bao hàm cả xâm phạm tính bí mật, bởi vì một đối tượng xâm phạm (sửa đổi thông tin) có thể đọc và làm sáng tỏ các thông tin. Không giống hiểm hoạ đối với tính bí mật (người xem đơn giản chỉ muốn xem thông tin), các hiểm hoạ đối với tính toàn vẹn là gây ra sự thay đổi trong các hoạt động của một cá nhân hoặc một công ty, do nội dung cuộc truyền thông đã bị sửa đổi.

Phá hoại điều khiển (Cyber vandalism) là một ví dụ về việc xâm phạm tính toàn vẹn. Cyber vandalism xoá (để khỏi đọc được) một trang Web đang tồn tại. Cyber vandalism xảy ra bất cứ khi nào, khi các cá nhân thay đổi định kỳ nội dung trang Web của họ.

Giả mạo (Masquerading) hoặc đánh lừa (spoofing) là một trong những cách phá hoại Web site. Bằng cách sử dụng một kẽ hở trong hệ thống tên miền (DNS), thủ phạm có thể thay thế vào đó các địa chỉ Web site giả của chúng. Ví dụ, một tin tặc có thể tạo ra một Web site giả mạo *www.widgetsinternational.com*, bằng cách lợi dụng một kẽ hở trong DNS để thay thế địa chỉ IP giả của tin tặc vào địa chỉ IP thực của Widgets International. Do vậy, mọi truy cập đến Widgets International đều bị đổi hướng sang Web site giả. Tấn công toàn vẹn chính là việc sửa đổi một yêu cầu và gửi nó tới máy chủ thương mại của một công ty thực. Máy chủ thương mại không biết được tấn công này, nó chỉ kiểm tra lại số thẻ tín dụng của khách hàng và tiếp tục thực hiện yêu cầu.

Các hiểm hoạ về toàn vẹn có thể sửa đổi các thông tin quan trọng trong các lĩnh vực tài chính, y học hoặc quân sự. Việc sửa đổi này có thể gây ra các hậu quả nghiêm trọng cho mọi người và kinh doanh thương mại.

Các hiểm hoạ đối với tính sẵn sàng

Mục đích của các hiểm hoạ đối với tính sẵn sàng (được biết đến như các hiểm hoạ làm chậm trễ hoặc chối bỏ) là phá vỡ quá trình xử lý thông thường của máy tính, hoặc chối bỏ toàn bộ quá trình xử lý. Một máy tính khi vấp phải hiểm hoạ này, quá trình xử lý của nó thường bị chậm lại với một tốc độ khó chấp nhận. Ví dụ, nếu tốc độ xử lý giao dịch của một máy rút tiền tự động bị chậm lại từ 1giây, 2 giây tới 30 giây, người sử dụng sẽ không sử dụng các máy này nữa. Tương tự, việc trì hoãn các dịch vụ Internet sẽ khiến cho các khách hàng chuyển sang các Web site hoặc site thương mại của các đối thủ cạnh tranh khác. Nói cách khác, việc làm chậm quá trình xử lý làm cho một dịch vụ trở nên kém hấp dẫn và không còn hữu ích. Rõ ràng là một tờ báo mang tính thời sự sẽ trở nên vô nghĩa hay chẳng có giá trị với mọi người nếu nó đưa ra các tin tức đã xảy ra từ 3 ngày trước đó.

Các tấn công chối bỏ có thể xoá bỏ toàn bộ hoặc loại bỏ một phần các thông tin trong một file hoặc một cuộc liên lạc. Như đã biết, Quicken là một chương trình tính toán, nó có thể được cài đặt vào tất cả các máy tính nhằm làm trệch hướng tiền gửi đến tài khoản của một nhà băng khác. Tấn công chối bỏ sẽ phủ nhận số tiền gửi của những người chủ hợp pháp đối với số tiền đó. Tấn công của Robert Morris Internet Worm là một ví dụ điển hình về tấn công chối bỏ.

Các mối hiểm hoạ đối với máy chủ

Máy chủ là liên kết thứ 3 trong bộ ba máy khách - Internet - máy chủ (Client-Internet-Server), bao gồm đường dẫn thương mại điện tử giữa một người sử dụng và một máy chủ thương mại. Máy chủ có những điểm yếu dễ bị tấn công và một đối tượng nào đó có thể lợi dụng những điểm yếu này để phá huỷ, hoặc thu được các thông tin một cách trái phép. Một điểm truy nhập là máy chủ Web và các phần mềm của nó. Các điểm truy nhập khác là các chương trình phụ trợ bất kỳ có chứa dữ liệu, ví dụ như một cơ sở dữ liệu và máy chủ của nó. Các điểm truy nhập nguy hiểm có thể là các chương trình CGI hoặc là các chương trình tiện ích được cài đặt trong máy chủ. Không một hệ thống nào được coi là an toàn tuyệt đối, chính vì vậy, người quản trị của máy chủ thương mại cần đảm bảo rằng các chính sách an toàn đã được đưa ra và xem xét trong tất cả các phần của một hệ thống thương mại điện tử.

Các hiểm hoạ đối với máy chủ Web

Phần mềm máy chủ Web được thiết kế để chuyển các trang Web bằng cách đáp ứng các yêu cầu của HTTP (giao thức truyền siêu văn bản). Với các phần mềm máy chủ Web ít gặp rủi ro, nó được thiết kế với dịch vụ Web và đảm bảo mục đích thiết kế chính. Phức tạp hơn, các phần mềm (có thể có các lỗi chương trình hoặc các lỗ hổng về an toàn) là các điểm yếu mà qua đó đối tượng xấu có thể can thiệp vào.

Các máy chủ Web được thực hiện trên hầu hết các máy, ví dụ như các máy tính chạy trên hệ điều hành UNIX, được thiết lập chạy ở các mức đặc quyền khác nhau. Mức thẩm quyền cao nhất có độ mềm dẻo cao nhất, cho phép các chương trình, trong đó có các máy chủ Web, thực hiện tất cả các chỉ lệnh của máy và không giới hạn truy nhập vào tất cả các phần của hệ thống, không ngoại trừ các vùng nhạy cảm và phải có thẩm quyền. Còn các mức thẩm quyền thấp nhất tạo ra một rào cản logic xung quanh một chương trình đang chạy, ngăn chặn không cho nó chạy tất cả các lớp lệnh của máy và không cho phép nó truy nhập vào tất cả các vùng của máy tính, chí ít là các vùng lưu giữ nhạy cảm. Quy tắc an toàn đặt ra là cung cấp một chương trình và chương trình này cần có thẩm quyền tối thiểu để thực hiện công việc của mình. Người quản trị hệ thống (người thiết lập các tài khoản (account) và mật khẩu cho những người sử dụng) cần một mức thẩm quyền rất cao, được gọi là "super user" trong môi trường UNIX, để sửa đổi các vùng nhạy cảm và có giá trị của hệ thống. Việc thiết lập một máy chủ Web chạy ở mức thẩm quyền cao có thể gây hiểm hoạ về an toàn đối với máy chủ Web. Trong hầu hết thời gian, máy chủ Web cung cấp các dịch vụ thông thường và thực hiện các nhiệm vụ với một mức thẩm quyền rất thấp. Nếu một máy chủ Web chạy ở mức thẩm quyền cao, một đối tượng xấu có thể lợi dụng một máy chủ Web để thực hiện các lệnh trong chế độ thẩm quyền.

Một máy chủ Web có thể dàn xếp tính bí mật, nếu nó giữ các danh sách thư mục tự động được lựa chọn thiết lập mặc định. Xâm phạm tính bí mật xảy ra khi một trình duyệt Web có thể phát hiện ra các tên danh mục của một máy chủ. Điều này xảy ra khá thường xuyên, nguyên nhân là do khi bạn nhập vào một URL, chẳng hạn như:

http://www.somecompany.com/FAQ/

và mong muốn được xem trang ngầm định trong thư mục FAQ. Trang Web ngầm định (máy chủ có thể hiển thị nó) được đặt tên là index.html. Nếu file này không có trong thư mục, máy chủ Web sẽ hiển thị tất cả các tên danh mục có trong thư mục. Khi đó, bạn có thể nhấn vào một tên danh mục ngẫu nhiên và xem xét các danh mục mà không bị giới hạn.

Những người quản trị của các site khác, ví dụ người quản trị của Microsoft, rất thận trọng trong việc hiển thị tên danh mục. Việc nhập tên người dùng vào một phần đặc biệt trong không gian Web, về bản chất không phải là sự xâm phạm tính bí mật hoặc tính riêng tư. Tuy nhiên, tên người dùng và mật khẩu bí mật có thể bị lộ khi bạn truy nhập vào nhiều trang trong vùng nội dung được bảo vệ và quan trọng của máy chủ Web. Điều này có thể xảy ra, vì một số máy chủ yêu cầu thiết lập lại tên người dùng và mật khẩu cho từng trang trong vùng nội dung quan trọng mà bạn truy cập vào do Web không lưu nhớ những gì đã xảy ra trong giao dịch cuối. Cách thích hợp nhất để nhớ tên người dùng và mật khẩu là lưu giữ các thông tin bí mật của người sử dụng trong một cookie có trên máy của người này. Theo cách này, một máy chủ Web có thể yêu cầu xác nhận dữ liệu, bằng cách yêu cầu máy tính gửi cho một cookie. Vấn đề rắc rối xảy ra là các thông tin có trong một cookie có thể được truyền đi không an toàn và một đối tượng nghe trộm có thể sao chép. Với tình trạng này, máy chủ Web cần yêu cầu truyền cookie an toàn.

Một SSI là một chương trình nhỏ, chương trình này có thể được nhúng vào một trang Web, nó có thể chạy trên máy chủ (đôi khi còn được gọi là servlet). Bất cứ khi nào chương trình chạy trên một máy chủ hay đến từ một nguồn vô danh và không tin cậy, ví dụ từ trang Web của một người sử dụng, có thể sẽ xảy ra khả năng SSI yêu cầu thực hiện một hoạt động bất hợp pháp nào đó. Mã chương trình SSI có thể là một chỉ thị của hệ điều hành yêu cầu hiển thị file mật khẩu, hoặc gửi ngược trở lại một vị trí đặc biệt.

Chương trình FTP có thể phát hiện các mối hiểm hoạ đối với tính toàn vẹn của máy chủ Web. Việc lộ thông tin có thể xảy ra khi không có các cơ chế bảo vệ đối với các danh mục, do đó người sử dụng FTP có thể duyệt qua.

Ví dụ, giả thiết có một máy khách thương mại hoàn toàn và máy này có account của máy tính thương mại khác, nó có thể tải dữ liệu lên máy tính của đối tác một cách định kỳ. Bằng chương trình FTP, người quản trị của hệ thống có thể đăng nhập vào máy tính của đối tác thương mại, tải dữ liệu lên, sau đó tiến hành mở và hiển thị nội dung của các danh mục khác có trong máy tính máy chủ Web. Việc làm này không có gì khó nếu thiếu các bảo vệ. Với một chương trình máy chủ Web, bạn có thể nhấn đúp chuột vào một danh mục của thư mục chính để thay đổi thứ bậc của danh mục này, nhấn đúp chuột vào danh mục khác, như danh mục đặc quyền của công ty khác, để tải về các thông tin mà bạn nhìn thấy. Điều này có thể thực hiện một cách đơn giản vì người ta đã quên giới hạn khả năng xem duyệt của một đối tác khác đối với một danh mục đơn lẻ.

Một trong các file nhạy cảm nhất trên máy chủ Web (nếu nó tồn tại) chứa mật khẩu và tên người dùng của máy chủ Web. Nếu file này bị tổn thương, bất kỳ ai cũng có thể thâm nhập vào các vùng thẩm quyền, bằng cách giả mạo một người nào đó. Do có thể giả danh để lấy được các mật khẩu và tên người dùng nên các thông tin liên quan đến người sử dụng không còn bí mật nữa. Hầu hết các máy chủ Web lưu giữ bí mật các thông tin xác thực người dùng. Người quản trị máy chủ Web có nhiệm vụ đảm bảo rằng: máy chủ Web được chỉ dẫn áp dụng các cơ chế bảo vệ đối với dữ liệu.

Những mật khẩu (người dùng chọn) cũng là một hiểm hoạ. Đôi khi, người sử dụng chọn các mật khẩu dễ đoán, vì chúng có thể là tên thời con gái của mẹ, tên của một trong số các con, số điện thoại, hoặc số hiệu nhận dạng. Người ta gọi việc đoán nhận mật khẩu qua một chương trình lặp sử dụng từ điển điện tử là tấn công từ điển. Một khi đã biết được mật khẩu của người dùng, bất kỳ ai cũng có thể truy nhập vào một máy chủ mà không bị phát hiện trong một khoảng thời gian dài.

Các đe dọa đối với cơ sở dữ liệu

Các hệ thống thương mại điện tử lưu giữ dữ liệu của người dùng và lấy lại các thông tin về sản phẩm từ các cơ sở dữ liệu kết nối với máy chủ Web. Ngoài các thông tin về sản phẩm, các cơ sở dữ liệu có thể chứa các thông tin có giá trị và mang tính riêng tư. Một công ty có thể phải chịu các thiệt hại nghiêm trọng nếu các thông tin này bị lộ hoặc bị sửa đổi. Hầu hết các hệ thống cơ sở dữ liệu có quy mô lớn và hiện đại sử dụng các đặc tính an toàn

cơ sở dữ liệu dựa vào mật khẩu và tên người dùng. Sau khi được xác thực, người sử dụng có thể xem các phần đã chọn trong cơ sở dữ liệu. Tính bí mật luôn sẵn sàng trong các cơ sở dữ liệu, thông qua các đặc quyền được thiết lập trong cơ sở dữ liệu. Tuy nhiên, một số cơ sở dữ liệu lưu giữ mật khẩu/tên người dùng một cách không an toàn, hoặc quên thiết lập an toàn hoàn toàn và dựa vào máy chủ Web để có an toàn. Nếu một người bất kỳ có thể thu được các thông tin xác thực người dùng, thì anh ta có thể giả danh thành một người sử dụng của cơ sở dữ liệu hợp pháp, làm lộ hoặc tải về các thông tin mang tính cá nhân và quý giá. Các chương trình con ngựa thành Tơroa nằm ẩn trong hệ thống cơ sở dữ liệu cũng có thể làm lộ các thông tin bằng việc giáng cấp các thông tin này (có nghĩa là chuyển các thông tin nhạy cảm sang một vùng ít được bảo vệ của cơ sở dữ liệu, do đó bất cứ ai cũng có thể xem xét các thông tin này). Khi các thông tin bị giáng cấp, tất cả những người sử dụng, không ngoại trừ những đối tượng xâm nhập trái phép cũng có thể truy nhập.

Chúng ta đã có một số lượng lớn các trang và Web site nói về an toàn cơ sở dữ liệu. Ví dụ, các liên kết trong Online Companion trình bày các mối quan tâm về an toàn cơ sở dữ liệu. Liên kết "SQL Server database threats" trong Online Companion trình bày các mối hiểm hoạ đối với SQL Server, nhưng các mối hiểm hoạ này cũng áp dụng cho các hệ thống cơ sở dữ liệu nói chung. An toàn cơ sở dữ liệu đòi hỏi người quản trị của một hệ thống phải hết sức cẩn thận.

Các hiểm hoạ đối với giao diện gateway thông thường

Như đã biết, CGI tiến hành chuyển các thông tin từ một máy chủ Web sang chương trình khác, chẳng hạn như một chương trình cơ sở dữ liệu. CGI và các chương trình (mà nó chuyển dữ liệu đến) cung cấp active content cho các trang Web. Ví dụ, một trang Web có thể chứa một hộp hội thoại để bạn điền tên đội thể thao chuyên nghiệp nổi tiếng. Chỉ khi bạn chấp nhận sự lựa chọn của mình, các chương trình CGI xử lý thông tin và tìm kiếm các tỷ số cuối cùng của đội này, đưa các tỷ số lên một trang Web và sau đó gửi trang Web (vừa được tạo ra) ngược trở lại cho máy khách trình duyệt của bạn. Do CGI là các chương trình, khi chúng bị lạm dụng sẽ xảy ra một hiểm hoạ an toàn. Gần giống với các máy chủ Web, CGI script có thể được thiết lập chạy ở các mức đặc quyền cao, không bị giới hạn. Một khi các CGI gây hại có thể truy nhập tự do vào các nguồn tài nguyên của hệ thống, chúng có khả năng làm cho hệ thống không hoạt động, gọi các chương trình hệ thống dựa vào đặc quyền để xóa các file, hoặc xem các thông tin bí mật của khách hàng, trong đó có tên người dùng và mật khẩu. Khi lập trình viên phát hiện ra sự không thích hợp hoặc lỗi trong các chương trình CGI, họ viết lại chương trình và thay thế chúng. Các CGI đã quá cũ và lỗi thời nhưng không bị xoá bỏ, sẽ gây ra một số kẽ hở về an toàn trong hệ thống. Đồng thời, do các chương trình CGI và CGI script có thể cư trú ở bất cứ nơi nào trên máy chủ Web (có nghĩa là, trên thư mục hoặc danh mục bất kỳ), nên khó có thể theo dõi dấu vết và quản lý chúng. Tuy nhiên, bất cứ người nào khi xác định được dấu vết của chúng, có thể thay thế các CGI script, kiểm tra, tìm hiểu các điểm yếu của chúng và khai thác các điểm yếu này để truy

nhập vào một máy chủ Web và các nguồn tài nguyên của máy chủ Web này. Không giống với JavaScript, CGI script không chạy trong một vòng bảo vệ an toàn.

Các hiểm hoạ đối với chương trình khác

Tấn công nghiêm trọng khác (đối với máy chủ Web) có thể xuất phát từ các chương trình do máy chủ thực hiện. Các chương trình Java hoặc C++ được chuyển tới các máy chủ Web thông qua một máy khách, hoặc cư trú thường xuyên trên một máy chủ nhờ sử dụng một bộ nhớ đệm. Bộ nhớ đệm là một vùng nhớ lưu giữ các dữ liệu được đọc từ một file hoặc cơ sở dữ liệu. Bộ nhớ đệm được sử dụng khi có các hoạt động đầu vào và đầu ra, do đó một máy tính có thể xử lý các thông tin có trong file nhanh hơn các thông tin được đọc từ các thiết bị đầu vào hoặc ghi vào các thiết bị đầu ra. Bộ nhớ đệm đóng vai trò như là một "vùng tạm trú" cho dữ liệu đến và đi. Ví dụ, các thông tin trong cơ sở dữ liệu được xử lý và tập hợp lại trong một bộ nhớ đệm, do vậy, toàn bộ tập hợp hoặc phần lớn tập hợp được lưu giữ trong bộ nhớ của máy tính. Sau đó, bộ xử lý có thể sử dụng dữ liệu này khi thao tác và phân tích. Vấn đề của bộ nhớ đệm chính là các chương trình lấp đầy chúng có thể bị hỏng và làm đầy bộ nhớ đệm, tràn dữ liệu thừa ra ngoài vùng nhớ đệm. Thông thường, điều này xảy ra do chương trình có lỗi hoặc bị hỏng, gây tràn bộ nhớ. Đôi khi, lỗi xảy ra do chủ tâm. Trong từng trường hợp, cần giảm bớt các hậu quả nghiêm trọng có thể xảy ra.

Một lập trình viên có thể rút ra kinh nghiệm khi nhận được hậu quả do việc tràn bộ nhớ hoặc chạy một đoạn mã của chương trình có các chỉ lệnh ghi đè dữ liệu lên vùng bộ nhớ khác (không phải là vùng nhớ được quy định trước). Kết quả là chương trình bị treo và ngừng xử lý, đôi khi treo hoặc phá huỷ toàn bộ máy tính (PC hoặc máy tính lớn). Các phá huỷ chủ tâm (do cố tình mã chương trình sai) chính là các tấn công chối bỏ. Tấn công kiểu sâu Internet (Internet Worm) là một chương trình như vậy. Nó gây tràn bộ nhớ, phá hỏng tất cả các nguồn tài nguyên cho đến khi máy chủ không hoạt động được nữa.

Một kiểu tấn công tràn bộ nhớ đệm là viết chỉ lệnh vào các vị trí thiết yếu của bộ nhớ, nhờ vậy chương trình của đối tượng xâm nhập trái phép có thể ghi đè lên các bộ nhớ đệm, máy chủ Web tiếp tục hoạt động, nạp địa chỉ của mã chương trình tấn công chính vào thanh ghi trong. Kiểu tấn công này có thể gây ra thiệt hại nghiêm trọng cho máy chủ Web, vì chương trình của đối tượng tấn công có thể giành được kiểm soát ở mức đặc quyền rất cao. Việc chiếm dụng chương trình dẫn đến các file bị lộ và phá huỷ.

Dữ liệu được chuyển vào một bộ nhớ đệm và sau đó được chuyển vào vùng lưu của hệ thống. Vùng lưu là nơi chương trình lưu giữ các thông tin thiết yếu, chẳng hạn như nội dung các thanh ghi của bộ xử lý trung tâm, các kết quả tính toán từng phần của một chương trình trước khi quyền kiểm soát được chuyển cho chương trình khác. Khi quyền kiểm soát được trả lại cho chương trình ban đầu, các nội dung của vùng lưu được nạp lại vào các thanh ghi của CPU và quyền kiểm soát được trả lại cho chỉ lệnh tiếp theo của chương trình. Tuy nhiên, khi quyền kiểm soát được trả lại cho chương trình tấn công, nó sẽ không từ bỏ quyền kiểm soát này. Các liên kết tấn công làm tràn bộ đệm (Buffer overflow attacks) trong

Online Companion trình bày chi tiết các điểm yếu dễ bị tấn công của bộ nhớ đệm của hai máy chủ Web khác nhau.

Một tấn công tương tự có thể xảy ra trên các máy chủ thư điện tử. Tấn công này được gọi là bom thư, nó xảy ra khi có hàng trăm, hàng ngàn người muốn gửi một thông báo đến một địa chỉ. Mục đích của bom thư là chất đống một số lượng lớn các thư và số lượng thư này vượt quá giới hạn kích cỡ thư cho phép, chính điều này làm cho các hệ thống thư tín rơi vào tình trạng tắc nghẽn hoặc trục trặc. Các bom thư có vẻ giống như spamming, nhưng chúng đối ngược nhau. Spamming xảy ra khi một cá nhân hoặc một tổ chức gửi một thông báo đơn lẻ cho hàng ngàn người và gây rắc rối hơn một hiểm hoạ an toàn.

1.4 CERT

Từ một thập kỷ trước, một nhóm các nhà nghiên cứu đã tập trung tìm hiểu và cố gắng loại bỏ tấn công kiểu sâu Internet. Trung tâm an toàn máy tính Quốc gia Mỹ (National Computer Security Center) và một bộ phận của Cục An ninh Quốc Gia là những đơn vị đi đầu trong việc tổ chức các cuộc hội thảo nhằm tìm ra phương cách đối phó với các xâm phạm an toàn có thể ảnh hưởng tới hàng ngàn người trong tương lai. Ngay sau cuộc hội thảo với các chuyên gia an toàn, DARPA thành lập trung tâm phối hợp CERT (Nhóm phản ứng khẩn cấp các sự cố về máy tính) và chọn trường đại học Carnegie Mellon ở Pittsburgh làm trụ sở chính. Các thành viên của CERT có trách nhiệm trong việc thiết lập một cơ sở hạ tầng truyền thông nhanh và hiệu quả, nhờ đó có thể ngăn chặn hoặc nhanh chóng loại bỏ các hiểm hoạ an toàn trong tương lai.

Trong mười năm đầu tiên kể từ khi thành lập, CERT đã đối phó được hơn 14.000 sự cố và các rắc rối liên quan đến an toàn xảy ra trong chính phủ Mỹ và khu vực tư nhân. Ngày nay, CERT vẫn tiếp tục nhiệm vụ của mình, cung cấp các thông tin phong phú để trợ giúp những người sử dụng Internet và các công ty nhận thức được các rủi ro trong việc xây dựng các site thương mại. Ví dụ, CERT gửi đi các cảnh báo cho cộng đồng Internet biết các sự cố liên quan đến an toàn mới xảy ra gần đây. Tư vấn và đưa các thông tin có giá trị để tránh các tấn công dịch vụ tên miền.

1.5 Tóm tắt

An toàn thương mại điện tử vô cùng quan trọng. Các tấn công có thể khám phá các thông tin độc quyền hoặc xử lý chúng. Một chính sách an toàn thương mại bất kỳ phải bao gồm tính bí mật, tính toàn vẹn, tính sẵn sàng và quyền sở hữu trí tuệ.

Các hiểm hoạ đối với thương mại có thể xảy ra ở bất kỳ mắt xích nào trong dây chuyền thương mại, bắt đầu với một máy khách, kết thúc với các máy chủ thương mại và văn phòng. Các thông tin về tấn công virus giúp cho người sử dụng nhận thức được các rủi ro thường gặp đối với các máy khách. Tuy nhiên, cũng có những hiểm hoạ khó phát hiện hơn, chúng là các applet phía máy khách. Java, JavaScript và ActiveX control là những ví dụ về các chương trình và script chạy trên các máy khách và có nguy cơ phá vỡ sự an toàn.

Nói chung, các kênh truyền thông và Internet là những điểm yếu đặc biệt dễ bị tấn công. Internet là một mạng rộng lớn và không một ai có thể kiểm soát hết được các nút mà thông tin đi qua. Các hiểm hoạ luôn có khả năng xảy ra như khám phá thông tin cá nhân trái phép, sửa đổi các tài liệu kinh doanh thiết yếu, ăn cắp và làm mất các thông báo thương mại quan trọng. Dạng tấn công kiểu sâu Internet được tung ra trong năm 1998 là một ví dụ điển hình về hiểm hoạ an toàn, nó sử dụng Internet như là một công cụ đi khắp thế giới và lây nhiễm sang hàng ngàn máy tính chỉ trong vài phút.

Cũng giống như các máy khách, máy chủ thương mại là đối tượng của các hiểm hoạ an toàn. Trầm trọng hơn, các hiểm hoạ an toàn có thể xảy ra với bất kỳ máy khách nào kết nối với máy chủ. Các chương trình CGI chạy trên các máy chủ có thể gây thiệt hại cho các cơ sở dữ liệu, các phần mềm cài đặt trong máy chủ và sửa đổi các thông tin độc quyền nhưng khó bị phát hiện. Các tấn công có thể xuất hiện ngay trong máy chủ (dưới hình thức các chương trình) hoặc có thể đến từ bên ngoài. Một tấn công bên ngoài xảy ra khi một thông báo tràn ra khỏi vùng lưu giữ nội bộ của máy chủ và ghi đè lên các thông tin thiết yếu. Thông tin này có thể bị thay thế bằng dữ liệu hoặc các chỉ lệnh, các chương trình khác trên máy chủ thực hiện các chỉ lệnh này.

CERT được thành lập để nghiên cứu và xem xét các hiểm hoạ an toàn. Khi có một số lượng lớn các tấn công an toàn xảy ra, các thành viên của nhóm tập trung lại và thảo luận các giải pháp nhằm xác định và cố gắng loại bỏ những đối tượng tấn công điện tử. Các mối hiểm hoạ ngày càng cao, nếu thiếu các biện pháp bảo vệ an toàn đầy đủ cho các máy khách và máy chủ thương mại điện tử thì thương mại điện tử không thể tồn tại lâu dài. Các chính sách an toàn hiệu quả, cùng với việc phát hiện và đưa ra các ràng buộc chính là các hình thức bảo vệ truyền thông điện tử và các giao dịch điện tử.

CHƯƠNG 2

THỰC THI AN TOÀN CHO THƯƠNG MẠI ĐIỆN TỬ

Việc bảo vệ các tài sản điện tử không phải là một tuỳ chọn, mà nó thực sự cần thiết khi thương mại điện tử ngày càng phát triển. Thế giới điện tử sẽ phải thường xuyên đối mặt với các hiểm hoạ như virus, sâu, con ngựa thành Torroa, những đối tượng nghe trộm và các chương trình gây hại mà mục đích của chúng là phá vỡ, làm trễ hoặc từ chối truyền thông luồng thông tin giữa khách hàng và nhà sản xuất. Để tránh nguy cơ mất hàng tỷ đôla, việc bảo vệ phải được phát triển không ngừng để các khách hàng tin cậy vào các hệ thống trực tuyến, nơi họ giao dịch và kiểm soát công việc kinh doanh. Phần này trình bày các biện pháp an toàn, thông qua chúng có thể bảo vệ các máy khách, Internet và máy chủ thương mại.

2.1 Bảo vệ các tài sản thương mại điện tử

Dù các công ty có tiến hành kinh doanh thương mại qua Internet hay không, thì an toàn vẫn là một vấn đề vô cùng nghiêm trọng. Các khách hàng cần có được sự tin cậy, các giao dịch của họ phải được an toàn, không bị xem trộm và sửa đổi. Ngày nay, việc kinh doanh thương mại trực tuyến trở nên quá lớn, thậm chí còn không ngừng phát triển trong vài năm tới. Một số địa điểm bán lẻ và bán buôn truyền thống tồn tại trước khi thương mại điện tử ra đời có thể biến mất trên thị trường.

Trước đây, an toàn có nghĩa là đảm bảo an toàn vật lý, chẳng hạn như cửa ra vào và cửa sổ có gắn chuông báo động, người bảo vệ, phù hiệu cho phép vào các khu vực nhạy cảm, camera giám sát, v.v. Điểm lại chúng ta thấy, các tương tác giữa con người và máy tính đã hạn chế các thiết bị đầu cuối cấm kết nối trực tiếp với các máy tính lớn. Giữa các máy tính không có kết nối nào khác. An toàn máy tính tại thời điểm này có nghĩa là đối phó với một số ít người truy nhập vào các thiết bị đầu cuối. Người ta chạy chương trình bằng cách đưa bìa đục lỗ vào thiết bị đọc. Sau đó họ lấy lại bìa cùng với các kết quả đầu ra. An toàn là một vấn đề khá đơn giản.

Ngày nay, hàng triệu người có thể truy nhập vào các máy tính trên mạng riêng và mạng công cộng (số lượng máy tính kết nối với nhau lên đến hàng ngàn máy). Thật không đơn giản khi xác định ai là người đang sử dụng một nguồn tài nguyên máy tính, bởi vì họ có thể ở bất cứ nơi nào trên thế giới, chẳng hạn như Nam Phi, nhưng họ lại sử dụng máy tính ở California. Ngày nay, nhiều công cụ và giải pháp an toàn mới được đưa ra và sử dụng nhằm bảo vệ các tài sản thương mại. Việc truyền các thông tin có giá trị (chẳng hạn như hóa đơn điện tử, yêu cầu đặt hàng, số thẻ tín dụng và xác nhận đặt hàng) đã làm thay đổi cách thức nhìn nhận về an toàn, cần đưa ra các giải pháp điện tử và tự động để đối phó lại các mối đe doạ đến tính an toàn.

Từ thời xa xưa, Julius Caesar đã mã hoá các thông tin nhằm ngăn chặn không cho đối phương đọc các thông tin bí mật và các kế hoạch phòng thủ trong chiến tranh. Trở lại 20 năm trước, Bộ quốc phòng Mỹ đã thành lập một cộng đồng để phát triển các nguyên tắc an toàn máy tính, quản lý các thông tin được phân loại trong máy tính. Kết quả mà cộng đồng này đạt được là cuốn "Trusted Computer System Evaluation Criteria". Trong đó trình bày các nguyên tắc mang tính bắt buộc trong việc kiểm soát truy nhập (phân loại thông tin thành 3 mức là mật, tuyệt mật và tối mật) và thiết lập tiêu chuẩn cho các mức chứng thực.

Việc định nghĩa các giới hạn an toàn, các điều kiện và các cuộc kiểm tra an toàn không đưa ra cách thức kiểm soát an toàn thương mại điện tử như thế nào. Tuy nhiên, công việc này vẫn có ích, bởi vì nó đặt ra các hướng nghiên cứu, tìm kiếm các giải pháp an toàn thiết thực và có thể áp dụng được. Ví dụ, các chuyên gia đã nghiên cứu và cho rằng chúng ta không thể xây dựng được một hệ thống thương mại an toàn nếu thiếu chính sách an toàn. Chính sách này phải nêu được các tài sản cần bảo vệ, cần những gì để bảo vệ các tài sản này, phân tích các khả năng đe doạ có thể xảy ra và các nguyên tắc bắt buộc để bảo vệ các tài sản này. Nó phải được xem xét thường xuyên do các mối đe doạ không ngừng phát sinh. Việc thực thi an toàn thực sự khó khăn khi chúng ta không có một chính sách an toàn.

Chúng ta cần phải bảo vệ các tài sản, tránh bị khám phá, sửa đổi, hoặc huỷ bỏ trái phép. Tuy nhiên, chính sách an toàn trong quân sự khác với chính sách an toàn trong thương mại, bởi vì các ứng dụng quân sự bắt buộc chia thành các mức an toàn. Thông thường, thông tin của công ty được phân loại thành "công khai" hoặc "bí mật công ty". Chính sách an toàn điển hình (liên quan đến các thông tin bí mật của công ty) cần phải dứt khoát - không làm lộ thông tin bí mật của công ty cho bất kỳ ai bên ngoài công ty.

Như đã biết, một chính sách an toàn phải đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của hệ thống và xác thực người dùng. Tiến sĩ Eugene Spafford, một giảng viên về khoa học máy tính của trường đại học Purdue, một chuyên gia về an toàn máy tính, đã trình bày tầm quan trọng của việc tiến hành thương mại điện tử an toàn. Trong một cuộc phỏng vấn với Purdue University Perspective, ông nói: "Việc bảo vệ thông tin là mối quan tâm chính, nó liên quan đến việc phòng thủ quốc gia, thương mại và thậm chí cả cuộc sống riêng của chúng ta. Nó cũng là một công việc kinh doanh với các triển vọng to lớn. Tại Mỹ, thương mại trực tuyến được ước tính sẽ vượt quá 15 tỷ đôla hàng năm cho đến năm 2000...". Rõ ràng, an toàn là yếu tố sống còn đối với sự tồn tại và phát triển của thương mại điện tử.

2.2 Bảo vệ sở hữu trí tuệ

Bảo vệ sở hữu trí tuệ số đặt ra nhiều vấn đề và chúng không giống với các vấn đề an toàn sở hữu trí tuệ truyền thống. Sở hữu trí tuệ truyền thống, chẳng hạn như văn học, hội hoạ và âm nhạc được bảo vệ bằng luật quốc gia và trong một số trường hợp, bằng luật quốc tế. Sở hữu trí tuệ số, chẳng hạn như hình ảnh, biểu trưng và âm nhạc trên Web site cũng được bảo vệ bằng luật. Các luật này không ngăn chặn các xâm phạm xảy ra, không cung cấp cách thức để tìm ra, bằng cách nào mà một đối tượng xâm phạm có được sở hữu trí tuệ. Tài sản số rơi vào tình trạng tiến thoái lưỡng nan, làm sao vừa hiển thị và làm cho sở hữu trí tuệ có

hiệu lực trên Web, vừa bảo vệ được các công việc có tính bản quyền này. Việc bảo vệ sở hữu trí tuệ an toàn tuyệt đối là rất khó, bạn cần thực hiện một số biện pháp nhằm cung cấp một mức bảo vệ và trách nhiệm nào đó đối với các bản quyền.

Quốc hội Mỹ đang cố gắng đưa ra luật xử lý các vấn đề bản quyền số. Tổ chức WIPO đang cố gắng giám sát các vấn đề bản quyền số mang tính toàn cầu. Trong lúc đó, một số công ty đưa ra một vài sản phẩm có khả năng cung cấp biện pháp bảo vệ cho người nắm giữ bản quyền số. Tình trạng xâm phạm bản quyền có xu hướng gia tăng và lĩnh vực này còn khá mới mẻ, ít nhất tại Mỹ, luật bản quyền đã được áp dụng cho Internet và môi trường số khác. ITAA là một tổ chức thương mại đại diện cho công nghệ thông tin của Mỹ, đã đưa ra một tài liệu đầy đủ về việc bảo vệ các thông tin số có bản quyền. Theo tài liệu "Bảo vệ sở hữu trí tuệ trong không gian máy tính", các vấn đề bảo vệ bản quyền số hiện nay cần được thảo luận và đưa ra một số giải pháp. Các giải pháp đó bao gồm:

- Khoá tên máy chủ
- Lọc gói
- Các máy chủ uỷ quyền

Trong đó, các nhà cung cấp dịch vụ Internet ngăn chặn truy nhập vào một site, bằng cách khoá IP, lọc gói, hoặc sử dụng một máy chủ uỷ quyền để lọc các yêu cầu. Tuy nhiên, không một giải pháp nào thực sự hiệu quả trong việc ngăn chặn nạn ăn cắp hoặc nhận dạng tài sản giành được mà không có sự đồng ý của người nắm giữ bản quyền.

Một số giải pháp tập trung vào việc bảo vệ bằng các giải pháp công nghệ số. Ví dụ như software metering, digital watermark, digital envelope (đôi khi chúng còn được gọi là các chương trình xác thực thông báo). Các giải pháp này chưa thật đầy đủ nhưng dù sao nó cũng cung cấp một khả năng bảo vệ nào đó.

2.3 Bảo vệ các máy khách

Các máy khách (thông thường là các PC) phải được bảo vệ nhằm chống lại các đe doạ xuất phát từ phần mềm hoặc dữ liệu được tải xuống máy khách từ Internet. Như chúng ta đã biết, các trang Web thông thường được chuyển tới máy tính của bạn nhằm đáp ứng yêu cầu (hiển thị tĩnh các thông tin và hoàn toàn vô hại với bất cứ ai) của trình duyệt của bạn. Các active content được chuyển qua Internet thông qua các trang Web động. Chúng có thể là một trong các mối đe doạ nghiêm trọng nhất đối với các máy khách.

Như chúng ta đã biết, active content bao gồm nhiều chương trình được nhúng vào các trang Web, tạo nên sự sống động cho các trang Web. Tuy nhiên, một active content giả có vẻ vô hại nhưng lại gây ra các thiệt hại khi chúng chạy trên máy tính của bạn. Các chương trình được viết bằng Java, JavaScript mang lại sự sống động cho các trang Web. Một số các công cụ active content phổ biến khác là các ActiveX control. Bên cạnh các mối đe doạ xuất phát từ các chương trình bên trong các trang Web, thì các trình đồ hoạ, các trình duyệt gài sẵn (trình duyệt plug-ins) và các phần đính kèm thư điện tử cũng là các mối đe doạ có thể gây hại cho các máy khách khi các chương trình ẩn này được thực hiện.

Nhiều active content gây hại có thể lan truyền thông qua các cookie. Các đoạn văn bản nhỏ này được lưu giữ trên máy tính của bạn và có chứa các thông tin nhạy cảm không được mã hoá. Điều này có nghĩa là bất kỳ ai cũng có thể đọc và làm sáng tỏ một cookie, thu được thông tin có trong đó. Thông tin này liên quan đến thẻ tín dụng, mật khẩu và thông tin đăng nhập. Do cookie giống như các thẻ đăng nhập vào các Web site, chúng không gây hại trực tiếp cho các máy khách nhưng nó vẫn là nguyên nhân gây ra các thiệt hại.

Một mối đe doạ khác đối với máy khách là một server site đóng giả một Web site hợp pháp. Đây thực sự là một mối quan tâm an toàn đối với máy khách, các máy khách cần có trách nhiệm nhận biết các máy chủ của mình. Các mục tiếp theo trình bày các cơ chế bảo vệ hiện có, chúng được thiết kế nhằm ngăn chặn hoặc giảm đáng kể khả năng các hiểm hoạ xảy ra đối với máy khách.

Giám sát Active content

Các trình duyệt Navigator của Netscape và Internet Explorer của Microsoft được trang bị để nhận biết các trang Web có chứa active content chuẩn bị được tải xuống. Khi bạn tải về và chạy các chương trình được nhúng vào các trang Web, bạn muốn đảm bảo rằng các chương trình này đến từ một nguồn bạn biết và tin cậy. Cách thức mà hai trình duyệt trên sử dụng để đảm bảo an toàn được trình bày trong các mục sau đây. Trước hết chúng ta xem xét các chứng chỉ số, chúng thực sự cần thiết cho phía máy khác và máy chủ khi xác thực.

Các chứng chỉ số

Một chứng chỉ số (hay ID số) là phần đính kèm với thông báo thư điện tử hoặc một chương trình được nhúng vào một trang Web. Khi một chương trình được tải xuống có chứa một chứng chỉ số, nó nhận dạng nhà phát hành phần mềm và thông báo thời hạn hợp lệ của chứng chỉ. Một chứng chỉ không chứa bất kỳ điều gì liên quan đến khả năng hoặc chất lượng của chương trình được tải xuống. Ngầm định của việc sử dụng các chứng chỉ là nếu bạn tin cậy nhà cung cấp phần mềm, chứng chỉ cung cấp cho bạn sự đảm bảo rằng phần mềm được ký có nguồn gốc từ nhà cung cấp tin cậy.

Cơ quan chứng thực (CA) phát hành chứng chỉ số cho cá nhân hoặc tổ chức. Nếu bạn so sánh chứng chỉ số với một thẻ hộ chiếu, CA giống như bộ ngoại giao, là một cơ quan phát hành các thẻ hộ chiếu. Bộ ngoại giao yêu cầu bất cứ người nào, khi họ muốn có một thẻ hộ chiếu, cần cung cấp một vài bằng chứng nhận dạng cùng với một bức ảnh. Cũng tương tự như vậy, CA yêu cầu các thực thể muốn có chứng chỉ cần cung cấp bằng chứng nhận dạng thích hợp. Một khi đáp ứng được điều này, CA sẽ phát hành một chứng chỉ. CA ký chứng chỉ (đóng tem phê chuẩn), theo dạng khoá mã công khai, "không giữ bí mật" đối với bất kỳ người nào nhận chứng chỉ (được gắn với phần mềm của nhà phát hành). Khoá là một số, thường là một số nhị phân dài (long binary), được sử dụng với thuật toán mã hoá nhằm "giữ bí mật" các ký tự có trong thông báo mà bạn muốn bảo vệ, vì vậy, không thể đọc được hoặc giải mã chúng (trừ khi bạn biết khoá). Các khoá dài có khả năng bảo vệ tốt hơn các khoá ngắn. Một trong các CA tồn tại lâu nhất và được nhiều người biết đến là VeriSign.

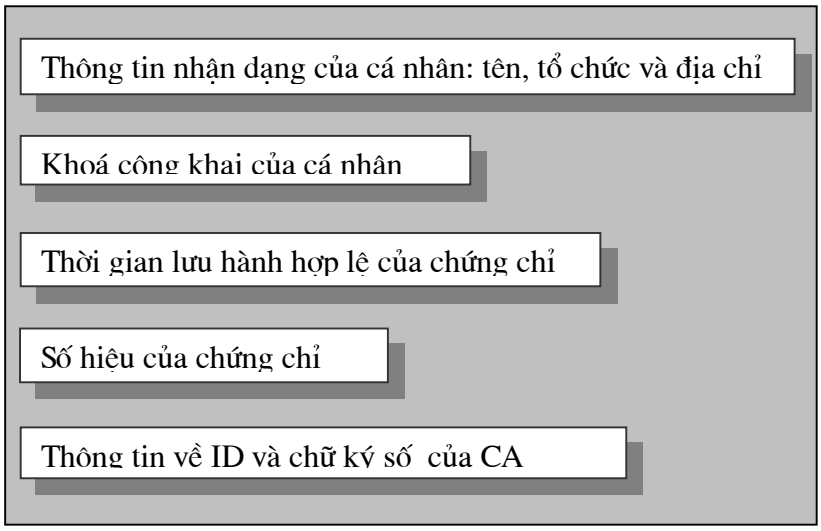
Yêu cầu nhận dạng của các CA cũng khác nhau. Một CA có thể yêu cầu bằng lái xe đối với các chứng chỉ cá nhân, trong khi các CA khác có thể yêu cầu vân tay. Các chứng chỉ được phân loại thành các lớp đảm bảo như sau: thấp, trung bình, hoặc cao, phụ thuộc phần lớn vào các yêu cầu nhận dạng cần phải đáp ứng.

VeriSign đưa ra một số lớp chứng chỉ, từ lớp 1 đến 4. Các chứng chỉ lớp 1 là các chứng chỉ ở mức thấp nhất, gắn liền với các địa chỉ thư điện tử và các khoá công khai. Các chứng chỉ lớp 4 áp dụng cho các máy chủ và tổ chức của chúng. Các yêu cầu đối với chứng chỉ lớp 4 cao hơn rất nhiều so với các yêu cầu dành cho chứng chỉ lớp 1. Ví dụ, các chứng chỉ lớp 4 của VeriSign đảm bảo nhận dạng cá nhân và mối quan hệ của cá nhân này cho công ty hoặc tổ chức xác định. Hình 2.1 minh hoạ cấu trúc tổng quát của một chứng chỉ VeriSign. Bạn có thể đọc các mục tiếp theo để biết được khi nào và làm thế nào để thay đổi các chứng chỉ để có sự đảm bảo giữa máy khách và máy chủ.

Mục tiếp theo trình bày các đặc tính an toàn được xây dựng trong hai trình duyệt phổ biến nhất, Internet Explorer của Microsoft và Navigator.

Trình duyệt Internet của Microsoft (Microsoft Internet Explorer)

Internet Explorer cung cấp quyền bảo vệ phía máy khách trong các trình duyệt. Ngoài việc đưa ra các cảnh báo nhằm ngăn chặn không cho trẻ em sử dụng các site không lành mạnh, Internet Explorer cũng đối phó lại các active content dựa vào Java và ActiveX. Internet Explorer sử dụng kỹ thuật mã xác thực (Authenticode) của Microsoft để kiểm tra nhận dạng của các active content được tải xuống. Các chương trình Authenticode có thể kiểm tra đối với một ActiveX control được tải xuống như sau: ai là người đã ký chương trình, chương trình có bị sửa đổi sau khi ký hay không và nội dung có nguồn gốc đúng từ nhà phát hành tin cậy hay không. Đồng thời kiểm tra xem chương trình có chứng chỉ hợp lệ hay không. Tuy nhiên, nó không thể ngăn chặn được việc tải xuống một chương trình gây hại và chạy trên máy tính của bạn. Có nghĩa là, kỹ thuật Authenticode chỉ có thể xác nhận đúng là công ty XYZ (bạn tin cậy) đã ký chương trình. Nếu nhà phát hành không gắn chứng chỉ vào active content, bạn có thể cài đặt Internet Explorer, vì vậy đoạn mã chương trình của trang Web không bị tải xuống. Tuy nhiên, Authenticode không thể đảm bảo Java hoặc ActiveX control của công ty XYZ có thực hiện đúng đắn hay không. Trách nhiệm này thuộc về bạn và bạn phải quyết định có nên tin cậy vào active content từ các công ty cá nhân hay không.



Hình 2.1 Cấu trúc một chứng chỉ của VeriSign

Nếu bạn định tải về một trang Web có chứa active content, nhưng active content này chưa được ký, sẽ xuất hiện một hộp thoại chỉ báo rằng ở đây không có chứng chỉ hợp lệ. Việc Internet Explorer có hiển thị cảnh báo an toàn hay không phụ thuộc vào việc bạn định cấu hình an toàn cho trình duyệt của mình như thế nào.

Các chứng chỉ có thời hạn tồn tại nhất định. Bạn có thể nhấn vào một siêu liên kết để xem nhãn thời gian của hãng. Nhãn thời gian này cho biết thời hạn tồn tại hợp lệ của một chứng chỉ. Các hãng phải kết hợp với CA một cách định kỳ để phê chuẩn lại chứng chỉ của mình. Chứng chỉ sẽ bị thu hồi nếu thời hạn tồn tại của nó kết thúc. Nếu CA xác định được một hãng đã có lần phân phối chương trình kém chất lượng và gây hại, CA có thể từ chối không phát hành các chứng chỉ mới và thu hồi các chứng chỉ đang tồn tại mà không cần có sự đồng ý của hãng.

Bạn có thể xác định các thiết lập an toàn khác nhau, các thiết lập này quyết định Internet Explorer quản lý các chương trình và các file mà nó tải xuống như thế nào, phụ thuộc vào nguồn gốc các file. Internet Explorer chia Internet thành nhiều vùng. Bạn có thể phân loại các Web site và xếp chúng vào một trong các vùng này, sau đó gán nhãn an toàn thích hợp cho từng vùng, hoặc nhóm các Web site. Ở đây có 4 vùng (zone) như sau: Internet, Intranet cục bộ, các site tin cậy và các site bị giới hạn. Internet zone là bất cứ thứ gì không có trong máy tính của bạn, không có trên Intranet, hoặc không được gán nhãn cho các vùng khác. Vùng Intranet cục bộ thường chứa các Web site không yêu cầu máy chủ uỷ quyền, mạng nội bộ của hãng trong đó máy khách của bạn được gắn vào, các site của Intranet cục bộ khác. Bạn có thể tải các nội dung xuống một cách an toàn từ các site này mà không phải lo lắng bởi vì chúng hoàn toàn tin cậy. Vùng các site bị giới hạn có chứa các Web site mà bạn

không tin cậy. Chúng là các site không cần thiết hoặc gây hại nhất thiết phải huỷ bỏ. Bạn có thể gán mức an toàn theo các mức sau: Low (thấp), Medium-Low (trung bình thấp), Medium (trung bình), High (cao).

Kỹ thuật Authenticode rút ngắn gọn thành các quyết định có/không (yes/no) đối với người và những gì mà bạn tin cậy. Bạn có thể tuỳ chỉnh các thiết lập an toàn của mình, nhưng bảo vệ vẫn là sự chọn lựa nên hay không nên chạy chương trình động. Authenticode giám sát liên tục chương trình khi nó đang chạy. Vì vậy, chương trình mà Authenticode cho phép vào máy tính của bạn vẫn có thể gặp sự cố (hoặc do lỗi chương trình hoặc hành động chủ tâm). Nói cách khác, một khi bạn không quan tâm đến tính tin cậy của một site, một vùng hay một nhà cung cấp, bạn gặp phải nhiều lỗ hổng về an toàn khi bạn tải nội dung về. Nguyên nhân của hầu hết các thiệt hại đối với các máy tính là do các lỗi chương trình, do không kiểm tra phần mềm cẩn thận.

Netscape Navigator

Trình duyệt Netscape Navigator cho phép kiểm soát việc tải các active content xuống máy tính của bạn. Nếu bạn cho phép Netscape Navigator tải xuống active content, bạn có thể xem chữ ký gắn kèm với Java và JavaScript control (ActiveX control không thực hiện với Netscape Navigator). Bắt đầu với hộp thoại Preferences, bạn chọn "Preferences" từ menu Edit, khi hộp thoại Preferences mở, bạn nhấn vào "Advanced" ở panel bên trái. Panel bên phải hiển thị các thiết lập an toàn của bạn. Bạn có thể chọn cho phép hoặc không cho phép Java, JavaScript. Trong cùng hộp thoại, bạn có thể quyết định những gì cần làm với các cookie. 3 nút tuỳ chọn thiết lập xử lý các cookie như thế nào, bạn có thể chọn chấp nhận vô điều kiện các cookie, hoặc chọn các cookie được gửi ngược trở lại cho máy chủ, hoặc không cho phép tất cả các cookie.

Nếu active content viết bằng Java và JavaScript, bạn sẽ thường xuyên nhận được một thông báo từ Netscape Navigator. Thông báo cho biết active content đã được ký hay chưa, cho phép bạn xem chứng chỉ đi kèm để xác định nên chấp nhận hay từ chối tải xuống các active content.

Lưu ý rằng, Netscape Navigator đánh giá rủi ro cao. Khi nhấn vào "Details" trên khung cảnh báo an toàn, chúng ta có thể biết thêm các thông tin về yêu cầu tải hiện thời. Nhấn vào "Grant" cho phép thực hiện quá trình tải xuống. Nhấn vào "Deny" từ chối truy nhập, không cho phép tải Java applet hoặc JavaScript. Bạn có thể kiểm tra chứng chỉ (gắn kèm với active content) của nhà cung cấp bằng cách nhấn vào "Certificate".

Lưu ý rằng, chứng chỉ của nhà cung cấp có số thứ tự duy nhất cho từng chứng chỉ và chữ ký (chuỗi các số và chữ cái tiếp ngay sau nhãn "Certificate Fingerprint"). Chứng chỉ có thời gian tồn tại cụ thể.

Đối phó với các cookie

Cookie được lưu giữ trong máy tính của bạn, hoặc được tạo ra, sử dụng và huỷ bỏ trong một lần duyệt Web. Bạn cũng có thể cho phép chúng tồn tại từ 10, 20 hoặc 30 ngày. Một cookie có chứa nhiều thông tin, chẳng hạn như tên của Web site phát hành nó, các trang mà bạn đã truy cập vào, tên người sử dụng và mật khẩu của bạn, các thông tin về thẻ tín dụng và địa chỉ của bạn. Chỉ site tạo ra các cookie mới có thể lấy lại các cookie này, chúng thu thập và lưu giữ các thông tin không nhìn thấy được. Chính vì thế bạn không phải nhập lại tên người sử dụng, mật khẩu cho lần truy cập tiếp theo. Các phiên bản trình duyệt ban đầu cho phép các site lưu giữ các cookie không có chú thích. Ngày nay, các trình duyệt cho phép bạn lưu giữ các cookie mà không cần sự cho phép, hoặc cảnh báo cho biết một cookie chuẩn bị được lưu giữ, hoặc không cho phép vô điều kiện tất cả các cookie.

Ví dụ, trong Internet Explorer 5, bạn có thể tìm ra cách để đối phó các cookie như thế nào, bằng cách nhấn vào mục "Internet Options" từ menu Tools. Sau đó, nhấn vào "Security" và "Custom Level" cho vùng an toàn mà bạn muốn sửa đổi, chẳng hạn vùng Internet. Cuộn hộp thoại "Settings" cho đến khi định vị được nhóm các cookie. Sau đó, có thể nhấn vào các nút tuỳ chọn sau: "Enable", "Disable", hoặc "Prompt" cho các cookie được lưu giữ trên máy tính của bạn và các cookie chỉ sử dụng trong phiên làm việc đó. Các khởi tạo cho phép, không cho phép, hoặc gợi nhắc bạn về quyết định của mình mỗi khi một cookie chuẩn bị đi qua máy tính của bạn. Nó cho phép kiểm soát toàn bộ các cookie. Như đã trình bày ở trên, bạn có thể kiểm soát các cookie trên Netscape Navigator bằng cách chọn các mục tuỳ chọn trên hộp thoại "Preferences".

Sử dụng phần mềm chống virus

Không một máy khách nào có thể phòng thủ tốt nếu thiếu phần mềm chống virus. Các phần mềm chống virus chỉ bảo vệ máy tính của bạn khỏi bị các virus đã được tải xuống máy tính của bạn. Vì vậy, chống virus là một chiến lược phòng thủ. Không quan tâm đến phần mềm bạn chọn là phần mềm nào của nhà cung cấp, nó chỉ hiệu quả khi bạn tiếp tục lưu giữ các file dữ liệu chống virus hiện thời. Các file chứa thông tin nhận dạng virus được sử dụng để phát hiện các virus trên máy tính của bạn. Do các virus mới được sinh ra rất nhiều, bạn cần đề phòng và cập nhật các file dữ liệu chống virus một cách định kỳ, nhờ vậy mới có thể phát hiện và loại trừ các virus mới nhất.

2.4 Bảo vệ các kênh thương mại điện tử

Chúng ta dễ dàng nhận thấy, việc bảo vệ các kênh thương mại điện tử là một trong các phần quan trọng trong an toàn máy tính. Khó có thể có một ngày mà các báo và tạp chí không đăng tin về các vụ tấn công trên Internet hoặc các tin tặc cố gắng truy nhập vào một hệ thống máy tính thông qua các kênh truyền thông không an toàn, chẳng hạn như các Intranet, Extranet hoặc Internet. Do vậy, cần tập trung vào việc bảo vệ các tài sản khi chúng được chuyển tiếp giữa các máy khách và máy chủ từ xa. Việc cung cấp kênh thương mại an toàn đồng nghĩa với việc đảm bảo tính bí mật của kênh, tính toàn vẹn của thông báo và tính

sẵn sàng của kênh. Thêm vào đó, một kế hoạch an toàn đầy đủ còn bao gồm cả xác thực, đảm bảo rằng người đang sử dụng máy tính đúng là người mà họ nhận. Việc xác thực người dùng là một biện pháp an toàn nhằm bảo vệ các máy chủ thương mại, không phải là các kênh thương mại, được trình bày trong mục "Bảo vệ máy chủ thương mại". Trong mục tiếp theo, chúng ta sẽ tìm hiểu xác thực là một phần của các giao thức (chúng cung cấp các dịch vụ an toàn) như thế nào, tìm hiểu chi tiết các thủ tục xác thực. Bây giờ chúng ta xem xét từng dịch vụ an toàn cho các kênh thương mại, bắt đầu với tính riêng tư giao dịch.

Cung cấp tính riêng tư giao dịch

Khi bạn không ngăn chặn được những đối tượng nghe trộm *snooping* (một kiểu tấn công vào Internet), thì công việc kinh doanh phải sử dụng các kỹ thuật nhằm ngăn chặn những đối tượng nghe trộm đọc các thông báo Internet. Việc gửi một thông báo qua Internet giống như việc gửi một bưu thiếp qua thư, nó có thể đến được đích nhưng những người chuyển thư có thể đọc bưu thiếp, chỉ có cách mã hoá nó trước khi gửi lên Internet. Việc mã hoá thư điện tử hoặc giao dịch thương mại Internet giống với việc viết thông báo lên bưu thiếp bằng một ngôn ngữ mà chỉ có bạn và người nhận hiểu được. Không ai khác hiểu được ngôn ngữ này, vì vậy nếu họ lấy được thông báo, nó cũng chẳng có ý nghĩa gì đối với họ ngoại trừ người nhận hợp pháp.

Mã hoá

Mã hoá là quá trình mã các thông tin, bằng cách sử dụng một phương pháp toán học và một khoá bí mật để sinh ra một chuỗi các ký tự khó hiểu. Thực chất là việc che dấu các thông báo, chỉ người gửi và người nhận có thể đọc nó. Khoa học nghiên cứu mã hoá được gọi là mật mã.

Mật mã không liên quan đến nguỵ trang ký. Nguỵ trang ký làm cho mắt thường không nhìn thấy văn bản. Mật mã không cố gắng che dấu văn bản, nó chuyển đổi văn bản sang dạng chuỗi ký tự, chúng ta có thể nhìn được nhưng không hiểu nghĩa của nó. Một chuỗi ký tự khó hiểu được sinh ra bằng cách kết hợp các bít, tương ứng với các ký tự trong bảng chữ cái hoặc số, tạo thành một thông báo có vẻ như được lắp ráp ngẫu nhiên.

Một chương trình chuyển đổi văn bản rõ sang văn bản mã (sự lắp ráp ngẫu nhiên các bit) được gọi là chương trình mã hoá. Các thông báo được mã hoá ngay trước khi chúng được gửi lên mạng hoặc Internet. Khi tới đích hợp lệ, thông báo được giải mã nhờ chương trình giải mã. Chương trình mã hóa và logic sau chúng, gọi là thuật toán mã hoá, được coi là yếu tố cực kỳ quan trọng. Biết được tầm quan trọng của một số thuật toán, chính phủ Mỹ đã ngăn cấm việc công bố rộng rãi và chi tiết đối với chúng. Hiện tại, việc xuất khẩu một trong các thuật toán này là bất hợp pháp. Điều này đã ảnh hưởng đến một số công ty Mỹ cung cấp các phần mềm mã hoá hoặc phần mềm có chứa phần mềm mã hoá. Các trang Web có chứa phần mềm (mà việc phân phối chúng bị giới hạn) đưa ra các cảnh báo về luật xuất khẩu của Mỹ. Freedom Forum Online có đưa ra một số bài báo nói về các vụ kiện cáo và việc ban hành luật, xung quanh luật xuất khẩu mã hoá.

Một thuộc tính hấp dẫn và cần thiết của các thuật toán hoặc các chương trình mã hoá là một người có thể biết chi tiết chương trình mã hoá nhưng vẫn không có khả năng giải mã thông báo nếu không biết khoá được sử dụng trong quá trình mã hoá. Độ dài tối thiểu của một khoá là 40 bit, nó có thể dài hơn, chẳng hạn 128 bit, sẽ đảm bảo an toàn hơn nhiều.Với một khoá đủ dài, các thông báo khó bị phát hiện.

Kiểu của khoá và chương trình mã hoá được sử dụng để "giữ bí mật" một thông báo. Các phép mã được chia thành 3 loại:

- Mã hàm băm
- Mã hoá đối xứng
- Mã hoá không đối xứng

Mã hàm băm là một quá trình sử dụng thuật toán băm để tính toán một số, được gọi là giá trị băm, từ một thông báo có độ dài bất kỳ. Nó chính là dấu vân tay cho một thông báo vì nó gần như duy nhất đối với mỗi thông báo. Do sinh ra các thuật toán băm chất lượng tốt, khả năng xảy ra tình trạng (hai thông báo khác nhau có cùng kết quả băm) là vô cùng nhỏ. Mã hoá băm là một cách thích hợp để phát hiện nếu thông báo bị sửa đổi trong quá trình chuyển tiếp, bởi vì giá trị băm ban đầu và giá trị băm mà người nhận tính toán được sẽ không trùng khớp nếu thông báo bị sửa đổi.

Mã không đối xứng (mã hoá khoá công khai) mã hoá các thông báo bằng cách sử dụng hai khoá. Năm 1977, Ronald Rivert, Adi Shamir và Leonard Adleman phát minh ra hệ thống mật mã khoá công khai RSA (lấy các chữ cái đầu tên của các tác giả đặt tên cho thuật toán). Trong hệ thống này, một khoá trong cặp khoá (gọi là khoá công khai) được phân phối công khai cho bất kỳ ai muốn truyền thông an toàn với người nắm giữ cả hai khoá. Khoá công khai được sử dụng để mã hoá các thông báo. Khoá thứ hai (gọi là khoá riêng) được người sở hữu lưu giữ cẩn thận. Người sở hữu khoá sử dụng khoá riêng để giải mã các thông báo nhận được. Nói chung, hệ thống mã hoá làm việc như sau: Nếu Herb muốn gửi một thông báo cho Allison, anh ta cần có khoá công khai của Allison. Sau đó, anh ta mã hoá thông báo định gửi cho Allison, bằng khoá công khai của cô. Một khi thông báo được mã hoá, chỉ có Allison mới có thể đọc thông báo, cô giải mã thông báo bằng khoá riêng của mình. Do các cặp khoá là duy nhất, chỉ dùng khoá riêng mới giải mã được thông báo được mã hoá bằng khoá công khai (trong cặp khoá) nên Allison có thể gửi một thông báo bí mật cho Herb, bằng cách sử dụng khoá công khai của Herb. Khi nhận được thông báo của Allison, Herb sử dụng khoá riêng bí mật của mình để giải mã thông báo và đọc nó. Nếu họ gửi thư điện tử cho nhau, thông báo chỉ bí mật trong khi chuyển tiếp. Khi thông báo được tải từ máy chủ thư tín (mail server) và được giải mã, có dạng văn bản rõ trên máy của người nhận và hoàn toàn có thể đọc được.

Mã đối xứng (còn gọi là mã khoá riêng) sử dụng một khoá chung cho cả mã hoá và giải mã, chẳng hạn như 45683942078 để mã hoá và giải mã dữ liệu. Do sử dụng chung một khoá, cả người gửi lẫn người nhận thông báo đều phải biết khoá. Việc mã hoá và giải mã

thông báo sử dụng mã hoá đối xứng rất nhanh và hiệu quả. Tuy nhiên, khoá phải được giữ cẩn thận. Nếu khoá bị lộ, tất cả các thông báo trước đó đều bị lộ và cả người gửi lẫn người nhận phải sử dụng khoá mới cho các cuộc truyền thông tiếp theo. Quá trình phân phối khoá mới cho các thành viên rất khó khăn. Lưu ý rằng, muốn truyền bí mật bất cứ thứ gì thì người ta cần phải mã hoá nó, bao gồm cả thông tin và khoá bí mật. Một vấn đề lớn đối với các khoá riêng là chúng không thích hợp trong các môi trường lớn, chẳng hạn như Internet. Vì phải có một khoá riêng cho mỗi cặp người sử dụng trên Internet khi họ muốn chia xẻ thông tin một cách bí mật, cho nên cần phải có số lượng lớn sự kết hợp các cặp khoá, giống như hệ thống các đường dây điện thoại riêng không có các trạm chuyển mạch. 12 người có thể có một cặp khoá riêng trong số các cặp khoá, đòi hỏi 66 khoá riêng. Nói chung, với N máy khách cá nhân, bạn cần khoảng $1/2N^2$ cặp khoá.

Trong các môi trường an toàn, việc sử dụng mã hoá khoá riêng rất đơn giản, trong thực tế, nó là một giải pháp phổ biến để mã hoá dữ liệu nhạy cảm. Trong khu vực quốc phòng, việc phân phối các thông tin (đã được phân loại) và các khoá mã không có gì khó khăn. Nó yêu cầu bảo vệ, kiểm soát hai bên và các kế hoạch truyền bí mật. DES là một chuẩn mã hoá dữ liệu, được chính phủ Mỹ chấp nhận sử dụng khi mã hoá các thông tin nhạy cảm hoặc thông tin thương mại. Nó là một hệ thống mã hoá khoá riêng được sử dụng rộng rãi nhất. Tuy nhiên, kích cỡ khoá riêng DES ngày càng tăng, lý do là số lượng cá nhân sử dụng máy tính tăng lên nhanh chóng, làm cho việc mã hoá thông báo bằng các khoá ngắn là không đủ an toàn.

Các hệ thống khoá công khai mang lại một số thuận lợi, so với các giải pháp mã hoá khoá riêng.Thứ nhất, việc kết hợp các khoá (được yêu cầu cung cấp cho các thông báo bí mật giữa một số lượng người khổng lồ) là nhỏ. Nếu có N người muốn chia xẻ thông tin với người khác một cách bí mật thì chỉ cần duy nhất N cặp khoá công khai, ít hơn rất nhiều so với hệ thống khoá riêng tương đương. Thứ hai, việc phân phối khoá không phải là một vấn đề. Khoá công khai của mỗi người có thể được gửi đi theo đường bí mật nếu cần thiết và không yêu cầu bất kỳ sự kiểm soát đặc biệt nào khi phân phối. Thứ ba, các hệ thống khoá công khai có khả năng thực thi chữ ký số. Điều này có nghĩa là một tài liệu điện tử có thể được ký và gửi cho người nhận bất kỳ, cùng với chống chối bỏ. Có nghĩa là, với kỹ thuật khoá công khai, khó có thể tồn tại một người nào khác ngoài người ký - sinh ra chữ ký điện tử; Thêm vào đó, người ký không thể chối bỏ việc ký tài liệu sau khi đã ký. Các hệ thống khoá công khai có một số khó khăn. Một trong các khó khăn đó là quá trình mã hoá và giải mã khá chậm so với các hệ thống khoá riêng. Khoảng thời gian chênh lệch này sẽ tăng lên một cách nhanh chóng nếu bạn và các khách hàng của bạn tiến hành thương mại trên Internet. Người ta không có ý định thay thế các hệ thống khoá riêng bằng các hệ thống khoá công khai. Chúng bổ xung lẫn nhau. Các hệ thống khoá công khai được sử dụng để truyền các khoá riêng cho các thành viên.

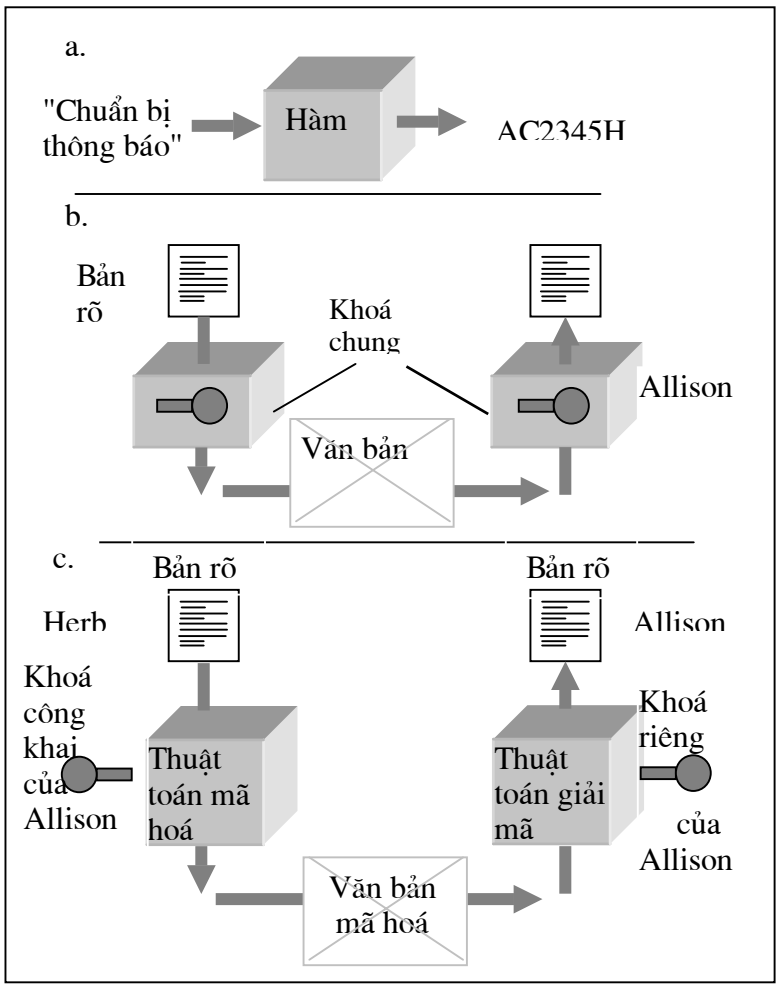
Hình 2.2 minh hoạ các giải pháp băm, mã hoá khoá riêng, mã hoá khoá công khai, trong đó Herb gửi một thông báo bí mật cho Allison.

Các chuẩn và thuật toán mã hoá

Hiện nay có một số thuật toán mã hoá và giải mã được sử dụng với các máy chủ thương mại an toàn. Chính phủ Mỹ đã phê chuẩn cho phép sử dụng một số thuật toán này trong phạm vi nước Mỹ, còn một số thuật toán yếu hơn được sử dụng bên ngoài nước Mỹ. Thông thường, các máy chủ thương mại an toàn dàn xếp hầu hết (nếu không muốn nói là tất cả) các thuật toán khác nhau này, bởi vì chúng phải có khả năng truyền thông với các trình duyệt. Để dàn xếp các trình duyệt (có phiên bản khác nhau), các máy chủ phải đưa ra một dãy mã nhỏ, nhằm ngăn chặn việc gửi nhiều lần các thuật toán quan trọng và có thể nhìn thấy.

Hiện có rất nhiều thuật toán như: Blowfish, DES, ECC, IDEA, LUC, MD2, MD4, MD5, RC2, RC4, RC5, RC6, RSA, SHA1, Skipjack, Triple DES thuộc các kiểu khoá công khai, khoá riêng và digest (Hash).

Một máy chủ hoặc trình duyệt an toàn sử dụng một hoặc nhiều thuật toán này khi nó mã hoá thông tin. Các thuật toán được trình bày ở trên có 3 kiểu khác nhau. Chúng ta đã tìm hiểu hai trong 3 kiểu này: khoá riêng và khoá công khai. Tại sao có nhiều hơn một thuật toán? Liệu một thuật toán có thể thoả mãn tất cả các yêu cầu an toàn không? Câu trả lời là các thuật toán khác nhau có độ mạnh khác nhau, một số thuật toán đã cũ và không còn phù hợp với việc sử dụng hiện nay và các đơn vị xử lý trung tâm tốc độ cao. Kiểu thứ 3 được gọi là Digest (Hash). Các thuật toán Digest không mã hoá các thông tin. Thay vào đó, chúng tính toán một số có độ dài định sẵn từ một thông báo. Số có độ dài định sẵn, thường dài 128 bít, là một chữ ký (tóm lược nội dung của thông báo). Chúng là chữ ký của thông báo. Các chữ ký này đảm bảo (với những người nhận thông báo) rằng thông báo không bị sửa đổi nếu thông báo nhận được có cùng tóm lược với thông báo gốc. Nếu không, người nhận biết rằng thông báo gốc đã bị sửa đổi. Các thuật toán kiểu này gồm có MD2, MD4 và MD5.



Hình 2.2 (a) Thực hiện mã băm, (b) Mã hoá khoá riêng, (c) Mã hoá khoá công khai

Giao thức Secure Socket Layer (SSL)

Giao thức SSL của Netscape và giao thức truyền siêu văn bản an toàn (S-HTTP) của CommerceNet là hai giao thức cho phép truyền thông tin an toàn qua Internet. SSL và S-HTTP cho phép các máy khách và máy chủ quản lý các hoạt động mã hoá và giải mã trong một phiên Web an toàn.

SSL và S-HTTP có các mục tiêu khác nhau. Trong khi SSL đảm bảo kết nối giữa hai máy tính, S-HTTP gửi các thông báo riêng lẻ an toàn. Việc mã hoá các thông báo gửi đi và giải mã các thông báo nhận diễn ra tự động và trong suốt đối với cả SSL và S-HTTP. SSL làm việc ở tầng vận tải, còn S-HTTP làm việc ở tầng ứng dụng.

SSL cung cấp một bắt tay (thoả thuận ban đầu, còn gọi là thủ tục handshake) an toàn, trong đó các máy khách và máy chủ trao đổi một khối dữ liệu ngắn gọn các thông báo. Trong các thông báo này, máy khách và máy chủ thoả thuận mức an toàn được sử dụng để trao đổi các chứng chỉ số. Mỗi máy luôn luôn phải nhận dạng được máy kia. Các máy khách và máy chủ nên có chứng chỉ hợp lệ khi tiến hành kinh doanh. Sau khi nhận dạng, SSL mã hoá và giải mã luồng thông tin giữa hai máy. Điều này có nghĩa là thông tin trong yêu cầu HTTP và đáp ứng HTTP đều được mã hoá. Thông tin được mã hoá bao gồm URL (địa chỉ IP của trang Web) mà máy khách đang yêu cầu, các dạng bất kỳ chứa thông tin (do người sử dụng tạo ra), nó có thể bao gồm cả số thẻ tín dụng) và dữ liệu liên quan đến quyền truy nhập HTTP (chẳng hạn như tên người sử dụng và mật khẩu). Tóm lại, tất cả truyền thông (giữa các máy khách và các máy chủ sử dụng SSL) được mã hoá. Khi SSL mã hoá tất cả dòng thông tin giữa máy khách và máy chủ, đối tượng nghe trộm chỉ có thể nhận được các thông tin không thể hiểu được.

Do SSL nằm ở đỉnh tầng TCP/IP của giao thức Internet, SSL có thể đảm bảo các kiểu truyền thông khác nhau giữa các máy tính, bổ xung thêm cho HTTP. Ví dụ, SSL có thể đảm bảo các phiên FTP, cho phép đưa lên hoặc tải xuống một cách riêng lẻ các tài liệu nhạy cảm, các bảng tính và các dữ liệu điện tử khác. SSL có thể đảm bảo các phiên Telnet an toàn, trong đó người sử dụng máy tính từ xa có thể đăng nhập vào các máy host của công ty hoặc gửi đi mật khẩu và tên người sử dụng. Giao thức (thực hiện SSL) là một phiên bản an toàn của HTTP, được gọi là HTTPS. Bằng cách đặt tên giao thức HTTPS trước URL, bạn báo hiệu rằng bạn muốn thiết lập một kết nối an toàn với máy chủ từ xa. Ví dụ, nếu bạn gõ vào giao thức và URL như sau *http://www.amazon.com*, lập tức bạn thiết lập được một liên kết an toàn với Amazon.com.

SSL có hai độ dài là 40 bít và 128 bít. Chúng chỉ ra độ dài của khoá phiên riêng, được sinh ra cho mọi giao dịch có mã hoá. Thuật toán mã hoá sử dụng khoá phiên để tạo ra văn bản mã (từ văn bản rõ) trong một phiên giao dịch an toàn. Khoá dài hơn có khả năng chống lại tấn công hiệu quả hơn. Chính phủ Mỹ chỉ cho xuất khẩu khoá phiên 40 bit và cấm xuất khẩu khoá 128 bít. Khi phiên giao dịch kết thúc, các khoá phiên bị loại bỏ hoàn toàn, không tái sử dụng cho các phiên giao dịch tiếp theo.

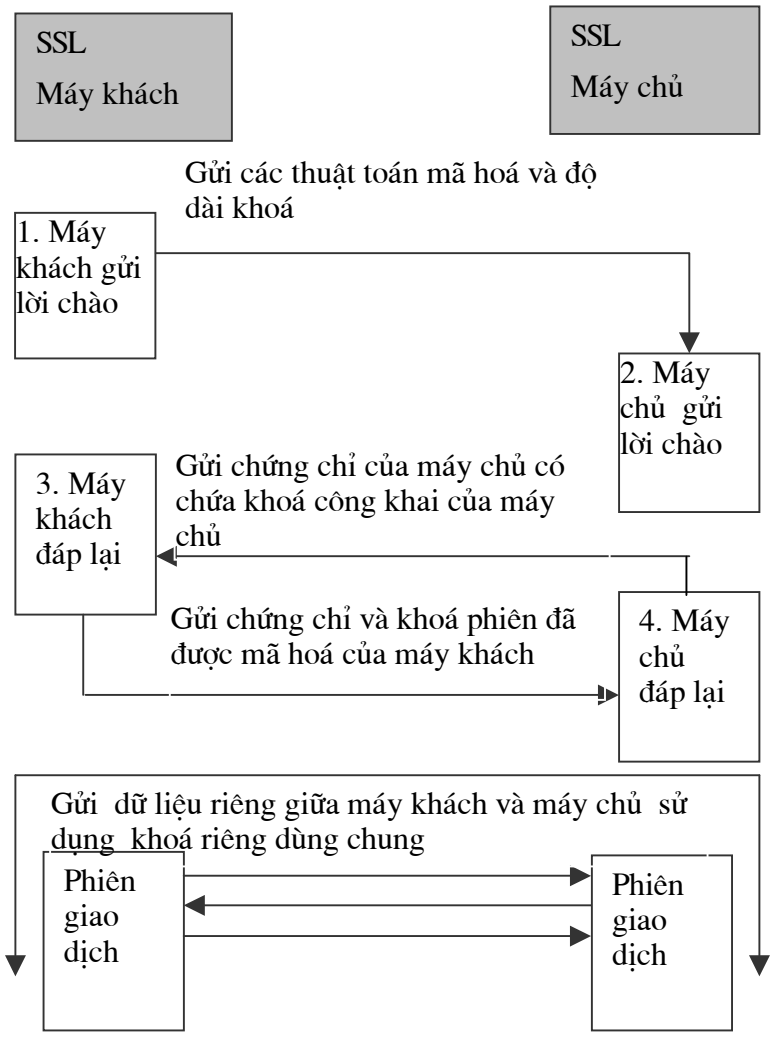
Sau đây, chúng ta có thể xem xét cách SSL làm việc (cuộc trao đổi giữa bên máy khách và máy chủ thương mại như thế nào: Nên nhớ rằng, SSL phải xác thực site thương mại (tối thiểu) và mã hoá mọi cuộc truyền giữa 2 máy tính. Khi trình duyệt của một máy khách đến một Web site bí mật của một máy chủ, máy chủ gửi một lời chào tới trình duyệt. Trình duyệt đáp lại bằng một lời chào. Việc tiến hành trao đổi lời chào, hoặc bắt tay cho phép 2 máy tính quyết định các chuẩn mã hoá và nén (mà chúng cùng hỗ trợ).

Tiếp theo, trình duyệt (bên máy khách) yêu cầu máy chủ đưa ra một chứng chỉ số, giống như việc yêu cầu nhận dạng ảnh: "Chứng minh cho tôi biết anh có phải là www.gateway.com hay không?". Đáp lại, máy chủ gửi cho trình duyệt một chứng chỉ. Một CA (được công nhận) đã ký chứng chỉ này. Trình duyệt kiểm tra chữ ký số có trên chứng

chỉ của máy chủ, dựa vào khoá công khai của CA, khoá này được lưu giữ trong trình duyệt. Hoạt động này xác thực máy chủ thương mại.

Máy khách và máy chủ thoả thuận rằng mọi trao đổi phải được giữ bí mật, bởi vì những thông tin được truyền đi trên Internet bao gồm số thẻ tín dụng, số hoá đơn và các mã kiểm tra. Để thực hiện bí mật, SSL sử dụng mã hoá khoá công khai (không đối xứng) và mã hoá khoá riêng (đối xứng). Mã hoá khoá công khai dễ sử dụng nhưng chậm hơn rất nhiều so với mã hoá khoá riêng. Đó chính là lý do tại sao SSL sử dụng mã hoá khoá riêng cho hầu hết các cuộc truyền thông an toàn của mình. Máy khách và máy chủ chia xẻ một khoá riêng cho nhau như thế nào để đối tượng nghe trộm không thể phát hiện được? Câu trả lời là trình duyệt sinh ra một khoá riêng dùng chung cho cả hai. Sau đó, trình duyệt mã hoá khoá riêng bằng khoá công khai của máy chủ. Khoá công khai của máy chủ được lưu giữ trong chứng chỉ số, máy chủ gửi chứng chỉ này cho trình duyệt trong quá trình xác thực. Một khi khoá được mã hoá, trình duyệt gửi nó cho máy chủ. Ngược lại, máy chủ giải mã thông báo bằng khoá riêng của nó và tìm ra khoá riêng dùng chung. Tất cả các thông báo giữa máy khách và máy chủ được mã hoá bằng khoá riêng dùng chung (cũng được biết đến như là một khoá phiên).

Sau khi kết thúc phiên giao dịch, khoá phiên bị huỷ bỏ. Một kết nối mới (giữa một máy khách và một máy chủ bí mật) lại bắt đầu tương tự. Tuỳ thuộc vào những gì đã thoả thuận, máy khách và máy chủ có thể sử dụng mã 40 bít hoặc 128 bit. Thuật toán mã hoá có thể là DES, hoặc RSA.



Hình 2.2 Thiết lập một phiên SSL

Máy khách và máy chủ có thể thoả thuận trước việc sử dụng kết hợp các thuật toán. Sau quá trình bắt tay, máy khách và máy chủ trao đổi khoá riêng với nhau và khoá này được sử dụng để mã hoá thông tin trong thời gian còn lại của phiên giao dịch an toàn, được minh hoạ trong hình 2.3.

Bạn có thể tìm hiểu chi tiết một SSL site, bằng cách truy cập vào site Web Server Survey của Netcraft. Để tìm hiểu các phần mềm và thuật toán mã hoá do một site thương mại hỗ trợ, bạn nhấn chuột vào " What's that SSL site running?"

Giao thức S-HTTP

S-HTTP là một mở rộng của HTTP, cung cấp một số đặc tính an toàn, trong đó có xác thực máy khách và máy chủ, mã hoá và chống chối bỏ yêu cầu/đáp ứng. Giao thức này được CommerceNet Consortium phát triển, hoạt động ở tầng ứng dụng. Nó cung cấp mã hoá đối

xứng để thiết lập xác thực máy khách/máy chủ và các tóm lược thông báo nhằm đảm bảo tính toàn vẹn dữ liệu. Máy khách và máy chủ có thể sử dụng các kỹ thuật S-HTTP một cách riêng lẻ. Điều này có nghĩa là trình duyệt của máy khách có thể yêu cầu an toàn bằng cách sử dụng một khoá riêng (khoá đối xứng), trong khi đó máy chủ có thể yêu cầu xác thực máy khách bằng cách sử dụng các kỹ thuật khoá công khai.

Các chi tiết về S-HTTP được máy khách và máy chủ thoả thuận trong phiên giao dịch đầu. Máy khách hoặc máy chủ có thể định rõ - một đặc tính an toàn riêng là *Required* (yêu cầu), *Optional* (tuỳ chọn) hoặc *Refused* (từ chối). Khi một thành viên quy định rằng đặc tính an toàn riêng là Required, nó sẽ chỉ tiếp tục kết nối nếu thành viên khác (máy khách hoặc máy chủ) đồng ý tuân theo đặc tính an toàn đã được định trước. Nếu không, sẽ không có kết nối an toàn nào được thiết lập.

Giả thiết, trình duyệt của máy khách định rõ yêu cầu mã hoá để đảm bảo an toàn tất cả các cuộc truyền thông. Điều này có nghĩa là các giao dịch yêu cầu đặt hàng tơ lụa của một nhà thiết kế trang phục chất lượng cao với hãng dệt Viễn Đông cần được duy trì bí mật. Những đối thủ cạnh tranh có thể nghe trộm nhưng không thể đoán biết được loại vải nào sẽ được sử dụng chủ đạo trong mùa tới. Hãng dệt muốn được đảm bảo rằng, người mua đúng là người anh ta nói, chứ không phải là đối tượng lừa đảo. Đồng thời yêu cầu chống chối bỏ để người mua không phủ nhận được việc anh ta đã đặt hàng. Trong thực tế, người ta sử dụng chữ ký số bí mật.

S-HTTP có cách thiết lập một phiên giao dịch an toàn khác với SSL. Trong khi SSL tiến hành bắt tay máy khách/máy chủ để thiết lập một cuộc truyền thông an toàn, S-HTTP thiết lập các chi tiết an toàn thông qua header (phần đầu trong gói tin) của gói đặc biệt. Header định nghĩa kiểu kỹ thuật an toàn, cụ thể là mã khoá riêng, xác thực máy chủ, xác thực máy khách và đảm bảo tính toàn vẹn thông báo. Header cũng quy định thuật toán nào được hỗ trợ, máy khách hay máy chủ (hoặc cả hai) hỗ trợ thuật toán đó, kỹ thuật an toàn nào được yêu cầu, đặc tính an toàn riêng là tuỳ chọn hay từ chối. Một khi máy khách và máy chủ thoả thuận được các thiết lập an toàn bắt buộc giữa chúng, tất cả các thông báo trong phiên giao dịch sau này được đóng gói an toàn trong một phong bì an toàn (secure envelope). Đây là một tiện ích an toàn đóng gói thông báo và đảm bảo tính bí mật, toàn vẹn và xác thực máy khách/máy chủ. Nhờ đó, mọi thông báo chuyển tiếp trên mạng hoặc Internet được mã hoá, không ai có thể đọc trộm. Mọi sửa đổi trên thông báo đều bị phát hiện, nhờ vào kỹ thuật toàn vẹn. Nó cung cấp một mã phát hiện thông báo bị sửa đổi. Người ta sử dụng các chứng chỉ số do một CA (được công nhận) phát hành để xác thực các máy khách và máy chủ. Phong bì an toàn bao gồm tất cả các đặc tính an toàn trên.

2.5 Đảm bảo tính toàn vẹn giao dịch

Tóm lại, cơ sở thương mại điện tử cần có:

- Trình duyệt của máy khách: gửi các thông tin thanh toán, đặt hàng và các chỉ dẫn thanh toán cho máy chủ thương mại.

- Máy chủ thương mại: đáp ứng thông tin từ phía máy khách, bằng cách gửi xác nhận điện tử đối với các chi tiết đặt hàng.

Nếu một đối tượng xâm nhập trên Internet có thể sửa đổi các thông tin đặt hàng trong quá trình chuyển tiếp (ví dụ anh ta có thể sửa đổi địa chỉ gửi hàng hay số lượng hàng), hậu quả của nó rất nghiêm trọng, khó lường trước. Đây là một ví dụ về tấn công toàn vẹn. Để ngăn chặn cần cho đối tượng xâm nhập nhận thấy rằng việc sửa đổi thông báo là rất khó và tốn kém. Hiện đã có các kỹ thuật an toàn cho phép người nhận phát hiện mọi sửa đổi trên thông báo.

Cần kết hợp các kỹ thuật để tạo ra thông báo có khả năng chống trộm cắp và xác thực. Để chống lại việc gian lận và lạm dụng khi thông báo bị sửa đổi, người ta áp dụng hai thuật toán riêng cho một thông báo. Các thuật toán băm là các hàm một chiều, có nghĩa là, không có cách nào để chuyển đổi từ giá trị băm ngược trở lại thông báo ban đầu. Điều này thực sự có lợi, bởi vì chúng ta có thể so sánh giá trị băm này với giá trị băm khác để tìm ra sự trùng khớp giữa chúng. MD5 là một ví dụ về thuật toán băm, nó được sử dụng rộng rãi trong thương mại điện tử an toàn. Một thuật toán băm có các đặc điểm như sau: nó sử dụng khoá không bí mật, tóm lược thông báo mà nó tạo ra không thể chuyển ngược lại thông tin ban đầu, thuật toán và các thông tin (về việc nó làm việc như thế nào) có hiệu lực công khai và các xung đột hầu như không xảy ra.

Một khi hàm băm tính toán được giá trị băm của một thông báo, giá trị này được gắn kèm vào thông báo. Giả thiết rằng, thông báo gửi đi là một đơn đặt hàng có chứa địa chỉ và thông tin thanh toán của khách hàng. Khi thương gia nhận được đơn đặt hàng và tóm lược thông báo đi kèm, anh ta tính toán tóm lược của thông báo nhận được, so sánh nó với tóm lược thông báo đi kèm và biết được thông báo có bị sửa đổi hay không.

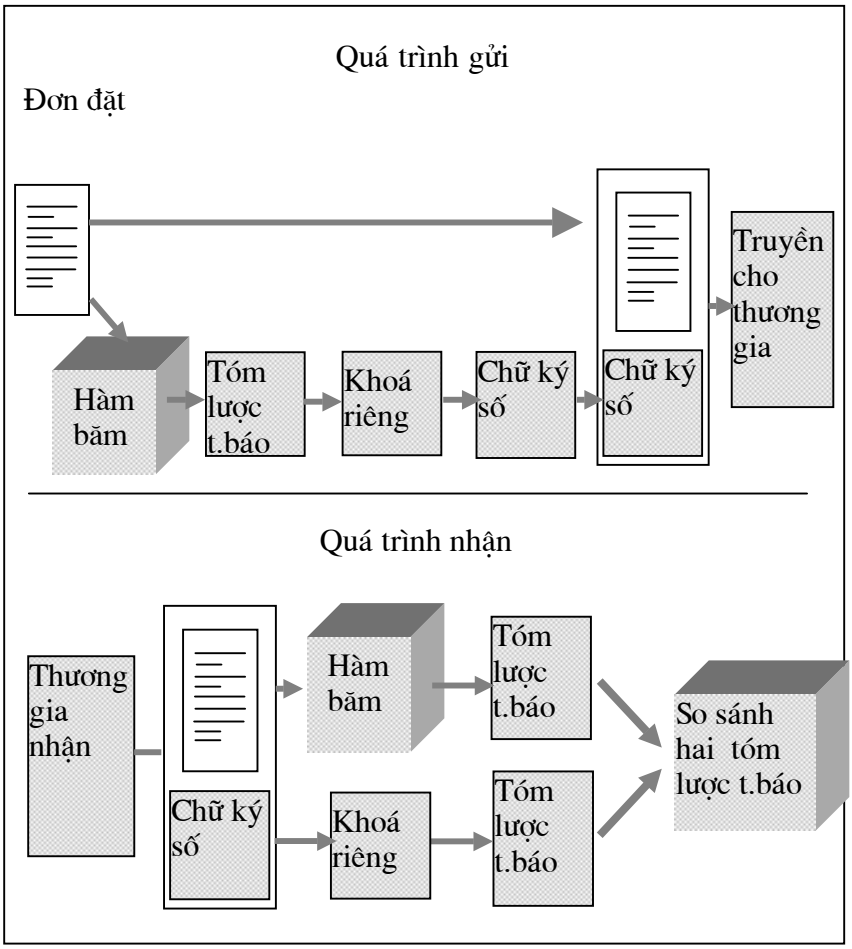
Tuy nhiên, ở đây cũng nảy sinh một vấn đề khác. Do thuật toán băm được biết rộng rãi và công khai, bất kỳ ai cũng có thể chặn lấy một đơn đặt hàng, sửa đổi địa chỉ gửi hàng và số lượng hàng yêu cầu, tạo ra một tóm lược mới, gửi thông báo (đã bị sửa đổi) cùng với tóm lược mới cho một thương gia. Thương gia tính toán tóm lược của thông báo nhận được, so sánh tóm lược này với tóm lược đính kèm và thấy chúng trùng khớp. Thương gia tin rằng thông báo nhận được chính là thông báo ban đầu. Để ngăn chặn kiểu gian lận này, người gửi mã hoá tóm lược thông báo bằng khoá riêng của mình.

Chữ ký số là tóm lược thông báo được mã hoá. Đơn đặt hàng có đi kèm chữ ký số cung cấp nhận dạng xác thực người gửi và đảm bảo thông báo không bị sửa đổi. Một chữ ký cung cấp tính toàn vẹn thông báo và xác thực máy khách như thế nào? Khi tóm lược thông báo được mã hoá nhờ dùng các kỹ thuật khoá công khai, có nghĩa là chỉ người chủ sở hữu của cặp khoá công khai/khoá riêng mới có thể mã hoá tóm lược thông báo. Vì vậy, khi thương gia giải chữ ký số bằng khoá công khai, tính toán tóm lược của thông báo nhận được, sự trùng khớp của các tóm lược thông báo là kết quả chứng minh tính đích thực của người gửi. Điều này giải quyết vấn đề làm giả (spoofing). Nếu cần, cả hai thành viên có thể thoả thuận giữ bí mật giao dịch, bổ xung thêm vào tính toàn vẹn và xác thực mà chữ ký số đã cung cấp.

Đơn giản chỉ cần mã hoá toàn bộ chuỗi (cả chữ ký số và thông báo) nhằm đảm bảo tính bí mật thông báo. Việc kết hợp sử dụng mã hoá khoá công khai, tóm lược thông báo và chữ ký số đảm bảo an toàn chất lượng cho các cuộc giao dịch trên Internet. Hình 2.4 minh hoạ một chữ ký số và một thông báo được tạo ra và gửi đi như thế nào.

Đảm bảo chuyển giao giao dịch

Tấn công chối bỏ hoặc làm trễ dịch vụ có thể loại bỏ hoặc sử dụng nhiều nguồn tài nguyên. Trong tấn công này, các chương trình Java có thể tải xuống với một trang Web và dần dần làm cho bộ xử lý của bạn không hoạt động được. Loại tấn công này cũng xảy ra trên các kênh thương mại, một mạng hoặc Internet. Một cách từ chối dịch vụ là làm tràn ngập Internet bằng một số lượng lớn các gói, nhằm phá hoại máy chủ hoặc giảm các mức an toàn của nó xuống mức khó có thể chấp nhận được đối với người muốn tiến hành kinh doanh. Một số tấn công là nguyên nhân phá hoại hệ điều hành. Các tấn công từ chối cũng có thể loại bỏ các gói Internet, làm cho chúng biến mất. Nếu điều này xảy ra thường xuyên đối với một site thương mại, những người mua hàng sẽ bắt đầu tránh xa site này.



Hình 2.7 Quá trình gửi và nhận một thông báo

Mã hoá hoặc các chữ ký số có thể bảo vệ các gói thông tin, tránh bị trộm cắp hoặc làm trễ. Tuy nhiên, TCP có trách nhiệm kiểm soát các gói tại các nút cuối. Tại đích, khi lắp ráp các gói theo đúng trật tự ban đầu, nó phát hiện được ngay các gói bị mất. Trách nhiệm lúc này của TCP là yêu cầu máy phía máy khách gửi lại dữ liệu. Điều này có nghĩa là không có giao thức an toàn máy tính đặc biệt nào (ngoại trừ TCP/IP) được sử dụng như là một biện pháp đối phó, chống lại các tấn công từ chối. Giao thức TCP/IP tiến hành kiểm tra dữ liệu, vì vậy nó có thể phát hiện các gói dữ liệu bị sửa đổi hoặc không hợp lệ.

2.6 Bảo vệ máy chủ thương mại

Các cách bảo đảm an toàn (được trình bày trong các mục trên) chủ yếu tập trung vào việc bảo vệ máy phía máy khách và các giao dịch thương mại trên Internet hoặc kênh thương mại. Trong phần này chúng ta đi sâu xem xét việc bảo vệ máy chủ thương mại, đây chính là trọng tâm của thương mại điện tử. Máy chủ thương mại, song song với máy chủ Web, đáp ứng các yêu cầu từ trình duyệt Web thông qua giao thức HTTP và CGI script. Phần mềm máy chủ thương mại bao gồm máy chủ FTP, máy chủ thư tín, máy chủ đăng nhập từ xa và hệ điều hành trên các máy host.

Kiểm soát truy nhập và xác thực

Kiểm soát truy nhập và xác thực nhằm kiểm soát ai và cái gì truy nhập vào máy chủ thương mại. Xác thực là kiểm tra nhận dạng của thực thể muốn truy nhập vào máy tính thông qua các chứng chỉ số. Khi máy chủ yêu cầu nhận dạng rõ ràng một máy khách và người sử dụng của nó, máy chủ yêu cầu máy khách gửi cho nó một chứng chỉ. Máy chủ có thể xác thực người sử dụng theo nhiều cách. Thứ nhất, nếu máy chủ không thể giải mã chữ ký số (có trong chứng chỉ) bằng cách sử dụng khoá công khai, điều này chứng tỏ rằng chứng chỉ không có nguồn gốc từ người sở hữu tin cậy. Thủ tục này ngăn chặn, không cho phép các chứng chỉ gian lận chui vào một máy chủ an toàn. Thứ hai, máy chủ kiểm tra tem thời gian (có trên chứng chỉ) để đảm bảo rằng chứng chỉ chưa quá hạn. Máy chủ sẽ loại bỏ các chứng chỉ đã hết hạn và không cung cấp thêm dịch vụ. Thứ ba, máy chủ có thể sử dụng một hệ thống gọi lại, trong đó địa chỉ máy khách và tên người sử dụng được kiểm tra, dựa vào danh sách tên người dùng và địa chỉ máy khách được gán trước.

Tên người sử dụng và mật khẩu là một yếu tố bảo vệ cho các máy chủ. Bạn sử dụng mật khẩu hàng ngày khi muốn truy nhập vào máy chủ lưu giữ hộp thư điện tử của bạn, truy nhập vào mạng của một trường đại học hoặc một công ty, đăng nhập vào các dịch vụ thuê bao, chẳng hạn như E*Trade, trên Internet. Để xác thực người dùng bằng sử dụng tên và mật khẩu, máy chủ phải lưu giữ một cơ sở dữ liệu (có chứa các thông tin liên quan đến người sử dụng hợp pháp, gồm tên người sử dụng và mật khẩu). Hệ thống cho phép người sử dụng bổ xung, xoá, thay đổi mật khẩu. Các hệ thống hiện đại nhất giúp người sử dụng nhớ lại mật khẩu trong trường hợp họ quên. Bạn có thể lấy lại một mật khẩu đã quên bằng cách gửi yêu cầu cho máy chủ thư tín.

Nhiều hệ thống máy chủ Web lưu giữ tên người sử dụng và mật khẩu trong một file. Không quan tâm đến việc thông tin đăng nhập được lưu giữ ở đâu, cách nhanh nhất và phổ biến nhất để lưu giữ các mật khẩu (một biện pháp được sử dụng trong các hệ thống UNIX) là lưu giữ tên người sử dụng ở dạng rõ và mã hoá mật khẩu. Khi bạn hoặc một hệ thống tạo ra một tên mới, mật khẩu được mã hoá nhờ thuật toán mã hoá một chiều. Do tên người sử dụng được lưu ở dạng rõ, hệ thống có thể phê chuẩn những người sử dụng khi họ đăng nhập, bằng cách kiểm tra tên của anh ta qua danh sách tên (được lưu giữ trong cơ sở dữ liệu). Sau đó mã hoá mật khẩu mà người sử dụng gõ vào khi đăng nhập hệ thống và so sánh nó với mật khẩu trong cơ sở dữ liệu (mật khẩu này được mã hoá, trước khi lưu vào cơ sở dữ liệu). Nếu trùng khớp, đăng nhập được chấp nhận.

Thông thường, máy chủ Web đưa ra danh sách kiểm soát truy nhập an toàn. ACL là một danh sách hoặc cơ sở dữ liệu, các nguồn tài nguyên, tên của người có thể truy nhập vào các file hoặc các nguồn tài nguyên khác. Mỗi file có một danh sách kiểm soát truy nhập riêng. Bất cứ khi nào, máy phía máy khách yêu cầu máy chủ Web truy nhập vào một file hoặc một tài liệu (có định trước cấu hình yêu cầu kiểm tra truy nhập), máy chủ Web sẽ kiểm tra ACL của nguồn tài nguyên và sẽ quyết định người sử dụng có được phép truy nhập hay không.

Các kiểm soát của hệ điều hành

Hầu hết các hệ điều hành (trừ các hệ điều hành chạy trên các máy tính nhỏ) sử dụng tên người dùng và mật khẩu cho hệ thống xác thực. Hệ thống này cung cấp một cơ sở hạ tầng an toàn cho máy chủ Web (chạy trên máy tính host). Hiện nay, hệ điều hành UNIX (và các biến thể của nó) là hệ điều hành nền chủ đạo cho các máy chủ Web. UNIX có một số cơ chế bảo vệ nhằm ngăn chặn khám phá trái phép và đảm bảo tính toàn vẹn dữ liệu.

Các bức tường lửa

Bức tường lửa được sử dụng như một hàng rào giữa một mạng (cần được bảo vệ) và Internet hoặc mạng khác (có khả năng gây ra mối đe doạ). Mạng và các máy tính cần được bảo vệ nằm bên trong bức tường lửa, các mạng khác nằm ở bên ngoài. Các bức tường lửa có các đặc điểm sau đây:

- Tất cả các luồng thông tin từ trong ra ngoài, từ ngoài vào trong đều phải chịu sự quản lý của nó.
- Chỉ có các luồng thông tin được phép (do chính sách an toàn cục bộ xác định) đi qua nó.
- Bức tường lửa tự bảo vệ mình.

Các mạng bên trong bức tường lửa được gọi là các mạng tin cậy, các mạng bên ngoài được gọi là các mạng không tin cậy. Đóng vai trò như một bộ lọc, bức tường lửa cho phép các thông báo (có chọn lọc) đi vào, hoặc ra khỏi các mạng được bảo vệ. Ví dụ, một chính sách an toàn cho phép tất cả các luồng thông tin HTTP (Web) vào ra, nhưng không cho

phép các yêu cầu FTP hoặc Telnet vào, hoặc ra khỏi các mạng được bảo vệ. Bức tường lửa ngăn chặn, không cho phép truy nhập trái phép vào các mạng bên trong bức tường lửa.

Các bức tường lửa hoạt động ở tầng ứng dụng. Chúng cũng có thể hoạt động ở tầng mạng và tầng vận tải. Các site của các công ty khác nhau phải có một bức tường lửa cho mỗi kết nối ngoài với Internet. Đảm bảo một phạm vi an toàn không thể phá vỡ. Ngoài ra, mỗi bức tường lửa trong công ty phải tuân theo chính sách an toàn.

Bức tường lửa nên loại ra các phần mềm không cần thiết. Giả sử rằng, một công ty nhỏ mua một máy tính chạy hệ điều hành UNIX, tất cả các phần mềm đi kèm với máy tính phải được kiểm tra và loại bỏ nếu chúng không phục vụ cho mục đích mà hệ điều hành hỗ trợ. Do các máy tính được sử dụng làm bức tường lửa, không phải là một máy tính toán phục vụ cho mục đích chung, nên chỉ có các phần mềm hệ điều hành cần thiết và phần mềm bảo vệ được duy trì trên máy.

Các bức tường lửa được chia thành 3 loại, bao gồm:

- *Packet filter firewall* (Loại lọc gói) để kiểm tra tất cả các luồng dữ liệu vào ra, giữa mạng tin cậy và Internet. Nó kiểm tra các địa chỉ nguồn và đích, các cổng, từ chối hoặc cho phép các gói vào khi thoả mãn tập các quy tắc được lập trình trước.

- *Gateway server firewall* được sử dụng để lọc các luồng thông tin, tuỳ thuộc vào ứng dụng mà chúng yêu cầu. Gateway server firewall hạn chế truy nhập vào các ứng dụng xác định, chẳng hạn như Telnet, FTP và HTTP. Khác với loại bức tường lửa đã trình bày ở trên, bức tường lửa mức ứng dụng lọc và ghi nhật ký tất cả các yêu cầu. Gateway server firewall cung cấp một điểm trung tâm, tất cả các yêu cầu được phân loại, ghi lại và phân tích tại điểm này.

- *Proxy server firewall* (Loại dùng máy uỷ quyền) thay mặt cho mạng riêng, truyền thông với Internet. Khi bạn định cấu hình cho một trình duyệt sử dụng uỷ quyền, bức tường lửa chuyển yêu cầu của trình duyệt lên Internet. Khi Internet gửi đáp ứng ngược trở lại, máy chủ uỷ quyền chuyển tiếp đáp ứng này cho trình duyệt. Các máy chủ uỷ quyền cũng được sử dụng như là một cache lớn (vùng nhớ tốc độ cao, được sử dụng để lưu giữ các trang Web).

2.7 Tóm tắt

Trong chương này, chúng ta đã trình bày một số giải pháp an toàn. Một số kỹ thuật có hiệu lực, hiện đang được phát triển nhằm bảo vệ sở hữu trí tuệ. 3 tài sản chung cần được bảo vệ là các máy khách, các kênh thương mại điện tử và các máy chủ thương mại. Cần đảm bảo tính bí mật, toàn vẹn và sẵn sàng cho liên kết *Khách hàng - Internet- Máy chủ thương mại*.

Mã hoá nhằm đảm bảo giữ bí mật, có hai loại mã hoá là mã hoá khoá công khai và mã hoá khoá riêng. Mã hoá khoá công khai giải quyết được vấn đề chia sẻ khoá bí mật, nhưng

thời gian xử lý của nó chậm hơn rất nhiều so với mã hoá khoá riêng. Mã hóa khoá riêng được sử dụng trong hầu hết các phiên thương mại, bởi nó nhanh và hiệu quả.

Các bảo vệ tính toàn vẹn đảm bảo rằng các giao dịch (các thông báo và các giao dịch thương mại) không bị sửa đổi. Các chứng chỉ số cung cấp kiểm soát toàn vẹn và xác thực người dùng. Một thành viên thứ ba tin cậy (CA) cung cấp các chứng chỉ số cho người sử dụng và các tổ chức. Một số giao thức Internet, bao gồm SSL, S-HTTP cung cấp khả năng truyền Internet an toàn. Cuối cùng là máy chủ thương mại, cũng giống với máy khách, nó phải được bảo vệ.

Việc bảo vệ máy chủ thương mại bao gồm kiểm soát truy nhập, xác thực, bằng cách sử dụng các thủ tục đăng nhập tên người dùng và mật khẩu, cùng với các chứng chỉ của máy khách.

Các bức tường lửa cung cấp một giải pháp phần cứng, cách biệt các mạng máy tính và máy khách bên trong bức tường lửa với các mạng không tin cậy bên ngoài.

Chương 3:

MỘT SỐ KỸ THUẬT AN TOÀN ÁP DỤNG CHO THƯƠNG MẠI ĐIỆN TỬ

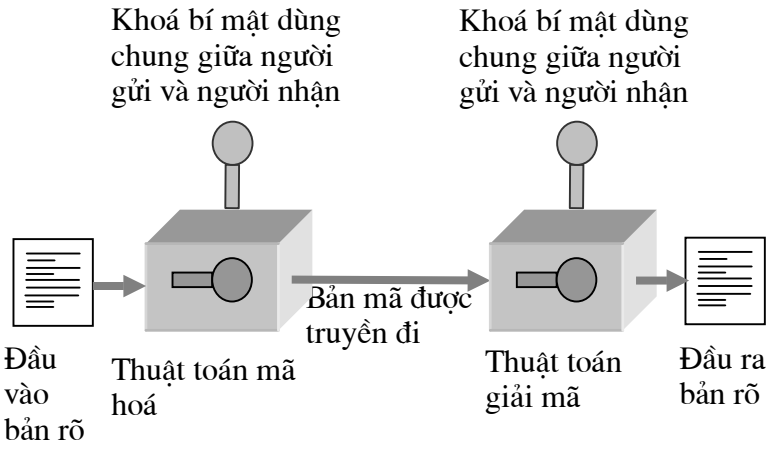
3.1 Mật mã đối xứng

Hình 3.1 minh hoạ quá trình mã hoá đối xứng. Bản rõ (dạng văn bản ban đầu có thể hiểu được) được chuyển thành bản mã (dạng văn bản vô nghĩa khó hiểu). Quá trình mã hoá gồm một thuật toán và một khoá. Khoá là một giá trị không phụ thuộc vào bản rõ. Đầu ra của thuật toán phụ thuộc vào khoá xác định (đây chính là khoá đang được sử dụng tại thời điểm này). Nếu chúng ta thay đổi khoá thì đầu ra của thuật toán cũng thay đổi theo.

Một khi bản mã được tạo ra, nó có thể được truyền đi. Tại nơi nhận, bản mã có thể được biến đổi trở lại dạng bản rõ ban đầu, nhờ một thuật toán giải mã và thuật toán này sử dụng cùng một khoá như đã được sử dụng trong khi mã hoá.

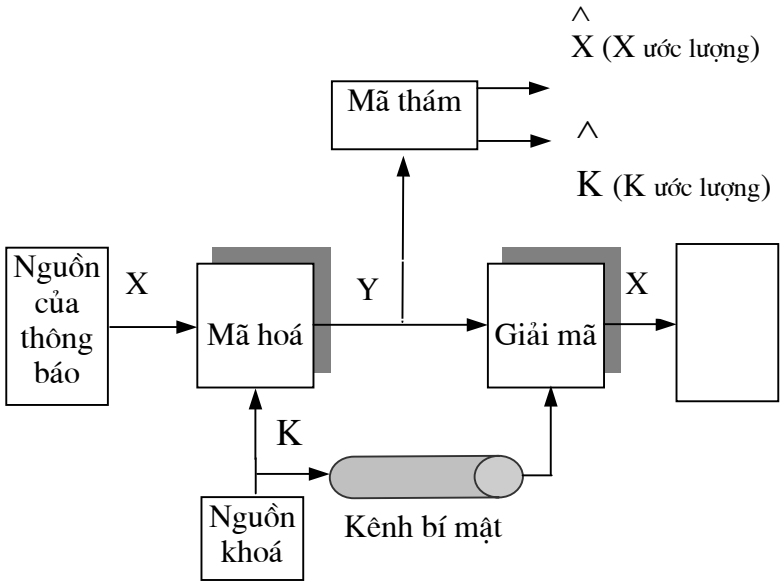
Độ an toàn của hệ mã này phụ thuộc vào một vài yếu tố. Trước hết, thuật toán mã hoá phải đủ mạnh, sao cho việc giải mã một thông báo mà chỉ dựa vào bản mã là không khả thi. Tiếp theo, độ an toàn của mã hoá đối xứng phụ thuộc vào sự bí mật của khoá, chứ không phải là sự bí mật của thuật toán. Có nghĩa là, việc giải mã một thông báo dựa vào bản mã và các thông tin về thuật toán mã hoá/giải mã là không khả thi. Nói cách khác, chúng ta không cần giữ bí mật thuật toán; Chúng ta cần giữ bí mật khoá.

Chính đặc tính này đã làm cho mã hoá đối xứng được sử dụng rộng rãi. Đó là vì các thuật toán không cần phải giữ bí mật, có nghĩa là các nhà sản xuất có thể sản xuất các chíp thuật toán mã giá thành thấp. Các chíp này có sẵn và dễ dàng ghép với một số sản phẩm khác. Khi sử dụng mã hoá đối xứng, vấn đề an toàn cần được quan tâm hàng đầu chính là sự bí mật của khoá.



Hình 3.1 Mô hình mã hoá đối xứng

Hãy quan sát kỹ các yếu tố cơ bản của lược đồ mã hoá đối xứng trong hình 3.2. Nguồn A tạo ra một thông báo ở dạng rõ, X= $\{X_1, X_2, ..., X_M\}$. M phần tử của X là các chữ cái trong một bảng chữ cái hữu hạn nào đó. Trước đây, bảng chữ cái thường bao gồm 26 chữ cái cơ bản. Hiện nay, bảng chữ cái nhị phân {0,1} thường được sử dụng. Khi mã hoá, một khoá có dạng K = $\{K_1, K_2,..., K_l\}$ được sinh ra. Nếu khoá do nguồn sinh ra, khoá phải được chuyển cho đích theo một kênh bí mật nào đó. Có thể dùng một thành viên thứ ba *a* sinh khoá và phân phối khoá một cách bí mật cho cả nguồn và đích.



Hình3.2 Mô hình hệ mật đối xứng

Với đầu vào là thông báo X và khoá mã K, đầu ra của thuật toán mã hoá là một bản mã Y= {Y_1, Y2,..., Y_N}. Chúng ta có thể viết như sau:

$Y= E_K(X)$

Khi người nhận hợp pháp nhận được bản mã, anh ta có thể giải mã bản mã nhờ dùng cùng một khoá (dùng trong khi mã hoá) như sau:

$X=D_K(Y)$

Khi có Y nhưng không có K hoặc X, đối phương không thể khôi phục lại X hoặc K, hoặc cả X và K. Giả thiết rằng, đối phương biết các thuật toán mã hoá (E) và giải mã (D). Nếu đối phương chỉ quan tâm đến một thông báo xác định nào đó, họ sẽ tập trung mọi nỗ lực vào việc khôi phục lại X bằng cách sinh ra một bản rõ X ước lượng. Tuy nhiên, nếu đối phương muốn đọc được các thông báo tiếp theo trong tương lai, đối phương cần khôi phục lại K bằng cách sinh ra một K ước lượng.

3.2 Mật mã khoá công khai

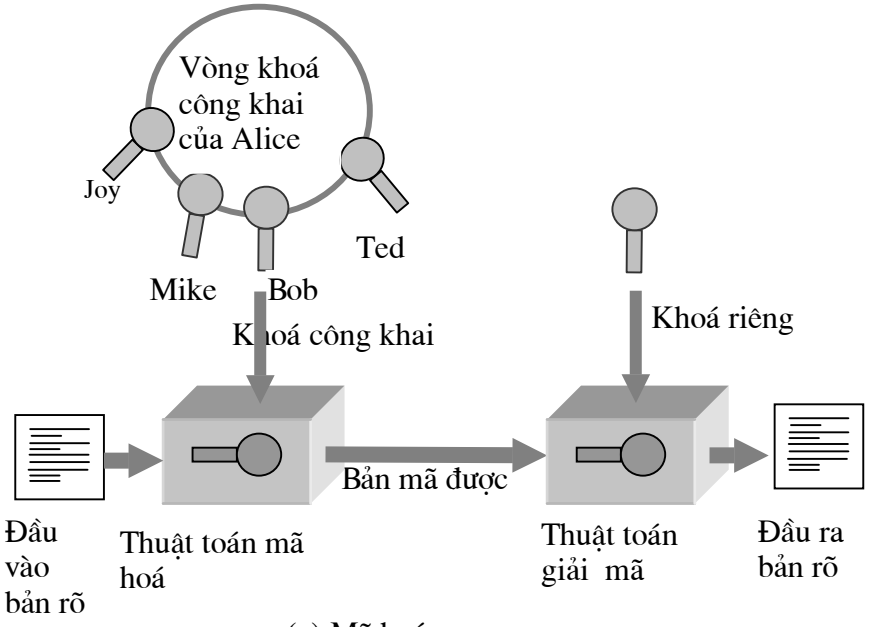
3.2.1 Các nguyên lý của các hệ thống mật mã khoá công khai

Khái niệm mật mã khoá công khai nảy sinh khi giải quyết hai vấn đề khó khăn trong mã đối xứng: phân phối khoá và chữ ký số. Vấn đề đầu tiên là phân phối khoá.

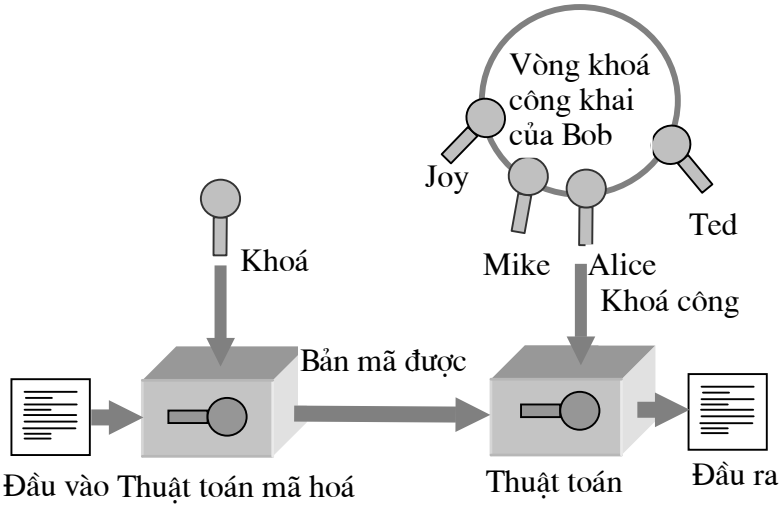
Như chúng ta đã biết, việc phân phối khoá trong mã hoá đối xứng yêu cầu hai bên liên lạc:

1. Dùng chung một khoá được phân phối theo cách nào đó; hoặc:
2. Sử dụng một trung tâm phân phối khoá.

Whitfield Diffie, một trong những người đã phát minh ra mã hoá khoá công khai (cùng với Martin Hellman, trường Đại học Stanford) đã suy luận và cho rằng, yêu cầu thứ hai phủ nhận bản chất của mật mã. Bản chất đó là đảm bảo tính bí mật trong liên lạc. Khó có thể tồn tại các hệ thống mật mã không thể phá được, nếu người sử dụng của các hệ thống này bắt buộc phải dùng chung các khoá của một trung tâm phân phối khoá (KDC), lý do là trung tâm này có thể để lộ khoá.



(a) Mã hoá



(b)Xác thực

Hình 3.3 Mã hoá khoá công khai

Vấn đề thứ hai mà Diffie đặt ra là "chữ ký số". Nếu việc sử dụng mật mã trở nên phổ biến, không chỉ trong lĩnh vực quân sự mà còn được sử dụng cho các mục đích thương mại và cá nhân, thì các thông báo và tài liệu điện tử cần có các chữ ký và chúng có hiệu lực tương tự như các chữ ký trên giấy tờ.

Các hệ thống mật mã khoá công khai

Các thuật toán khoá công khai sử dụng một khoá để mã hoá và một khoá khác để giải mã (tạo thành một cặp khoá). Chúng có tính chất quan trọng sau đây:

- Không thể xác định được khoá giải mã nếu chỉ căn cứ vào các thông tin về thuật toán và khoá mã hoá.

Một số thuật toán, chẳng hạn như RSA, cũng có tính chất sau:

- Một trong hai khoá được sử dụng để mã hoá, khoá còn lại được sử dụng để giải mã.

Hình 3.3 minh hoạ quá trình mã hoá khoá công khai. Các bước cơ bản gồm:

1. Mỗi hệ thống cuối trên một mạng sinh ra một cặp khóa, cặp khoá này được sử dụng để mã hoá và giải mã các thông báo mà nó nhận được.

2. Mỗi hệ thống công bố khóa mã hoá của mình bằng cách đặt khoá này vào trong một thanh ghi công khai hoặc một file. Đây chính là khoá công khai. Khoá cùng cặp được giữ bí mật.

3. Nếu A muốn gửi cho B một thông báo, nó mã hoá thông báo bằng khoá công khai của B.

4. Khi B nhận được thông báo, B giải mã thông báo bằng khoá riêng của B. Không một người nhận nào khác có thể giải mã thông báo, bởi vì chỉ có B mới biết khoá riêng của mình.

Với cách giải quyết này, tất cả các thành viên tham gia truyền thông có thể truy nhập vào các khoá công khai. Khoá riêng do mỗi thành viên sinh ra không bao giờ được phân phối. Quá trình liên lạc chỉ an toàn chừng nào hệ thống còn kiểm soát được khoá riêng của mình. Một hệ thống có thể thay đổi các khoá riêng của nó bất cứ lúc nào, đồng thời công bố các khoá công khai cùng cặp để thay thế khoá công khai cũ.

Bảng 3.1 trình bày một số điểm quan trọng của mã hoá khoá công khai và mật mã truyền thống (mã đối xứng). Để phân biệt chúng, người ta gọi khoá (được sử dụng trong mã đối xứng) là khoá bí mật. Hai khoá (dùng trong mã hoá khoá công khai) là khoá công khai và khoá riêng.

Chúng ta xem xét chi tiết các yếu tố cần thiết trong lược đồ mã hoá khoá công khai (hình 3.4).

Nguồn A đưa ra một thông báo và bản rõ của thông báo là X=[X1, X2,...,X_M] . Các phần tử M của X là các chữ cái trong bảng chữ cái. A dự định gửi thông báo cho đích B. B sinh ra một cặp khoá là khoá công khai KU_b, khoá riêng KR_b. Chỉ có B biết KR_b, còn KU_b được công bố công khai, do vậy A có thể có được khoá công khai này.

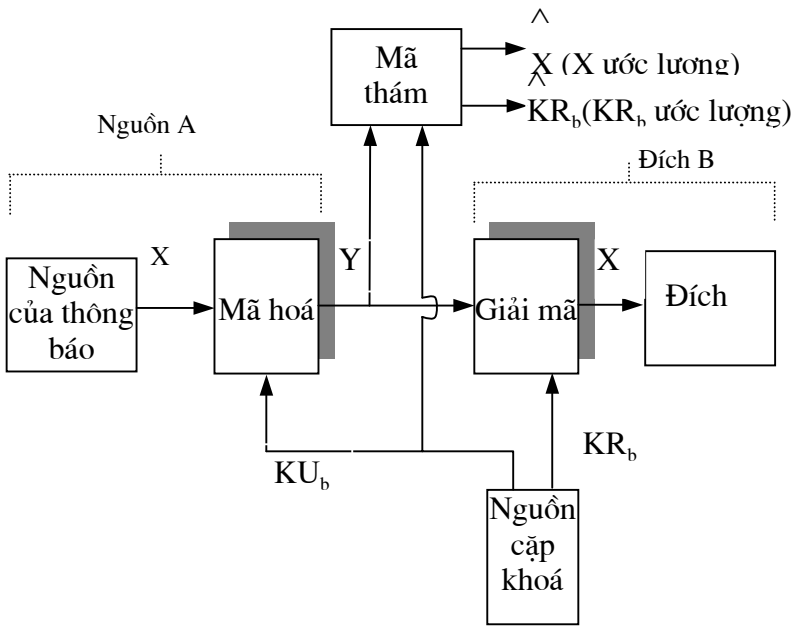
Với đầu vào là thông báo X và khoá mã hoá KU_b, A tạo ra một bản mã Y =[Y_1, Y_2, ..., Y_N] với $Y=E_{KUb}(X)$.

Người nhận hợp lệ (người sở hữu khoá riêng) thu được X, qua phép biến đổi ngược $X=D_{KRb}(Y)$.

Đối phương (có thể có được Y và KU_b nhưng không có KR_b hoặc X) phải tìm cách khôi phục lại X và/hoặc KR_b. Giả sử rằng, anh ta có các thông tin về thuật toán mã hoá (E) và giải mã (D), có thể khôi phục thông báo X, bằng cách sinh ra một bản rõ X ước lượng. Tuy nhiên, để đọc được các thông báo mới, đối phương phải khôi phục được KR_b bằng cách sinh ra một KR_b ước lượng.

Mã đối xứng	Mã khoá công khai
Các yêu cầu khi sử dụng	*Các yêu cầu khi sử dụng*
Quá trình mã hoá và giải mã sử dụng cùng một thuật toán với cùng một khoá. Người gửi và người nhận phải sử dụng chung thuật toán và khoá.	Một thuật toán sử dụng một cặp khoá khi mã hoá và giải mã, một khoá được sử dụng khi mã hóa, khoá còn lại được sử dụng khi giải mã. Người gửi và người nhận, mỗi người có một khoá trong cặp khoá.
Các yêu cầu an toàn	*Các yêu cầu an toàn*
Khóa phải được giữ bí mật Không thể giải mã được thông báo nếu không có các thông tin có giá trị khác. Các thông tin về thuật toán, các mẫu bản mã không đủ để xác định khoá.	Một trong hai khóa phải được giữ bí mật. Không thể giải mã được thông báo nếu không có các thông tin có giá trị khác. Các thông tin về thuật toán, một trong các khoá và các mẫu bản mã không đủ để xác định khoá còn lại.

Bảng 3.1 Mã hoá khoá công khai và đối xứng



Hình 3.4 Hệ mật khoá công khai: Bí mật

Chúng ta đã biết, một trong hai khoá trong cặp khoá có thể được sử dụng để mã hoá, khoá còn lại được sử dụng để giải mã. Điều này cho phép thực hiện một lược đồ mật mã hơi khác một chút. Lược đồ được minh hoạ trong hình 3.4 cung cấp tính bí mật. Hình 3.3b và 3.5 minh hoạ việc sử dụng mã hoá khoá công khai cho xác thực:

$Y= E_{KRa}(X)$

$X=D_{KUa}(Y)$

Trong trường hợp này, A chuẩn bị một thông báo để gửi cho B và mã hoá thông báo bằng khoá riêng của A trước khi truyền đi. B có thể giải mã thông báo bằng khoá công khai của A.Thông báo được mã hoá bằng khoá riêng của A, nên có thể xác định chỉ có A là người tạo ra thông báo. Do vậy, toàn bộ thông báo mã hoá được sử dụng như một chữ ký số. Hơn nữa, không thể sửa đổi thông báo nếu không có khoá riêng của A, chính vì vậy thông báo được xác thực cả nguồn gốc lẫn tính toàn vẹn dữ liệu.

Trong lược đồ trước, toàn bộ thông báo được mã hoá, nó đòi hỏi khả năng lưu giữ lớn. Mỗi tài liệu phải được lưu giữ ở dạng rõ. Bản sao được lưu giữ ở dạng mã, nên chúng ta có thể kiểm tra được nguồn gốc và các nội dung trong trường hợp tranh chấp. Một cách hiệu quả hơn để có được các kết quả như trên là mã hoá một khối nhỏ các bit. Khối này được gọi là dấu xác thực. Nó phải có tính chất là mọi thay đổi trên tài liệu dẫn đến sự thay đổi của dấu xác thực. Nếu dấu xác thực được mã hoá bằng khoá riêng của người gửi, nó được sử dụng như một chữ ký. Chữ ký được sử dụng để kiểm tra nguồn gốc, nội dung và trình tự.

Việc sử dụng lược đồ khoá công khai có thể đảm bảo tính xác thực và bí mật (hình 3.6):

$Z=E_{KUb}[E_{KRa}(X)]$

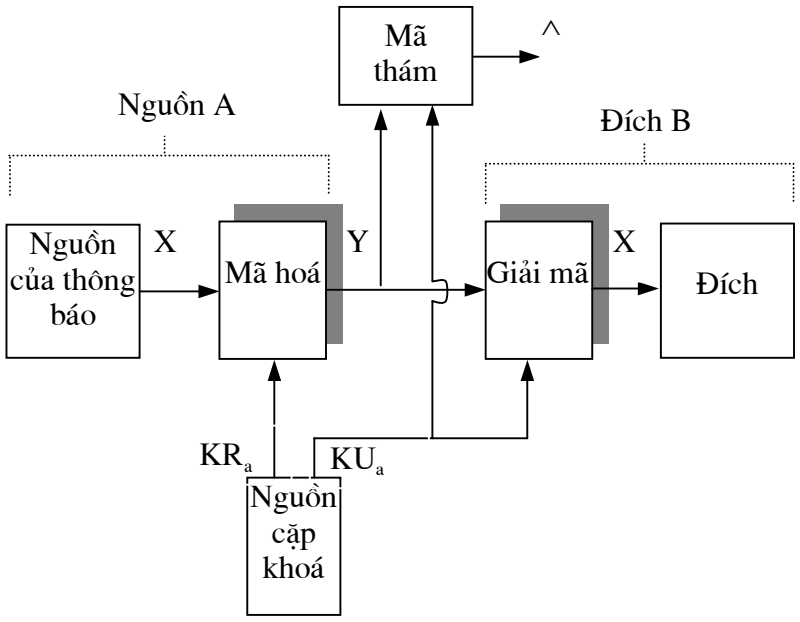
$X=D_{KUa}[D_{KRb}(Z)]$

Trước hết, chúng ta mã hoá một thông báo bằng khoá riêng của người gửi, đưa ra một chữ ký số. Tiếp theo, mã hoá một lần nữa bằng khoá công khai của người nhận. Chỉ có người nhận hợp pháp mới giải mã được bản mã cuối cùng này vì anh ta có khoá riêng cùng cặp. Như vậy sẽ đảm bảo được tính bí mật. Khó khăn của biện pháp này là thuật toán khoá công khai, nó thực sự phức tạp, phải tiến hành 4 lần (chứ không phải là 2 lần) cho mỗi cuộc truyền thông .

Các ứng dụng hệ thống khoá công khai

Trước tiên, chúng ta cần làm rõ một khía cạnh của các hệ thống mật mã khoá công khai. Việc sử dụng một kiểu thuật toán mật mã với 2 khoá (một khoá riêng, một khoá công khai) là đặc trưng của các hệ thống khoá công khai.

Tuỳ thuộc vào ứng dụng, người gửi sử dụng khoá riêng của người gửi hoặc khoá công khai của người nhận, hoặc cả hai.



Hình 3.5 Hệ mật khoá công khai: Xác thực

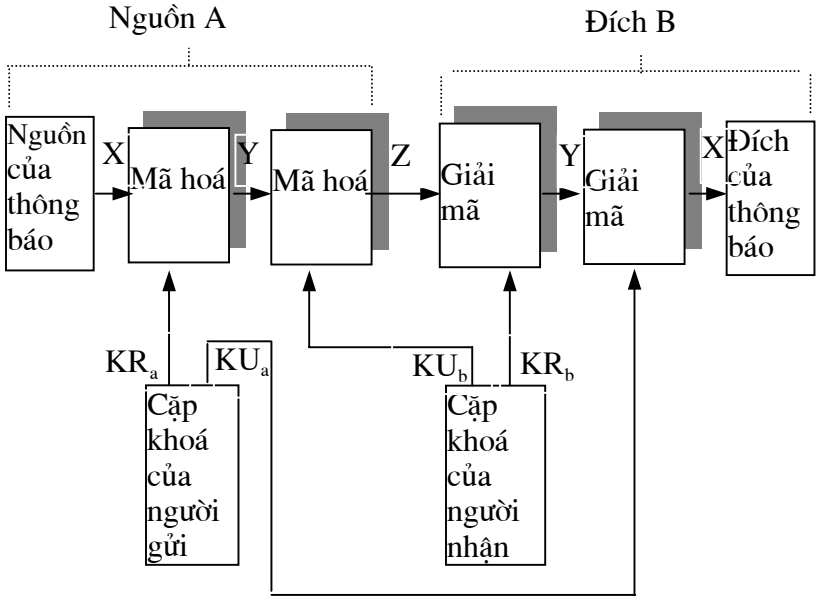
Nói rộng hơn, chúng ta có thể phân loại việc sử dụng các hệ thống mật mã khoá công khai thành 3 loại:

Mã hoá/ giải mã: Người gửi mã hoá một thông báo bằng khoá công khai của người nhận.

Chữ ký số: Người gửi "ký" thông báo bằng khoá riêng của mình. Quá trình ký được thực hiện nhờ dùng một thuật toán mật mã đối với thông báo hoặc một khối dữ liệu nhỏ.

Trao đổi khoá: Hai thành viên trao đổi một khoá phiên. Có một vài hướng giải quyết khác nhau, cần đến một (hoặc nhiều) khoá riêng của một hoặc hai thành viên.

Một số thuật toán phù hợp cho tất cả các ứng dụng, còn một số thuật toán khác chỉ được sử dụng cho một hoặc hai ứng dụng của chúng.



Hình 3.6 Hệ mật khoá công khai: Bí mật và xác thực

Thuật toán	Mã hoá/Giải mã	Chữ ký số	Trao đổi khoá
RSA	Có	Có	Có
Diffie-Hellman	Không	Không	Có
DSS	Không	Có	Không

Bảng 3.2 Các ứng dụng được các thuật toán hỗ trợ

Các yêu cầu đối với mật mã khoá công khai

Các ứng dụng hệ mật được minh hoạ trong hình 3.4, 3.6 phụ thuộc vào một thuật toán mật mã với hai khoá cùng cặp. Diffie và Hellman đưa ra các điều kiện mà các thuật toán trên phải đáp ứng như sau:

1. Thành viên B có thể dễ dàng sinh ra được một cặp khoá (khoá công khai KU_b và khoá riêng KR_b).

2. Người gửi A dễ dàng biết được khoá công khai, mã hoá thông báo M và tạo ra một bản mã tương ứng:

$$C=E_{KUb}(M)$$

3. Người nhận B dễ dàng giải mã được bản mã bằng cách sử dụng khoá riêng, khôi phục lại thông báo ban đầu.

$$M=D_{KRb}(C) =D_{KRb}[E_{KUb}(M)]$$

4. Đối phương khó có thể xác định được khoá riêng KR_b, mặc dù biết khoá công khai KU_b.

5. Đối phương khó có thể khôi phục lại thông báo M ban đầu dù biết khoá công khai KU_b và bản mã C.

Chúng ta có thể bổ xung thêm yêu cầu thứ 6. Mặc dù nó hữu ích nhưng nó không cần thiết cho tất cả các ứng dụng khoá công khai .

6. Các hàm mã hóa và giải mã có thể được áp dụng như sau:

$$M=E_{KUb}[D_{KRb}(M)]$$

Ở đây có một vài yêu cầu khắt khe (đã kiểm nghiệm trong thực tế). Ví dụ, các yêu cầu cần đáp ứng hàm cửa sập một chiều. Hàm một chiều là một hàm đơn trị hai chiều, rất dễ dàng tính toán hàm nhưng tính toán hàm nghịch đảo rất khó.

$Y=f(X)$ dễ dàng

$X=f^{-1}(Y)$ không thể

Chúng ta tiếp tục với định nghĩa hàm cửa sập một chiều, nó dễ dàng tính toán theo một chiều, khó có thể tính toán theo chiều kia trừ khi biết thêm thông tin nào đó. Với thông tin này, có thể tính toán được hàm nghịch đảo trong thời gian đa thức. Tóm lại, hàm cửa sập một chiều là họ các hàm nghịch đảo f_k, sao cho:

$Y=f_k(X)$ dễ dàng, nếu biết k và X

$X=f^{-1}_k(Y)$ dễ dàng, nếu biết k và Y

$X=f^{-1}_k(Y)$ khó có thể, nếu biết Y nhưng không biết k

Do vậy, việc phát triển một lược đồ khoá công khai thiết thực phụ thuộc vào việc tìm ra một hàm cửa sập một chiều phù hợp.

3.2.2 Quản lý khoá

Một trong các vai trò chính của mã hoá khoá công khai là giải quyết vấn đề phân phối khoá. Khi sử dụng mã hoá khoá công khai, chúng ta cần phân biệt hai khái niệm sau:

- Phân phối các khoá công khai.
- Sử dụng mã hoá khoá công khai để phân phối các khoá bí mật.

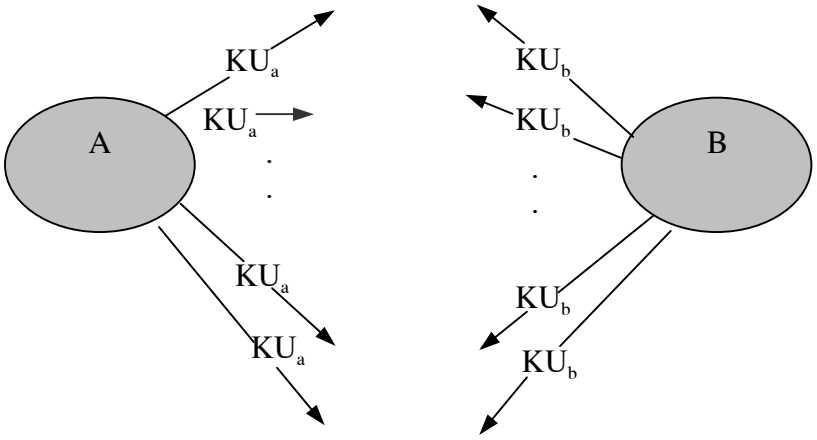
Chúng ta sẽ xem xét từng khái niệm sau đây.

Phân phối các khoá công khai

Người ta đã đề xuất một số kỹ thuật phân phối khoá công khai. Các đề xuất này có thể được nhóm lại như sau:

- Khai báo công khai
- Thư mục công khai
- Cơ quan quản lý khoá công khai
- Các chứng chỉ khoá công khai

Khai báo công khai các khoá công khai



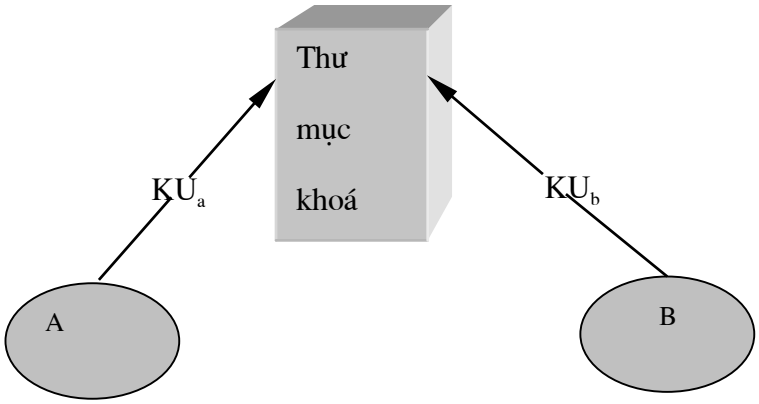
Hình 3.7 Phân phối khoá công khai không kiểm soát

Xuất phát điểm của mật mã khoá công khai là khoá công khai được công bố công khai. Do vậy, nếu có một thuật toán được chấp nhận rộng rãi, chẳng hạn như RSA, bất kỳ thành viên nào cũng có thể gửi khoá công khai của mình cho thành viên khác hoặc quảng bá cho cộng đồng lớn (Hình 3.7).

Ví dụ, những người sử dụng PGP chấp nhận gắn kèm khoá công khai của họ vào các thông báo gửi đến các nơi công cộng, chẳng hạn như các nhóm tin của USERNET, các danh sách thư tín trên Internet.

Mặc dù giải pháp này khá thích hợp, nhưng nó có nhược điểm là bất kỳ ai cũng có thể giả mạo một khoá công khai. Có nghĩa là, một người sử dụng nào đó có thể giả danh là người sử dụng A và gửi một khoá công khai cho thành viên khác. Khoảng thời gian cho đến khi người sử dụng A phát hiện ra sự gian lận và thông báo cho các thành viên khác, đối

tượng giả mạo có thể đã đọc toàn bộ các thông báo mã hoá gửi cho A và có thể sử dụng các khoá giả cho xác thực.



Hình 3.8 Công bố khoá công khai

Thư mục công khai

Chúng ta có thể có được độ an toàn cao, bằng cách duy trì một thư mục công khai. Việc duy trì và phân phối thư mục công khai thuộc trách nhiệm của một tổ chức tin cậy nào đó (hình 3.8).

Một lược đồ như vậy gồm các yếu tố sau:

Cơ quan quản lý duy trì một thư mục, mỗi thành viên có một đầu vào entry {tên, khoá công khai}.

Mỗi thành viên đăng ký một khoá công khai với cơ quan quản lý thư mục. Việc đăng ký này có thể được thực hiện bởi một cá nhân hoặc qua hình thức liên lạc có xác thực an toàn nào đó.

Một thành viên có thể thay thế một khoá mới bất kỳ lúc nào, chẳng hạn khi họ muốn thay thế một khoá công khai đã được sử dụng nhiều, hoặc khi khoá riêng cùng cặp bị lộ.

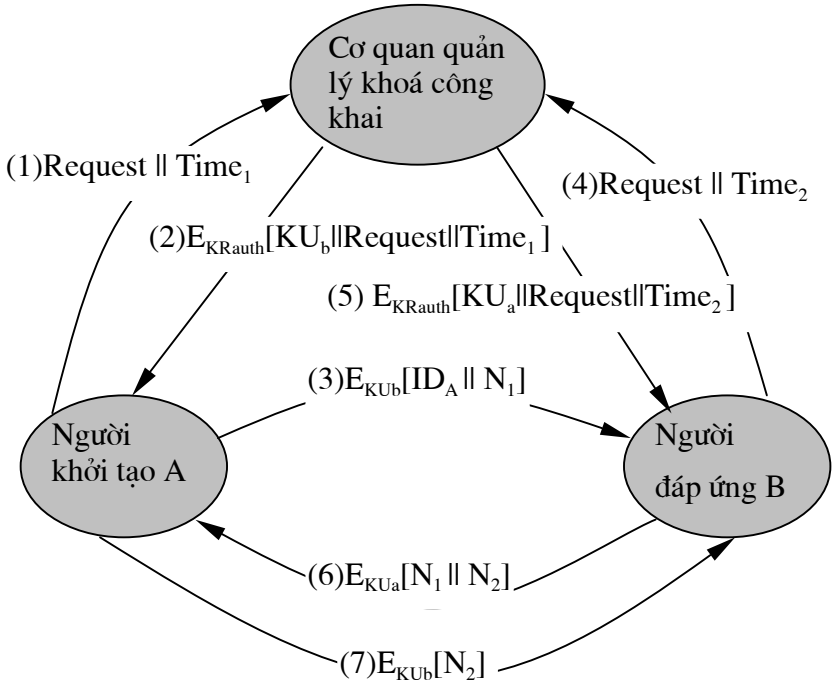
Cơ quan quản lý công bố toàn bộ thư mục hoặc cập nhật thư mục một cách định kỳ.

Các thành viên cũng có thể truy nhập vào thư mục. Chính vì vậy, việc truyền thông xác thực an toàn (từ cơ quan quản lý đến thành viên) phải mang tính bắt buộc.

Cơ quan quản lý khoá công khai

Việc phân phối khoá công khai được đảm bảo an toàn cao hơn nếu cung cấp các kiểm soát chặt chẽ khi phân phối khoá công khai từ thư mục (được minh hoạ trong hình 3.9).

Một cơ quan trung tâm duy trì một thư mục khoá công khai động cho tất cả các thành viên. Mỗi thành viên biết một khoá công khai nhưng chỉ có cơ quan này biết khoá riêng cùng cặp.



Hình 3.9 Lược đồ phân phối khoá công khai

Các bước tiếp theo như sau:

A gửi một thông báo có gán nhãn thời gian cho cơ quan quản lý khoá công khai, yêu cầu khoá công khai hiện thời của B.

Cơ quan quản lý trả lời bằng một thông báo. Thông báo này được mã hoá bằng khoá riêng của cơ quan quản lý, KR_{auth}. Như vậy, A có khả năng giải mã thông báo bằng cách sử dụng khoá công khai của cơ quan quản lý, A được đảm bảo rằng thông báo có nguồn gốc từ cơ quan quản lý. Thông báo gồm có:

Khoá công khai của B là KU_b - A có thể sử dụng nó để mã hoá các thông báo gửi cho B.

Yêu cầu gốc - A so khớp yêu cầu này với yêu cầu A đã gửi đi trước đó, nhờ đó A có thể biết yêu cầu gốc có bị sửa đổi trước khi cơ quan quản lý nhận được hay không.

Nhãn thời gian gốc - cho phép A xác định: đây không phải là một thông báo cũ mà là thông báo có chứa khoá công khai hiện thời của B.

A lưu giữ khoá công khai của B và sử dụng nó để mã hoá một thông báo gửi cho B, thông báo này có chứa tên của A (ID_A) và một nonce (N_1) được sử dụng để nhận dạng giao dịch này.

B lấy khoá công khai của A từ cơ quan quản lý (tương tự như A lấy khoá công khai của B).

Đến lúc này, các khoá công khai được chuyển giao an toàn cho A và B, họ có thể trao đổi với nhau. Tuy nhiên, 2 bước sau được bổ xung thêm (tuỳ chọn):

B gửi một thông báo cho A, thông báo này được mã hoá bằng KU_a và có chứa N_1 của A và một nonce mới (N_2) do B sinh ra. Do chỉ có B mới có thể giải mã thông báo (3) và sự có mặt của N_1 trong thông báo (6) đảm bảo với A rằng B chính là người A đang liên lạc.

A trả lại N_2 được mã hoá bằng khoá công khai của B, đảm bảo với B rằng A chính là người B đang liên lạc.

Các chứng chỉ khoá công khai

Lược đồ trong hình 3.9 rất hấp dẫn nhưng nó cũng có một số nhược điểm. Cơ quan quản lý khoá công khai gần giống như một cổ chai trong hệ thống. Người sử dụng phải yêu cầu cơ quan quản lý cấp khoá công khai cho người sử dụng khác khi họ muốn liên lạc. Như đã trình bày từ trước, cơ quan quản lý duy trì thư mục (mỗi đầu vào bao gồm tên và khoá công khai) - đây cũng là chính là điểm yếu dễ bị giả mạo.

Một giải pháp lựa chọn là sử dụng chứng chỉ. Các thành viên sử dụng chứng chỉ này để trao đổi khoá mà không cần liên lạc với cơ quan quản lý khoá công khai. Mỗi chứng chỉ chứa một khoá công khai và các thông tin khác. Nó được một cơ quan quản lý chứng chỉ tạo ra và phát hành cho các thành viên. Một thành viên chuyển thông tin khoá của mình cho thành viên khác thông qua các chứng chỉ. Các thành viên khác có thể kiểm tra chứng chỉ do cơ quan quản lý tạo ra.

Chúng ta có thể đưa vào lược đồ này các yêu cầu như sau:

Một thành viên có thể đọc chứng chỉ để xác định tên và khoá công khai của người sở hữu chứng chỉ.

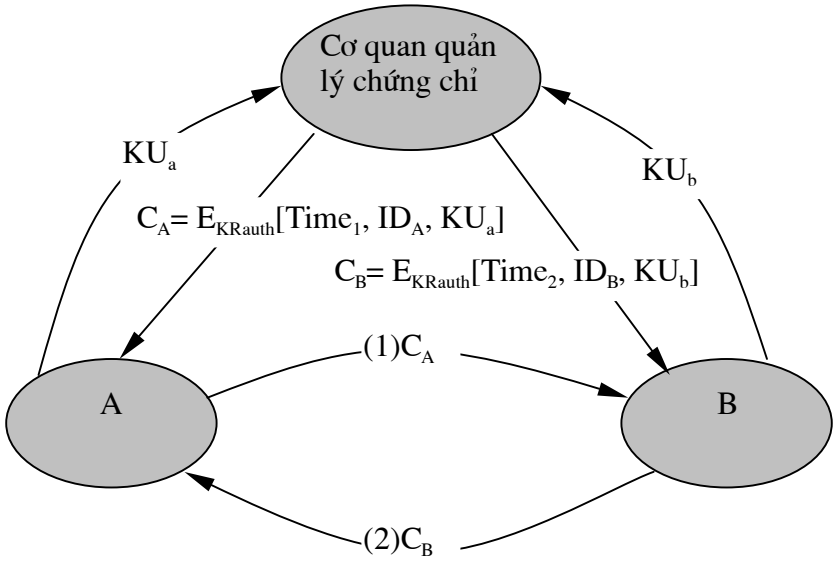
Mọi thành viên có thể kiểm tra: chứng chỉ có nguồn gốc từ cơ quan quản lý chứng chỉ và nó không bị giả mạo.

Chỉ có cơ quan quản lý chứng chỉ mới có thể tạo ra và cập nhật các chứng chỉ.

Và một yêu cầu được bổ xung thêm như sau:

Mọi thành viên có thể kiểm tra sự lưu hành của chứng chỉ.

Hình 3.10 minh hoạ một lược đồ chứng chỉ.Trong đó, mỗi thành viên yêu cầu cơ quan quản lý chứng chỉ cung cấp một khoá công khai và một chứng chỉ. Đối với thành viên A, cơ quan quản lý cung cấp cho A một chứng chỉ như sau:



Hình 3.10 Trao đổi các chứng chỉ khoá công khai

$C_A = E_{KRauth}[T, ID_A, KU_a]$

KR_{auth} là khoá riêng được cơ quan quản lý sử dụng. Sau đó, A có thể chuyển chứng chỉ này cho thành viên khác, thành viên này đọc và kiểm tra chứng chỉ như sau:

$D_{KUauth}[C_A] = D_{KUauth}[E_{KRauth}[T, ID_A, KU_a]] = (T, ID_A, KU_a)$

Người nhận sử dụng khoá công khai của cơ quan quản lý (KU_{auth}) để giải mã chứng chỉ. Do chỉ có thể đọc chứng chỉ bằng cách sử dụng khoá công khai của cơ quan quản lý nên việc kiểm tra này chứng tỏ rằng: chứng chỉ có nguồn gốc từ cơ quan quản lý chứng chỉ.

ID_A và KU_a cung cấp cho người nhận tên và khoá công khai của người nắm giữ chứng chỉ.

Nhãn thời gian T phê chuẩn sự lưu hành của chứng chỉ. Nó được sử dụng để đối phó khi khoá riêng của A bị lộ. A sinh ra một cặp khoá mới và yêu cầu cơ quan quản lý chứng chỉ cấp một chứng chỉ mới. Trong lúc đó, đối phương vẫn sử dụng chứng chỉ cũ với B. Sau đó, nếu B mã hoá các thông báo bằng khoá công khai cũ, đối phương có thể đọc toàn bộ các thông báo này.

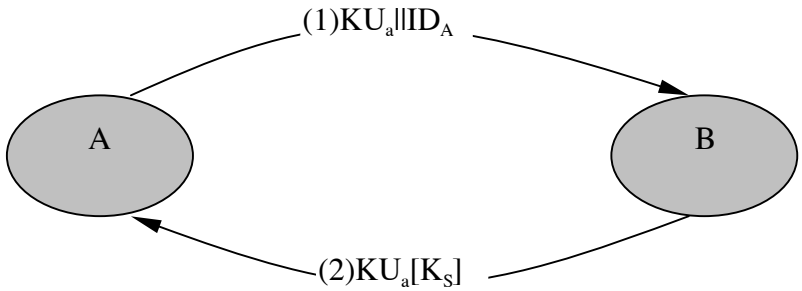
Việc làm lộ khoá riêng được so sánh với việc mất một thẻ tín dụng. Người chủ sở hữu huỷ bỏ số thẻ tín dụng, nhưng vẫn có thể xảy ra rủi ro cho đến khi tất cả những người liên lạc nhận thức được - thẻ tín dụng cũ không được sử dụng nữa. Nhãn thời gian chỉ ra thời hạn kết thúc.

Sử dụng mã hoá khoá công khai để phân phối khoá bí mật

Một khi các khoá công khai được phân phối hoặc có thể truy nhập vào chúng, liên lạc an toàn có thể ngăn chặn nghe trộm, giả mạo. Tuy nhiên, một số người không muốn sử dụng mã khoá công khai do thời gian mã/giải mã lớn. Mã khoá công khai được sử dụng để phân phối khoá bí mật cho mã hoá đối xứng.

Phân phối khoá bí mật đơn giản

Merkle đưa ra một lược đồ rất đơn giản (được minh hoạ trong hình 3.11.



Hình 3.11 Sử dụng mã khoá công khai để thiết lập một khoá phiên

Nếu A muốn truyền thông với B, thủ tục được thực hiện như sau:

A tạo ra một cặp khoá $\{KU_a, KR_a\}$ và truyền thông báo cho B. Thông báo gồm KU_a và tên của A (ID_A).

B tạo ra khoá bí mật (K_s) và truyền cho A. Khoá được mã bằng khoá công khai của A.

A tính toán $D_{KRa}[E_{KUa}[K_s]]$ để khôi phục lại khoá bí mật. Chỉ A mới có thể giải mã thông báo. Chỉ A và B biết được K_s.

A huỷ bỏ KU_a và KR_a, B huỷ bỏ KU_a.

Bây giờ, A và B có thể truyền thông an toàn bằng cách sử dụng mã đối xứng và khoá phiên K_s. Sau khi trao đổi xong, A và B cùng huỷ bỏ K_s. Tuy đơn giản nhưng nó là một giao thức hấp dẫn. Không có khoá nào tồn tại trước khi liên lạc và cũng không có khoá nào tồn tại sau khi kết thúc liên lạc. Do đó, rủi ro lộ khoá sẽ rất nhỏ. Tại thời điểm này, liên lạc được đảm bảo không bị nghe trộm.

Thủ tục này có điểm yếu là rất dễ bị tấn công chủ động. Nếu đối phương E có thể kiểm soát được kênh truyền thông, E có thể dàn xếp cuộc truyền thông mà không bị phát hiện, theo hình thức sau đây:

A sinh ra một cặp $\{KU_a, KR_a\}$ và truyền một thông báo cho B. Thông báo gồm có KU_a và tên của A (ID_A).

E chặn lấy thông báo, tạo ra một cặp $\{KU_e, KR_e\}$ của nó và truyền $KU_e \| ID_A$ cho B.

B sinh ra một khoá bí mật, K_s, và truyền $E_{KUe}[K_s]$

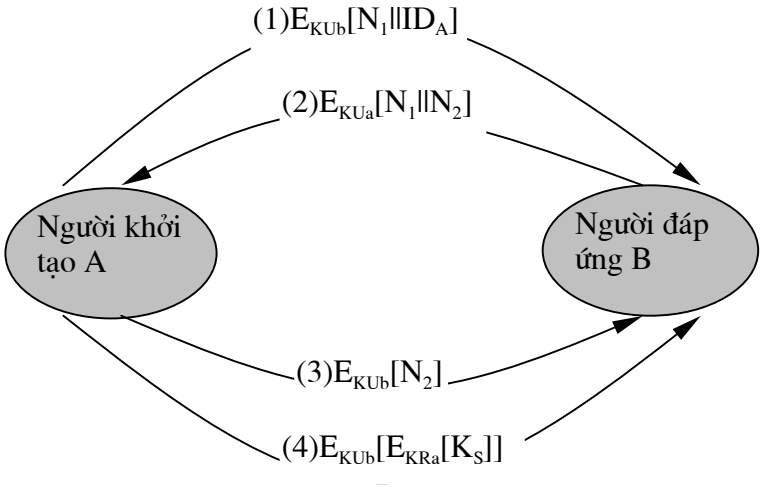
E chặn lấy thông báo, biết được K_s bằng cách tính toán $D_{KRe}[E_{KUe}[K_s]]$.

E truyền $E_{KUa}[K_s]$ cho A.

Kết quả là A và B cùng biết K_s nhưng không biết K_s đã bị E làm giả. A và B trao đổi các thông báo bằng cách sử dụng K_s. Chẳng cần mất nhiều thời gian, E có thể can thiệp vào kênh truyền thông và nghe trộm một cách đơn giản. Do biết K_s, E có thể giải mã tất cả các thông báo nhưng cả A và B đều không biết.

Phân phối khoá bí mật đảm bảo tính bí mật và xác thực

Lược đồ (được minh hoạ trong hình 3.12) có thể chống lại các kiểu tấn công chủ động và thụ động. Chúng ta bắt đầu tại thời điểm khi A và B trao đổi các khoá công khai, nhờ một trong các lược đồ được mô tả trong các phần trước.



Hình 3.12 Phân phối khoá công khai của các khoá bí mật

Các bước tiếp theo xảy ra như sau:

A sử dụng khoá công khai của B để mã hoá thông báo (1) gửi cho B. Thông báo có chứa tên của A (ID_A) và N_1 (được sử dụng để nhận diện giao dịch này).

B gửi thông báo (2) cho A. Thông báo được mã hoá bằng KU_a. Nó có chứa N_1 của A và một nonce mới (N_2) do B sinh ra. Do chỉ có B mới có thể giải mã thông báo (1), sự xuất hiện của N_1 trong thông báo (2) đảm bảo rằng A đang liên lạc với B.

A trả lại N_2, được mã hoá bằng khoá công khai của B để đảm bảo rằng B đang liên lạc với A.

A chọn một khoá bí mật K_s và gửi thông báo (3) $M= E_{KUb}[E_{KRa}[K_s]]$ cho B. Việc mã hoá thông báo này bằng khoá công khai của B đảm bảo chỉ B mới có thể đọc nó; Việc mã hoá bằng khoá riêng của A đảm bảo rằng chính A là người đã gửi thông báo.

B tính toán $D_{KUa}[D_{KRb}[M]]$ để khôi phục khoá bí mật.

Lưu ý rằng, 3 bước đầu của lược đồ này giống với 3 bước cuối trong lược đồ minh hoạ trong hình 3.9. Kết quả mà lược đồ này mang lại là đảm bảo tính tin cậy và xác thực trong trao đổi khoá bí mật.

Một lược đồ kết hợp (lai)

Có cách khác sử dụng mã hoá khoá công khai để phân phối các khoá bí mật là sử dụng lược đồ lai. Lược đồ này duy trì một trung tâm phân phối khoá, viết tắt là KDC chia xẻ một khoá chủ bí mật cho mỗi người sử dụng và phân phối các khoá phiên bí mật. Các khoá phiên bí mật này được mã hoá bằng khoá chủ. Người ta sử dụng một lược đồ khoá công khai chỉ để phân phối các khoá chủ. Lý do là:

Hiệu năng: Hiện có nhiều ứng dụng, đặc biệt các ứng dụng hướng giao dịch, trong đó các khoá phiên được thay đổi thường xuyên. Việc phân phối các khoá phiên thông qua mã hoá khoá công khai có thể làm giảm hiệu năng của toàn bộ hệ thống, do phải tính toán mã hoá và giải mã khoá công khai rất lớn. Mã hoá khoá công khai đôi khi được sử dụng để cập nhật khoá chủ giữa người sử dụng và KDC.

Khả năng tương thích: Lược đồ lai dễ dàng bao trùm lên lược đồ KDC đang tồn tại.

Lược đồ này phù hợp với cấu hình, trong đó một KDC đáp ứng một tập hợp những người sử dụng phân tán.

3.3 Xác thực thông báo và các hàm băm

3.3.1 Các yêu cầu xác thực

Trong phạm vi truyền thông qua Internet, người ta đã nhận dạng được các tấn công sau đây:

Khám phá (Disclosure): Để lộ các nội dung của thông báo do không xử lý khoá mật mã thích hợp.

Phân tích luồng thông tin (Traffic analysis): Phát hiện luồng thông tin giữa các thành viên. Trong một ứng dụng hướng kết nối, người ta có thể xác định được tần số và khoảng thời gian kết nối. Trong môi trường hướng kết nối hoặc không kết nối, người ta có thể xác định được số lượng và độ dài của các thông báo giữa các thành viên.

Giả mạo (Masquerade): Đưa thêm các thông báo có nguồn gốc giả mạo lên mạng. Thông thường, đối phương tạo ra các thông báo và gửi nó cùng với các thông báo của một thực thể hợp pháp.

Sửa đổi nội dung (content modification): Thay đổi các nội dung của một thông báo, chẳng hạn như chèn thêm, xoá bỏ, xáo trộn và sửa đổi.

Sửa đổi trình tự (sequence modification): Sửa đổi trình tự của các thông báo giữa các thành viên, chẳng hạn như chèn thêm, xoá bỏ hoặc sắp xếp lại theo trình tự mới.

Sửa đổi thời gian (Timing modification): Làm trễ hoặc chuyển tiếp thông báo nhiều lần. Trong một ứng dụng hướng kết nối, toàn bộ phiên liên lạc hoặc trình tự của các thông báo có thể bị ghi lại, sau đó được truyền đi, mặc dù chúng đã được truyền trong các phiên liên lạc hợp lệ trước đó; hoặc các thông báo riêng lẻ có thể bị làm trễ hoặc chuyển tiếp nhiều lần. Trong một ứng dụng không kết nối, một thông báo riêng lẻ (ví dụ: datagram) có thể bị làm trễ hoặc chuyển tiếp nhiều lần.

Chối bỏ (Repudiation): Bên nhận (đích) chối bỏ đã nhận thông báo hoặc bên gửi (nguồn) chối bỏ đã truyền thông báo.

Xác thực thông báo là một thủ tục nhằm kiểm tra các thông báo nhận được, xem chúng có đến từ một nguồn hợp lệ và có bị sửa đổi hay không. Xác thực thông báo cũng có thể kiểm tra trình tự và tính đúng lúc. Chữ ký số là một kỹ thuật xác thực, nó cũng bao gồm nhiều biện pháp để chống lại việc chối bỏ đã gửi hay nhận thông báo của hai bên gửi và nhận.

3.3.2 Các hàm xác thực

Trong mục này chúng ta xem xét các hàm có thể được sử dụng để tạo ra dấu xác thực (một giá trị dùng để xác thực một thông báo). Chúng có thể được nhóm thành 3 loại: mã thông báo, mã xác thực thông báo (MAC) và hàm băm.

Loại mã hoá thông báo

Bản mã của toàn bộ thông báo được sử dụng làm dấu xác thực của chính nó. Hình 3.13 minh hoạ các sử dụng cơ bản của mã hoá thông báo. Tiếp theo chúng ta phân tích sự khác nhau của hai lược đồ: mã hoá đối xứng (hay còn gọi là mã hoá khoá riêng) và mã hoá khoá công khai.

Trong mã hoá đối xứng, thông báo được truyền từ nguồn A đến đích B được mã hoá, bằng cách sử dụng một khoá bí mật K. A và B cùng nhau chia xẻ khoá K này.

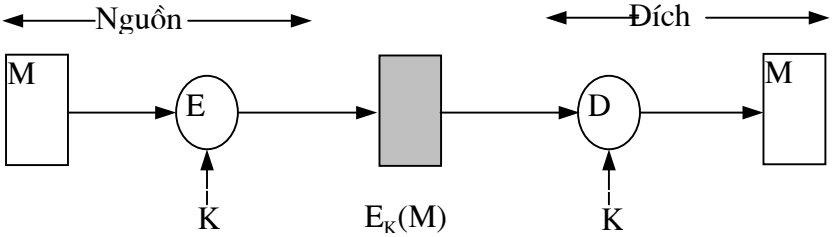
Tính bí mật được đảm bảo khi không một thành viên nào khác biết được khoá này và họ không thể khôi phục lại bản rõ của thông báo. Hơn nữa, B được đảm bảo rằng - thông báo B nhận được do A sinh ra và nó không bị sửa đổi. Mọi sửa đổi trên bản mã đều bị B phát hiện.

Mã hoá đối xứng cũng cung cấp tính xác thực. Tuy nhiên, điều này cũng cần được xem xét cẩn thận. Chúng ta quan sát những gì xảy ra ở đích B. Biết trước hàm giải mã D và khoá bí mật K, với một đầu vào X bất kỳ, chúng ta có đầu ra như sau: $Y=D_K(X)$. Nếu X là bản mã của thông báo gốc M thì đầu ra Y chính là bản rõ của thông báo đó. Nếu không, Y sẽ là một chuỗi bít vô nghĩa. B cần có một số hình thức xác định tự động, Y có phải là bản rõ đích thực hay không, nếu đúng thì nó có nguồn gốc từ A.

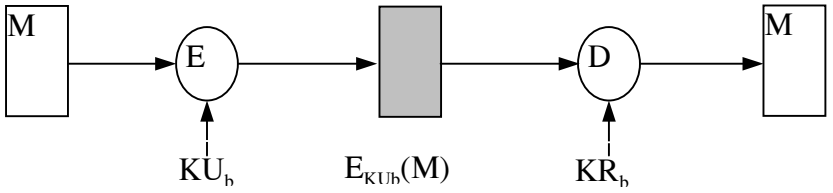
Mã hoá khoá công khai cung cấp tính bí mật nhưng không cung cấp tính xác thực. Nguồn A sử dụng khoá công khai (KU_b) của đích B để mã hoá thông báo M. Do B có khoá riêng tương ứng (KR_b) nên chỉ B mới có thể giải mã thông báo. Lược đồ này không cung

cấp tính xác thực, bởi vì bất kỳ người nào cũng có thể sử dụng khoá công khai của B để mã hoá thông báo, tự nhận mình là A.

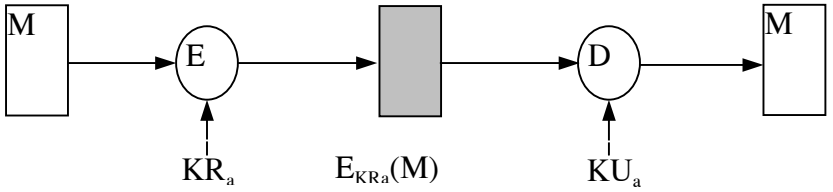
Để đảm bảo tính xác thực, A sử dụng khoá riêng của mình để mã thông báo và B sử dụng khoá công khai của A để giải mã (hình 3.13c). Cũng lập luận như trong trường hợp mã hoá đối xứng - thông báo phải có nguồn gốc từ A, do A là thành viên duy nhất sở hữu khoá KR_a. A sử dụng KR_a và các thông tin cần thiết để tạo ra bản mã. Bản mã được giải mã bằng khoá KU_a. Một lập luận nữa là cần phải có một cấu trúc bên trong nào đó cho bản rõ, qua đó người nhận có thể phân biệt bản rõ được định dạng trước với các bít ngẫu nhiên.



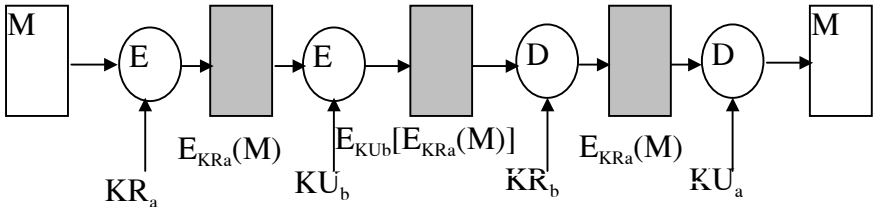
(a)Mã hoá đối xứng: bí mật và xác thực



(b)Mã hoá khoá công khai: bí mật



(c)Mã hoá khoá công khai: xác thực và chữ ký



(d) Mã hoá khoá công khai: bí mật, xác thực và chữ ký

Hình 3.13 Các sử dụng cơ bản của mã hoá thông báo

Giả sử có một cấu trúc như vậy thì lược đồ trong hình 3.13c cung cấp tính xác thực và chữ ký số. A là thành viên duy nhất tạo ra bản mã vì A sở hữu khoá KR_a. Thậm chí cả người nhận B cũng không thể tạo ra bản mã. Vì vậy, nếu B có bản mã, B cần chứng minh thông báo có nguồn gốc từ A. Thực tế là A đã "ký" thông báo bằng khoá riêng.

Lưu ý rằng, lược đồ này không cung cấp tính bí mật vì bất cứ ai sở hữu khoá công khai của A cũng có thể giải được bản mã.

Để đảm bảo cả tính bí mật lẫn xác thực, trước tiên A mã thông báo M bằng khoá riêng của A (nhằm cung cấp chữ ký số), sau đó là khoá công khai (đảm bảo tính bí mật). Khó khăn của giải pháp này là thuật toán khoá công khai phức tạp, phải thực hiện 4 lần (chứ không phải là 2 lần) cho mỗi cuộc truyền thông.

(a) Mã hoá đối xứng
$A \rightarrow B$: $E_K[M]$ Cung cấp tính bí mật - Chỉ A và B cùng nhau chia xẻ khoá K Cung cấp một mức độ xác thực - Chỉ có thể đến từ A - Không bị sửa đổi trong quá trình chuyển tiếp - Yêu cầu định dạng/phép kiểm tra dư thừa Không cung cấp chữ ký số - Người nhận có thể giả mạo thông báo - Người gửi có thể chối bỏ thông báo
(b) Mã hoá khoá công khai (phi đối xứng)
$A \rightarrow B$: $E_{KUb}[M]$ Cung cấp tính bí mật - Chỉ B có khoá KR_b để giải mã Không cung cấp tính xác thực - Bất kỳ thành viên nào cũng có thể sử dụng KU_b để mã hoá thông báo và tự nhận mình là A
$A \rightarrow B$: $E_{KRa}[M]$ Cung cấp tính xác thực và chữ ký số - Chỉ A có KR_a để mã hoá - Không bị sửa đổi trong quá trình chuyển tiếp - Yêu cầu định dạng/ phép kiểm tra dư thừa - Mọi thành viên đều có thể sử dụng KU_a để kiểm tra chữ ký
$A \rightarrow B$: $E_{KUb}[E_{KRa}(M)]$ Cung cấp tính bí mật nhờ KU_b Cung cấp tính xác thực và chữ ký nhờ KR_a

Bảng 3.3 Mối quan hệ mật thiết giữa tính bí mật và xác thực trong mã hoá thông báo

Loại dùng MAC

Một kỹ thuật xác thực (mang tính lựa chọn) như sau: sử dụng một khoá bí mật để tạo ra một khối dữ liệu nhỏ có kích thước cố định (được gọi là MAC, đây là các chữ cái đầu của Message Authentication Code, hay mã xác thực thông báo). MAC được gắn với thông báo.

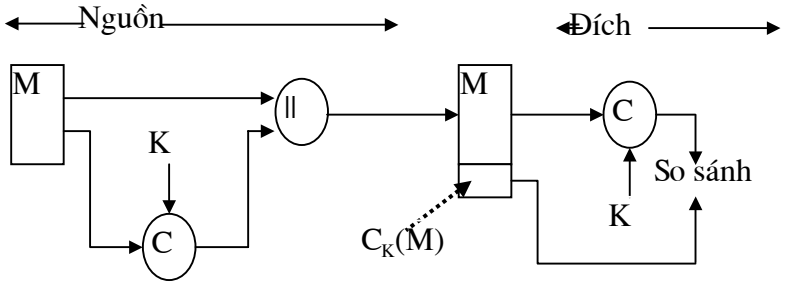
Kỹ thuật này tiến hành như sau: hai thành viên, chẳng hạn là A và B, cùng chia xẻ một khoá bí mật K. Khi A muốn gửi một thông báo cho B, A tính toán MAC như sau: $MAC=C_K(M)$. Thông báo cùng với MAC được gửi cho người nhận hợp pháp. Người nhận tiến hành tính toán tương tự trên thông báo nhận được bằng khoá bí mật chung để tạo ra một MAC mới. So sánh MAC đi kèm với thông báo và MAC mới (hình 3.14a). Giả thiết rằng, chỉ có người nhận và người gửi biết khoá bí mật, đồng thời MAC nhận được trùng khớp với MAC mới tính toán, thì:

Người nhận được đảm bảo thông báo không bị sửa đổi. Nếu đối tượng tấn công sửa đổi thông báo nhưng không sửa đổi MAC, thì giá trị MAC mới (do người nhận tính toán) sẽ không trùng khớp với MAC nhận được. Do giả thiết đối tượng tấn công không biết khoá bí mật nên chúng không thể sửa đổi MAC sao cho phù hợp với mọi sửa đổi trên thông báo.

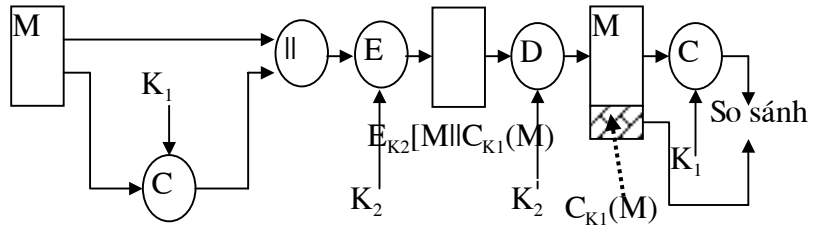
Người nhận được đảm bảo rằng thông báo có nguồn gốc từ người gửi hợp pháp. Do không ai khác (ngoài người gửi và người nhận hợp pháp) biết khoá bí mật, nên không ai có thể chuẩn bị thông báo với một MAC hợp lệ.

Nếu thông báo có số thứ tự (được sử dụng với HDLC, X.25 và TCP), người nhận được đảm bảo rằng - số thứ tự là hợp lệ, bởi vì đối tượng tấn công không thể thành công trong việc sửa đổi số thứ tự.

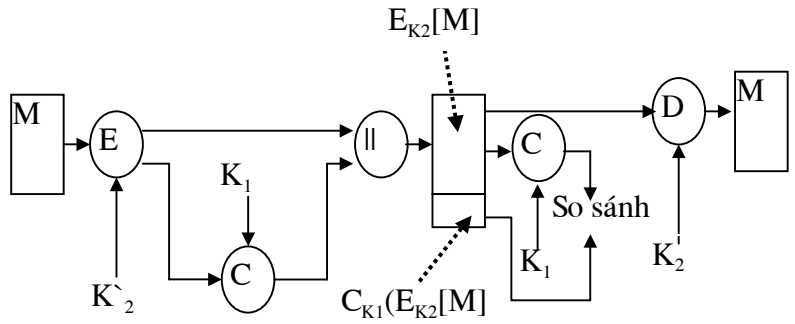
Quá trình này cung cấp tính xác thực nhưng không cung cấp tính bí mật, bởi vì toàn bộ thông báo được truyền đi ở dạng rõ. Chúng ta có thể đảm bảo tính bí mật bằng cách mã hoá thông báo sau hoặc trước thuật toán MAC (minh hoạ trong hình 3.14b,c). Trong những trường hợp này, ta cần hai khoá riêng lẻ, người gửi và người nhận cùng chia xẻ chúng.



(a) Xác thực thông báo



(b) Bí mật và xác thực thông báo; Xác thực đối với bản rõ



(c) Bí mật và xác thực thông báo; Xác thực đối với bản mã

Hình 3.14 Các sử dụng cơ bản của MAC

Do mã hoá đối xứng cung cấp tính xác thực và được sử dụng rộng rãi, người ta đã đề xuất 3 trường hợp sử dụng MAC như sau:

1. Một số ứng dụng cần gửi một thông báo tới nhiều đích. Các ví dụ, chỉ báo cho người sử dụng biết hiện tại mạng chưa sẵn sàng, hoặc một tín hiệu báo hiệu tại trung tâm kiểm soát quân sự. Nó rẻ hơn và tin cậy hơn. Do vậy, thông báo phải được gửi ở dạng rõ cùng với MAC. Hệ thống (có khoá bí mật) có trách nhiệm tiến hành xác thực. Nếu xảy ra một xâm phạm nào đó, các hệ thống đích khác đều được loan báo về tình trạng này thông qua một báo hiệu chung.

2. Trong trường hợp phải tải quá nhiều và không đủ thời gian để giải mã tất cả các thông báo gửi đến, việc xác thực được tiến hành trên cơ sở chọn lựa, có nghĩa là chọn ngẫu nhiên các thông báo để kiểm tra.

3. Xác thực chương trình máy tính ở dạng rõ là một dịch vụ hấp dẫn. Chương trình máy tính có thể được thực hiện mà không cần giải mã ở mọi thời điểm, nếu không sẽ gây ra tình trạng lãng phí các nguồn tài nguyên của bộ xử lý. Tuy nhiên, nếu chương trình có gắn kèm MAC, cần kiểm tra MAC để đảm bảo tính toàn vẹn của chương trình.

Có thể bổ xung thêm ba lý do cơ bản như sau:

Đối với một số ứng dụng, việc giữ bí mật các thông báo không phải là mối quan tâm, nhưng việc xác thực các thông báo đối với chúng lại rất quan trọng. SNMP phiên bản 3 là một ví dụ, nó tách rời các chức năng xác thực và bí mật. Trong ứng dụng này, thông thường việc hệ thống xác thực các thông báo SNMP gửi đến rất quan trọng, đặc biệt nếu thông báo có chứa lệnh thay đổi tham số của hệ thống này. Nói cách khác, nó không cần che dấu dòng thông báo SNMP.

Việc tách rời các chức năng xác thực và bí mật làm cho kiến trúc mềm dẻo hơn. Ví dụ, khi bạn muốn xác thực ở mức ứng dụng nhưng lại đảm bảo tính bí mật tại một mức thấp hơn, chẳng hạn như tầng vận tải.

Khi người sử dụng muốn kéo dài khoảng thời gian bảo vệ vượt qua thời gian nhận và cho phép xử lý các thông báo. Với mã hoá thông báo, quá trình bảo vệ kết thúc khi thông báo được giải mã, vì vậy thông báo chỉ được bảo vệ chống lại các sửa đổi gian lận trong quá trình chuyển tiếp, nhưng không được bảo vệ tại các hệ thống đích.

(a) A→B: M || C_K(M) Cung cấp tính xác thực - Chỉ A và B chia xẻ K
(b) A→B: E_{K2} [M || C_{K1}(M)] • Cung cấp tính xác thực - Chỉ A và B chia xẻ K_1 • Cung cấp tính bí mật - Chỉ A và B chia xẻ K_2
(c) A→B: E_{K2} [M] || C_{K1}(E_{K2}(M)) • Cung cấp tính xác thực - Sử dụng K_1 • Cung cấp tính bí mật - Sử dụng K_2

Bảng 3.4 Mối quan hệ mật thiết giữa tính bí mật và xác thực của các giải pháp trong hình 3.14

Cuối cùng, lưu ý rằng MAC không cung cấp chữ ký số bởi vì cả người gửi và người nhận cùng chia xẻ một khoá.

Hàm băm

Một biến thể của MAC là hàm băm một chiều. Hàm băm có đầu vào là thông báo M có kích thước thay đổi, đầu ra là một mã băm H(*M*) có kích thước cố định. Đôi khi người ta còn gọi đầu ra của hàm băm là tóm lược thông báo. Mã băm là một hàm của tất cả các bit có trong thông báo, đồng thời nó cung cấp khả năng phát hiện lỗi: nếu A thay đổi một bit bất kỳ hoặc nhiều bit trong thông báo dẫn đến kết quả là mã băm cũng thay đổi theo.

Mục đích của hàm băm là tạo ra một "dấu vân tay" cho một file, một thông báo, hoặc khối dữ liệu. Để đáp ứng được việc xác thực thông báo, một hàm băm H phải bao gồm các tính chất sau đây:

1. H được áp dụng cho một khối dữ liệu có kích cỡ bất kỳ.
2. Đầu ra của H có độ dài cố định.
3. Dễ dàng tính toán được H(*x*) với mọi x cho trước.
4. Với mọi mã *h* cho trước, không thể tìm được *x* sao cho H(*x*)=*h*. Đôi khi, tính chất này còn được gọi là tính chất một chiều.

5. Với mọi khối x cho trước, không thể tìm được $y \neq x$ sao cho $H(y)=H(x)$. Đôi khi, tính chất này được gọi là va chạm yếu (khả năng trùng ít).

6. Không thể tìm được bất cứ cặp (x,y) nào sao cho $H(x)=H(y)$. Tính chất này được gọi là va chạm mạnh.

Hình 3.15 minh hoạ các sử dụng cơ bản của mã băm để đảm bảo xác thực thông báo, như sau:

Thông báo cùng với mã băm được mã hoá, bằng cách sử dụng mã hoá đối xứng. Với cùng lập luận như sau: do A và B cùng dùng chung khoá bí mật, nên thông báo phải có nguồn gốc từ A và không bị sửa đổi. Mã băm cung cấp cấu trúc hoặc phép kiểm tra dư thừa nhằm đảm bảo xác thực. Do mã hoá được áp dụng cho toàn bộ thông báo và mã băm nên đảm bảo được tính bí mật.

Chỉ mã hoá mã băm, bằng cách sử dụng mã hoá đối xứng. Điều này làm giảm gánh nặng xử lý cho các ứng dụng không yêu cầu tính bí mật. Lưu ý rằng, trong thực tế, việc kết hợp các kết quả băm và mã hoá chính là MAC (hình 3.14a). Có nghĩa là, $E_K[H(M)]$ là một hàm của thông báo M (thông báo này có độ dài thay đổi) và một khoá bí mật K, nó tạo ra một đầu ra có kích thước cố định. đối phương không biết khoá bí mật nên không thể biết đầu ra này.

Chỉ mã hoá mã băm, bằng cách sử dụng mã hoá khoá công khai và khoá riêng của người gửi. Giống như (b), nó đảm bảo tính xác thực. Nó cũng cung cấp chữ ký số, bởi vì chỉ có người gửi mới có thể đưa ra mã băm mã hoá. Trong thực tế, đây chính là bản chất của kỹ thuật chữ ký số.

Để đảm bảo tính bí mật và cung cấp chữ ký số, thông báo cùng với mã băm (mã băm này đã được mã hoá bằng khoá công khai) có thể được mã hoá, bằng cách sử dụng một khoá bí mật cổ điển.

Sử dụng một hàm băm (nhưng không mã hoá) khi xác thực thông báo. Quá trình như sau: hai thành viên tham gia truyền thông chia xẻ một giá trị bí mật S. A tính toán giá trị băm từ M và S, sau đó gắn giá trị băm này vào M. Do B sở hữu S, B có thể tính toán lại giá trị băm để kiểm tra. Do giá trị bí mật không được gửi đi, đối phương không thể sửa đổi thông báo và tạo ra một thông báo giả.

Để bổ xung thêm tính bí mật vào (e), chúng ta có thể mã hoá toàn bộ thông báo cùng với mã băm.

Khi không cần đảm bảo tính bí mật, các giải pháp (b) và (c) có một thuận lợi là ít phải tính toán. Tuy nhiên, người ta ngày càng quan tâm đến các giải pháp này, vì một vài lý do sau đây:

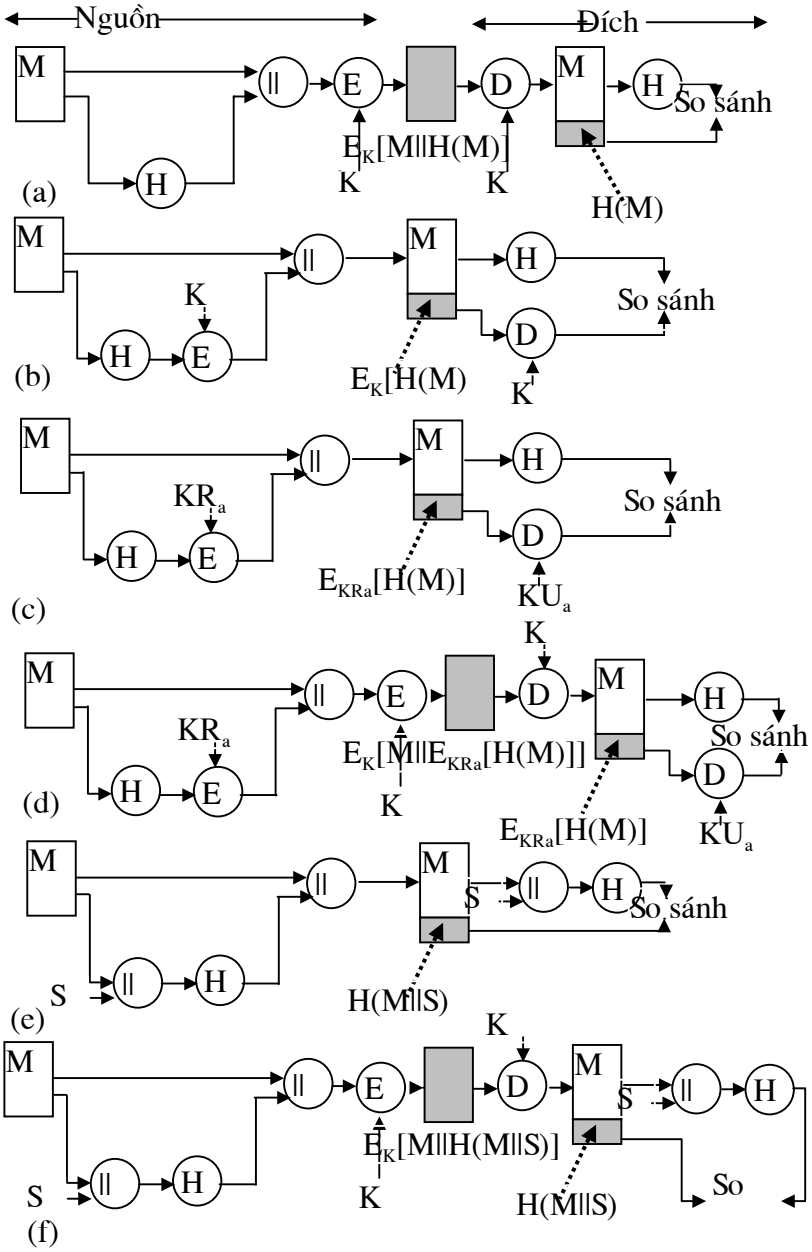
Phần mềm mã hoá tương đối chậm. Mặc dù, lượng dữ liệu được mã hoá trên mỗi thông báo không lớn, dòng các thông báo đi vào và đi ra một hệ thống ổn định.

Chi phí cho phần cứng mã hoá không nhỏ.

Phần cứng mã hoá được tối ưu theo kích cỡ dữ liệu.

Một số thuật toán mã hoá, chẳng hạn như thuật toán khoá công khai RSA, được cấp bằng sáng chế và phải được đăng ký.

Một số thuật toán bị Mỹ kiểm soát xuất khẩu.



Hình 3.15 Các sử dụng cơ bản của hàm băm

(a) A→B: E_K[M ‖ H(M)] • Cung cấp tính bí mật Chỉ A và B chia xẻ K • Cung cấp xác thực H(M) được bảo vệ mật mã	(d) A→B:E_K [M ‖ E_{KRa} [H(M)] Cung cấp xác thực và chữ ký số Cung cấp tính bí mật - Chỉ A và B chia xẻ K
(b) A→B: M ‖ E_K [H(M)] Cung cấp xác thực - H(M) được bảo vệ mật mã	(e) A→B: M‖H(M‖S) • Cung cấp xác thực - Chỉ A và B chia xẻ S
(c) A→B: M ‖ E_{KRa} [H(M)] • Cung cấp xác thực và chữ ký số - H(M) được bảo vệ mật mã - Chỉ A có thể tạo ra E_{KRa}[H(M)]	(f) A→B:E_K[M‖ H(M ‖ S)] • Cung cấp xác thực - Chỉ A và B chia xẻ S • Cung cấp tính bí mật - Chỉ A và B chia xẻ K

Bảng 3.5 Mối quan hệ mật thiết giữa xác thực và bí mật trong các giải pháp được minh hoạ trong hình 3.15

3.4 Chữ ký số

2.4.1 Các yêu cầu

Xác thực thông báo sẽ bảo vệ hai thành viên (trao đổi các thông báo qua thành viên thứ ba). Tuy nhiên, hai thành viên không bảo vệ lẫn nhau. Ví dụ, giả thiết John gửi một thông báo đã được xác thực cho Mary, bằng một trong các lược đồ được minh hoạ trong hình 3.14. Có thể xảy ra một số dạng tranh chấp giữa hai thành viên như sau:

Mary có thể làm giả một thông báo khác và tuyên bố rằng thông báo này có nguồn gốc từ John. Mary có thể tạo ra một thông báo và gắn mã xác thực một cách đơn giản bằng khoá chung của họ.

John có thể chối bỏ đã gửi thông báo. Vì Mary có thể làm giả thông báo và vì vậy không có cách nào để chứng minh John đã gửi thông báo.

Các tranh chấp xảy ra do giữa người gửi và người nhận không có sự tin cậy tuyệt đối. Giải pháp hiệu quả nhất cho vấn đề này là chữ ký số. Chữ ký số tương tự như chữ ký bằng tay. Nó phải có một số tính chất như sau:

1. Có khả năng xác thực tác giả và thời gian ký.
2. Có khả năng xác thực các nội dung tại thời điểm ký.

3. Các thành viên thứ ba có thể kiểm tra chữ ký để giải quyết các tranh chấp.

Vì vậy, chức năng ký số bao hàm cả chức năng xác thực. Dựa vào các tính chất cơ bản này, chúng ta có thể đưa ra các yêu cầu sau đây đối với một chữ ký số:

4. Chữ ký phải là một mẫu bit phụ thuộc vào thông báo được ký.

5. Chữ ký phải sử dụng một thông tin duy nhất nào đó từ người gửi, nhằm ngăn chặn tình trạng làm giả và chối bỏ.

6. Tạo ra chữ ký số dễ dàng.

7. Dễ dàng nhận ra và kiểm tra chữ ký số.

8. Khó có thể làm giả chữ ký số bằng cách tạo ra một thông báo mới cho một chữ ký số hiện có, hoặc tạo ra một chữ ký số giả cho một thông báo cho trước.

9. Trong thực tế, cần phải lưu giữ một bản sao của chữ ký số.

Có rất nhiều hướng tiếp cận được đề xuất cho chữ ký số. Các hướng tiếp cận này chia thành 2 loại: chữ ký số trực tiếp và chữ ký số của thành viên thứ ba.

Chữ ký số trực tiếp

Chữ ký số trực tiếp chỉ bao gồm các thành viên tham gia truyền thông (nguồn và đích). Giả thiết đích biết khoá công khai của nguồn. Một chữ ký số được tạo ra bằng cách mã hoá toàn bộ thông báo bằng khoá riêng của người gửi (hình 3.13c), hoặc mã hoá mã băm của thông báo bằng khoá riêng của người gửi (hình 3.15c).

Có thể đảm bảo tính bí mật bằng cách mã hoá toàn bộ thông báo và chữ ký hoặc bằng khoá công khai của người nhận (nếu dùng mã khoá công khai), hoặc khoá bí mật chung (nếu dùng mã đối xứng); Ví dụ trong hình 3.13d và 3.15d. Trong trường hợp xảy ra tranh chấp, thành viên thứ ba phải xem xét thông báo và chữ ký của nó. Nếu ký sau - mã hoá trước, thành viên thứ ba cần phải có khoá giải mã để đọc thông báo gốc. Tuy nhiên, nếu ký trước - mã hoá sau, thì người nhận có thể lưu giữ thông báo ở dạng rõ và chữ ký của nó, phòng trường hợp xảy ra tranh chấp.

Tất cả các lược đồ trực tiếp đều có chung một điểm yếu là tính hợp lệ của lược đồ phụ thuộc vào sự an toàn của khoá riêng của người gửi. Sau đó, nếu người gửi muốn chối bỏ việc anh ta đã gửi một thông báo, anh ta có thể tuyên bố: khoá riêng bị mất hoặc bị đánh cắp, một người nào đó đã làm giả chữ ký của anh ta. Để ngăn chặn tình trạng này, cần phải thực hiện các biện pháp kiểm soát quản lý (liên quan đến sự an toàn của các khoá riêng), nhưng hiểm hoạ vẫn còn tồn tại. Ví dụ, yêu cầu tất cả các thông báo được ký phải có nhãn thời gian (ngày và giờ), yêu cầu báo cáo cho cơ quan trung tâm về tình trạng các khoá bị lộ.

Một đe doạ khác là khoá riêng nào đó có thể bị đánh cắp từ X tại thời điểm T. Sau đó, đối phương có thể gửi thông báo đã được ký với chữ ký của X và gán một nhãn thời gian trước hoặc đúng thời điểm T.

Chữ ký số của thành viên thứ ba-thành viên trọng tài

Có thể giải quyết các vấn đề liên quan đến chữ ký số trực tiếp nhờ một thành viên thứ ba. Có một số lược đồ chữ ký của thành viên thứ ba như sau:

Khi X muốn gửi các thông báo cho Y, X ký tất cả các thông báo, sau đó chuyển chúng cho thành viên thứ ba A trước khi gửi cho Y. A kiểm tra nguồn gốc, nội dung của thông báo và chữ ký của nó. Sau đó, thông báo được gán nhãn thời gian và gửi cho Y với chỉ báo là thông báo đã được thành viên thứ ba kiểm tra. Sự xuất hiện của A có thể giải quyết vấn đề (X chối bỏ thông báo) trong các lược đồ chữ ký số trực tiếp.

Thành viên thứ ba đóng một vai trò nhạy cảm và quyết định trong kiểu lược đồ này. Bảng 3.6 trình bày một số ví dụ về chữ ký số của thành viên thứ ba.

Kỹ thuật đầu tiên sử dụng mã hoá đối xứng. Giả định rằng, X và A cùng chia xẻ một khoá bí mật K_{xa}, A và Y cùng chia xẻ khoá bí mật K_{ay}. X tạo ra một thông báo M và tính toán giá trị hàm băm H(M) của thông báo này. Sau đó, X gửi thông báo cùng với một chữ ký cho A. Chữ ký (gồm tên của X và giá trị băm) được mã hoá bằng khoá K_{xa}. A giải mã chữ ký và kiểm tra giá trị băm để xác nhận tính hợp lệ của thông báo. Sau đó A gửi cho Y một thông báo đã được mã hoá bằng K_{ay}.Thông báo bao gồm ID_X, thông báo gốc của X, chữ ký và một nhãn thời gian. Y có thể giải mã để khôi phục lại thông báo và chữ ký. Nhãn thời gian báo cho Y biết, thông báo đến đúng lúc và không phải là thông báo bị chuyển tiếp nhiều lần. Y có thể lưu giữ M và chữ ký. Trong trường hợp xảy ra tranh chấp, Y xác nhận đã nhận được thông báo M từ X, Y gửi cho A một thông báo như sau:

E_{Kay} [ID_X || M || E_{Kxa} [ID_X || H(M)]]

Mã đối xứng, thành viên thứ ba xem thông báo
X→A: M || E_{Kxa}[ID_X|| H(M)] A→Y: E_{Kay}[ID_X || M || E_{Kxa}[ID_X|| H(M)] || T]
Mã hoá đối xứng, thành viên thứ ba không xem thông báo
X→A: ID_X || E_{Kxy}[M] || E_{Kxa} [ID_X || H(E_{Kxy} [M])] A→Y: E_{Kay}[ID_X || E_{Kxy}[M] || E_{Kxa} [ID_X || H(E_{Kxy} [M])] || T]
Mã khoá công khai, thành viên thứ ba không xem thông báo
X→A: ID_X || E_{KRx}[ID_X || E_{KUy} (E_{KRx} [M])] A→Y: E_{KRa}[ID_X || E_{KUy} [E_{KRx} [M]] || T]

Bảng 3.6 Các kỹ thuật chữ ký số của thành viên thứ ba

Thành viên thứ ba sử dụng K_{ay} để khôi phục lại ID_X, M và chữ ký, sau đó sử dụng K_{xa} để giải mã chữ ký và kiểm tra mã băm. Trong lược đồ này, Y không thể kiểm tra trực tiếp chữ ký của X. Chính vì vậy, chỉ có chữ ký mới giải quyết được tranh chấp. Y quan tâm đến tính đích thực của thông báo (của X) vì nó được gửi đến từ A. Trong trường hợp này, cả hai phía đều phải tin cậy vào A:

10. X phải tin cậy A không làm lộ K_{xa} và không tạo ra các chữ ký (theo dạng $E_{Kxa}[ID_X || H(M)]$) giả.

11. Y phải tin cậy A chỉ gửi $E_{Kay}[ID_X || M || E_{Kxa}[ID_X || H(M)] || T]$ khi nào giá trị băm đúng và chữ ký do X tạo ra.

12. Cả hai phải tin cậy A giải quyết tranh chấp công bằng.

Nếu A đáp ứng được sự tin cậy này thì X được đảm bảo rằng không một ai có thể làm giả chữ ký của anh ta, đồng thời Y được đảm bảo X không thể chối bỏ chữ ký của anh ta. Trong trường hợp này, đối tượng nghe trộm vẫn có thể đọc được các thông báo X gửi cho Y. Trường hợp thứ hai có thể đảm bảo cả tính bí mật. Giả định rằng, X và Y dùng chung khoá bí mật K_{xy}. X gửi cho A tên của X, một bản sao của thông báo đã được mã hoá bằng khoá K_{xy} và một chữ ký. Chữ ký (gồm tên của X và giá trị băm của thông báo đã được mã hoá) được mã hoá bằng khoá K_{xa}. Do vậy, A giải mã chữ ký và kiểm tra giá trị băm để xác nhận tính hợp lệ của thông báo. Trong trường hợp này, A chỉ làm việc với bản sao của thông báo đã được mã hoá, chính vì vậy A không thể xem thông báo. Sau đó, A mã hoá mọi thứ (mà A nhận được từ X), cùng với một nhãn thời gian bằng khoá K_{ay}, rồi gửi chúng cho Y.

Mặc dù không xem được thông báo nhưng thành viên thứ ba vẫn có thể ngăn chặn được tình trạng gian lận của một trong hai phía, X hoặc Y. Một vấn đề tồn tại (như trong trường hợp đầu tiên) là thành viên thứ ba có thể liên kết với người gửi chối bỏ một thông báo đã được ký, hoặc liên kết với người nhận làm giả chữ ký của người gửi.

Có thể giải quyết được tất cả các vấn đề này, bằng một lược đồ khoá công khai. Trong trường hợp này, X mã hoá thông báo M hai lần, lần thứ nhất bằng khoá riêng của X (KR_X), lần thứ hai bằng khoá công khai của Y (KU_Y). Đây chính là một bản sao bí mật của thông báo đã được ký. Thông báo này cùng với ID_X được mã bằng khoá KR_X, sau đó đều được gửi đến A.

Thông báo (được mã hoá hai lần liên tiếp) được giữ bí mật, thành viên thứ ba (cũng như mọi thành viên khác trừ Y) không thể xem nó. Tuy nhiên, A có thể giải mã thông báo (được mã hoá sau đó) để đảm bảo rằng thông báo có nguồn gốc từ X (bởi vì chỉ X có KR_X). A kiểm tra để đảm bảo rằng - cặp khoá (công khai/riêng) của X vẫn còn hợp lệ. Sau đó, A gửi cho Y một thông báo và thông báo này được mã hoá bằng khoá KR_a. Thông báo bao gồm ID_X, thông báo được mã hoá hai lần liên tiếp và một nhãn thời gian.

Lược đồ này có một số thuận lợi so với hai lược đồ trước. Thứ nhất, các thành viên không phải chia xẻ thông tin trước khi liên lạc, vì thế có thể ngăn chặn tình trạng liên kết gian lận.

Thứ hai, không thể gửi các thông báo có thời gian không hợp lệ. Cuối cùng, nội dung của thông báo (X gửi cho Y) được giữ bí mật, A cũng như mọi thành viên khác không thể xem nó.

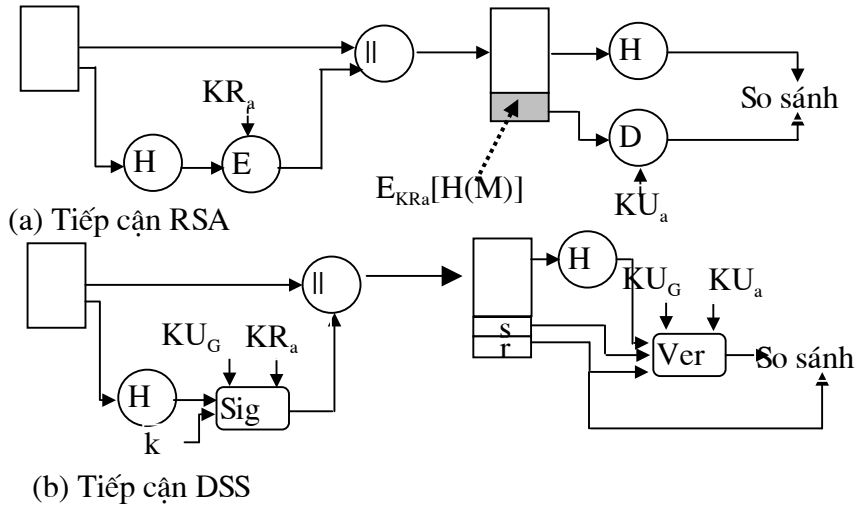
3.4.2 Chuẩn chữ ký số

Chuẩn chữ ký DSS

DSS được NIST công bố. DSS sử dụng thuật toán băm an toàn (SHA) và đưa ra một kỹ thuật chữ ký số mới (DSA). DSS được đề xuất lần đầu tiên vào năm 1991, lần tiếp theo vào năm 1993 và lần gần đây vào năm 1996.

DSS sử dụng một thuật toán cung cấp duy nhất chức năng chữ ký số. Không giống RSA, nó không được sử dụng cho để mã hoá, hoặc trao đổi khoá. Tuy nhiên, nó là một kỹ thuật khoá công khai.

Hình 3.16 trình bày sự khác nhau trong quá trình sinh chữ ký số của RSA và DSS. Trong RSA, thông báo chính là đầu vào của hàm băm. Đầu ra là một mã băm bí mật có độ dài cố định. Sau đó, mã băm được mã hoá bằng khoá riêng của người gửi để tạo ra chữ ký. Cuối cùng, thông báo cùng với chữ ký được gửi đi. Người nhận lấy thông báo và tính toán một mã băm, đồng thời giải mã chữ ký bằng khoá công khai của người gửi. Nếu mã băm vừa được tính toán trùng khớp với phần chữ ký được giải mã, chữ ký được công nhận là hợp lệ. Do chỉ người gửi biết khoá riêng nên chỉ người gửi có thể đưa ra chữ ký hợp lệ.



Hình 3.16 Hai tiếp cận chữ ký số

DSS cũng sử dụng một hàm băm. Mã băm cùng với một số ngẫu nhiên *k* (k được sinh ra cho từng chữ ký riêng biệt) là các đầu vào của một hàm ký. Hàm ký cũng phụ thuộc vào khoá riêng của người gửi (KR_a) và một tập hợp các tham số (của một nhóm các chủ thể truyền thông) tạo thành một khoá công khai toàn cục (KU_G). Kết quả là chữ ký có hai thành phần, được gọi là *s* và *r*.

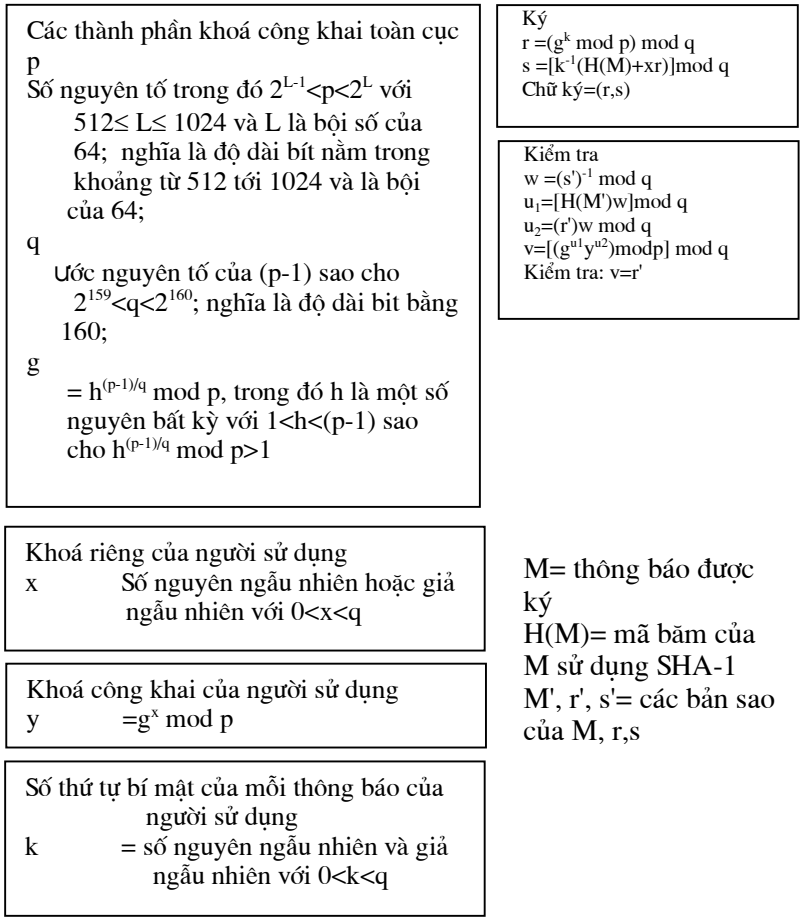
Tại nơi nhận, người nhận tính toán mã băm của thông báo gửi đến. Mã băm này cùng với chữ ký là các đầu vào của hàm kiểm tra. Hàm kiểm tra cũng phụ thuộc vào KU_G và khoá công khai KU_a của người gửi (KU_a và KR_a là hai khoá của cùng một cặp khoá). Đầu ra của hàm kiểm tra là một giá trị, nếu giá trị này trùng khớp với thành phần *r* của chữ ký, thì chữ ký được công nhận là hợp lệ. Do duy nhất người gửi biết khoá riêng nên chỉ người gửi có thể đưa ra chữ ký hợp lệ. Chúng ta sẽ xem xét chi tiết thuật toán chữ ký số trong mục tiếp theo.

Thuật toán chữ ký số

DSA dựa vào độ phức tạp tính toán logarit rời rạc và các lược đồ do ElGamal và Schnorr đưa ra.

Hình 3.17 trình bày tóm tắt thuật toán. Ở đây có 3 tham số công khai và có thể là sở hữu chung của một nhóm người sử dụng. Chọn một số nguyên tố *q* có độ dài 160 bit, tiếp theo chọn một số *p* có độ dài nằm trong khoảng từ 512 tới 1024 bit sao cho *q* chia hết cho *(p-1)*. Cuối cùng, chọn $g = h^{(p-1)/q} \bmod p$, với *h* là một số nguyên nằm trong khoảng từ 1 tới (*p-1*) trong đó g phải lớn hơn 1.

Với các số đã chọn, người sử dụng chọn một khoá riêng và sinh ra một khoá công khai. Khoá riêng *x* phải là một số nằm trong khoảng từ 1 tới (*q-1*) và nên được chọn ngẫu nhiên hoặc giả ngẫu nhiên. Khoá công khai được tính toán từ khoá riêng như sau: $y=g^x \bmod p$.

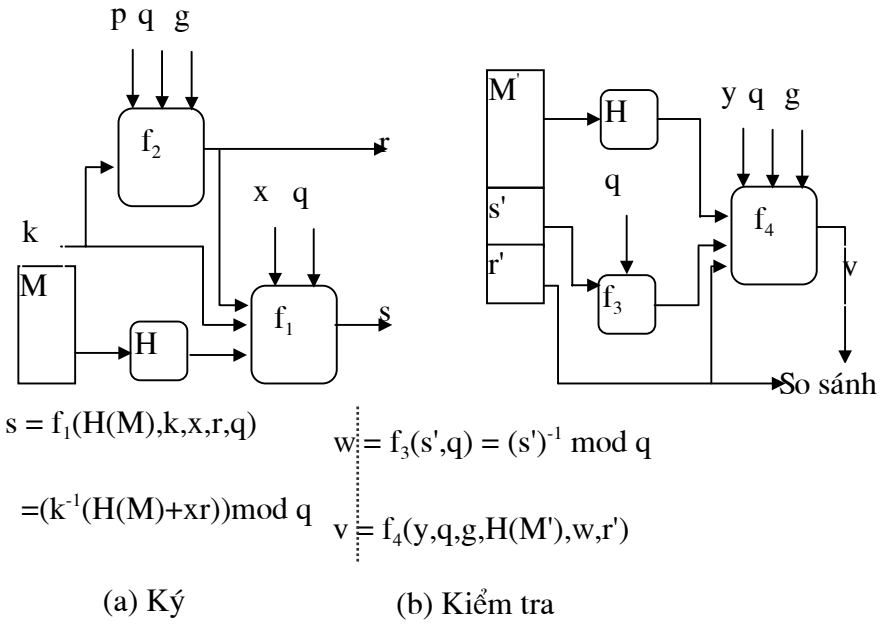


Hình 3.17 Thuật toán chữ ký số (DSA)

Dễ dàng tính toán được *y* từ *x* cho trước. Tuy nhiên, nếu biết trước khoá công khai *y*, việc tính toán *x* lại không khả thi.

Để tạo ra một chữ ký, người sử dụng tính toán *r* và *s*, chúng là các hàm của các thành phần khoá công khai (*p*, *q*, *g*), khoá riêng của người sử dụng (*x*), mã băm của thông báo, H(M) và số nguyên *k* (*k* được sinh ra ngẫu nhiên hoặc giả ngẫu nhiên, là số duy nhất cho mỗi lần ký).

Tại nơi nhận, người nhận tạo ra *v*. *v* là một hàm của các thành phần khoá công khai, khoá công khai của người gửi và mã băm của thông báo nhận được. Nếu *v* trùng khớp với *r* thì chữ ký được xác nhận hợp lệ.



Hình 3.18 Quá trình ký và kiểm tra của DSS

Hình 3.18 mô tả các hàm ký và kiểm tra. Trong đó, cấu trúc của thuật toán khá hấp dẫn. Lưu ý rằng, việc kiểm tra tại đích dựa vào việc tính toán giá trị *r*, nó hoàn toàn không phụ thuộc vào thông báo. *r* là một hàm của *k* và 3 thành phần khoá công khai toàn cục. *s* được tính như sau: $s = (k^{1}(H(M)+ xr)) \bmod q$ trong đó k^{-1} là phần tử nghịch đảo của k đối với phép nhân. Cấu trúc của hàm này giúp người nhận khôi phục lại *r* từ thông báo nhận được, chữ ký, khoá công khai của người sử dụng và khoá công khai toàn cục. Việc khôi phục *k* từ *r* hoặc khôi phục *x* từ *s* là không khả thi.

Có một điểm cần lưu ý trong quá trình ký là việc tính toán số mũ $g^k \bmod p$. Do giá trị này không phụ thuộc vào thông báo được ký, nó có thể được tính toán trước. Thực vậy, người sử dụng có thể tính toán trước một số các giá trị của *r* , khi cần thiết có thể sử dụng các giá trị này để ký các tài liệu.

Chương 4: CHỨNG CHỈ ĐIỆN TỬ

Chứng chỉ là một "tài liệu có chứa một tuyên bố được chứng thực, như là sự đúng đắn của một điều gì đó". Trong lĩnh vực điện tử, một chứng chỉ là một tài liệu chứa một tập hợp thông tin có chữ ký số của một người có thẩm quyền và người này được cộng đồng những người sử dụng chứng chỉ chấp nhận và tin cậy.

Trong thương mại điện tử, nhiều kiểu chứng chỉ được sử dụng cho các mục đích khác nhau. Một trong các kiểu chứng chỉ quan trọng là chứng chỉ khoá công khai. Trong đó, một khoá công khai được gắn kết chặt chẽ với một cá nhân, một thiết bị, hoặc một thực thể riêng biệt khác. Chứng chỉ khoá công khai được cơ quan chứng thực, CA (người hay thực thể) ký. CA chứng thực nhận dạng hoặc các thuộc tính khác của đối tượng (con người, thiết bị, hoặc thực thể nào đó) nắm giữ khoá riêng tương ứng. Các kỹ thuật mã hoá khoá công khai và chữ ký số là các yếu tố thiết yếu để đảm bảo an toàn thương mại điện tử; các chứng chỉ khoá công khai là yếu tố cần thiết để áp dụng các kỹ thuật này trên một phạm vi đủ rộng.

Trong phần này chúng ta tập trung vào các chứng chỉ khoá công khai, cách sử dụng chúng, các chuẩn liên quan và một số các vấn đề liên quan đến luật pháp xung quanh chúng, đồng thời cũng trình bày việc sử dụng các chứng chỉ cho các mục đích khác.

4.1 Giới thiệu về các chứng chỉ khoá công khai

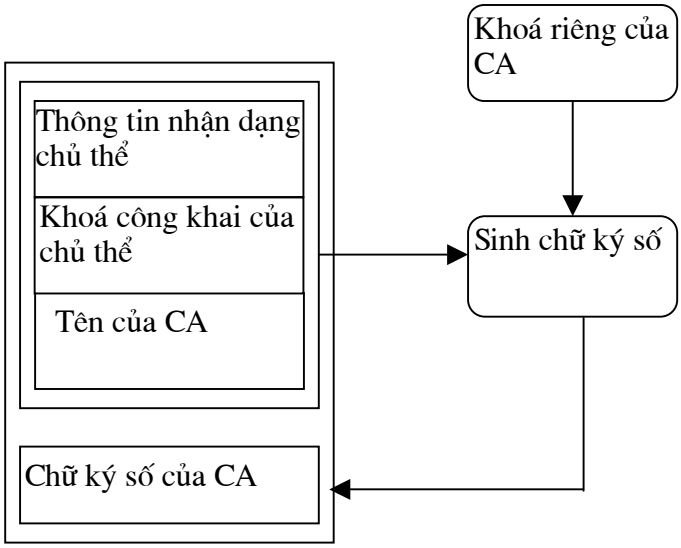
Khi người khởi tạo (người gửi) thông báo muốn sử dụng kỹ thuật khoá công khai để mã hoá một thông báo và gửi cho người nhận, anh ta cần một bản sao khoá công khai của người nhận. Khi một người bất kỳ muốn kiểm tra chữ ký số do người khác sinh ra, người kiểm tra cần một bản sao khoá công khai của người ký. Chúng ta gọi cả người mã hoá thông báo và người kiểm tra chữ ký số là những người sử dụng khoá công khai hay gọi ngắn gọn là người dùng.

Khi một khoá công khai được gửi đến cho một người dùng thì không cần thiết phải giữ bí mật khoá công khai này. Tuy nhiên, người sử dụng khoá công khai phải đảm bảo rằng khoá công khai được sử dụng đúng là dành cho thành viên khác (có nghĩa là, dành cho người nhận thông báo chủ định hoặc người tạo chữ ký số). Nếu một đối tượng truy nhập có thể dùng một khoá công khai khác thay thế cho khoá công khai hợp lệ, các nội dung của thông báo mã hoá có thể bị lộ, các thành viên bất hợp pháp khác biết được và chữ ký số có thể bị làm giả. Nói cách khác, các biện pháp bảo vệ (xuất phát từ các kỹ thuật này) bị lộ hoàn toàn nếu một đối tượng truy nhập có thể thay thế các khoá công khai không xác thực.

Đối với các nhóm thành viên nhỏ, yêu cầu này có thể được thoả mãn một cách dễ dàng. Ví dụ trong trường hợp có hai người quen biết nhau, khi người này muốn truyền thông an toàn với người kia, họ có thể có được bản sao khoá công khai của nhau bằng cách trao đổi các đĩa có chứa các khoá công khai của từng người, nhờ vậy đảm bảo rằng, các khoá công khai được lưu giữ an toàn trên mỗi hệ thống cục bộ của từng người. Đây chính là hình thức

phân phối khoá công khai thủ công. Tuy nhiên, hình thức phân phối khoá công khai thủ công này bị coi là không thực tế hoặc không thoả đáng trong phần lớn các lĩnh vực ứng dụng khoá công khai, đặc biệt khi số lượng người sử dụng trở nên quá lớn và/hoặc ở phân tán. Các chứng chỉ khoá công khai giúp cho việc phân phối khoá công khai trở nên có hệ thống.

Hệ thống khoá công khai làm việc như sau: một CA phát hành các chứng chỉ cho những người nắm giữ cặp khoá công khai và khoá riêng. Mỗi chứng chỉ gồm có một khoá công khai và thông tin dùng để nhận dạng duy nhất chủ thể (subject) của chứng chỉ. Chủ thể của chứng chỉ có thể là một người, thiết bị, hoặc một thực thể khác có nắm giữ khoá riêng tương ứng (xem hình 4.1). Khi chủ thể của chứng chỉ là một người hoặc một thực thể hợp pháp nào đó, chủ thể thường được nói đến như là một thuê bao (subscriber*)* của CA. Các chứng chỉ được CA ký, bằng khoá riêng của CA.



Hình 4.1 Chứng chỉ khoá công khai đơn giản

Một khi các chứng chỉ này được thiết lập, nhiệm vụ của người sử dụng rất đơn giản. Giả thiết rằng, một người sử dụng đã có khoá công khai của CA một cách bí mật (ví dụ, thông qua phân phối khoá công khai thủ công) và anh ta tin cậy CA phát hành các chứng chỉ hợp lệ. Nếu người dùng cần khoá công khai của một trong các thuê bao của CA này, anh ta có thể thu được khoá công khai của một thuê bao bằng cách lấy một bản sao chứng chỉ của thuê bao, lấy ra khoá công khai, kiểm tra chữ ký của CA có trên chứng chỉ bằng cách sử dụng khoá công khai của CA. Người sử dụng các chứng chỉ theo cách này được gọi là một thành viên tin cậy.

Kiểu hệ thống này tương đối đơn giản và kinh tế khi thiết lập trên diện rộng và theo hình thức tự động, bởi vì một trong các đặc tính quan trọng của các chứng chỉ là:

"*Các chứng chỉ có thể được phát hành mà không cần phải bảo vệ thông qua các dịnh vụ an toàn truyền thông truyền thống để đảm bảo tính bí mật, tính xác thực và tính toàn vẹn.*"

Chúng ta không cần giữ bí mật khoá công khai, như vậy các chứng chỉ không phải là bí mật. Hơn nữa, ở đây không đòi hỏi các yêu cầu về tính xác thực và toàn vẹn, do các chứng chỉ tự bảo vệ (chữ ký số của CA có trong chứng chỉ cung cấp bảo vệ xác thực và toàn vẹn). Nếu một đối tượng truy nhập trái phép định làm giả một chứng chỉ khi chứng chỉ này đang được phát hành cho những người sử dụng khoá công khai, anh ta sẽ bị những người này phát hiện ra việc làm giả, bởi vì chữ ký số của CA được kiểm tra chính xác. Chính vì vậy, các chứng chỉ khoá công khai được phát hành theo các cách không an toàn, ví dụ như thông qua các máy chủ, các hệ thống thư mục và/hoặc các giao thức truyền thông không an toàn.

Lợi ích cơ bản của một hệ thống chứng chỉ là một người sử dụng có thể có được một số lượng lớn các khoá công khai của các thành viên khác một cách đáng tin cậy, xuất phát từ thông tin khoá công khai của một thành viên, đó chính là khoá công khai của CA.

Lưu ý rằng, một chứng chỉ chỉ hữu ích khi người sử dụng khoá công khai tin cậy CA phát hành các chứng chỉ hợp lệ.

4.1.1 Đường dẫn chứng thực

Nếu việc thiết lập một CA (có thể phát hành các chứng chỉ khoá công khai cho tất cả những người giữ các cặp khoá công khai và khoá riêng trên thế giới) là khả thi và tất cả những người sử dụng tin cậy vào các chứng chỉ do CA này phát hành thì chúng ta có thể giải quyết được vấn đề phân phối khoá công khai. Rất tiếc là điều này không thể thực hiện được. Đơn giản vì nó không thực tế đối với một CA. CA không thể có đầy đủ thông tin và các mối quan hệ với các thuê bao để có thể phát hành các chứng chỉ được tất cả những người sử dụng chấp nhận. Vì vậy, chúng ta cần chấp nhận sự tồn tại của nhiều CA trên thế giới.

Giả thiết khi có nhiều CA, một người sử dụng giữ khoá công khai của một CA (CA này đã phát hành một chứng chỉ cho thành viên mà anh ta muốn truyền thông an toàn) một cách bí mật là không thực tế. Tuy nhiên, để có được khoá công khai của CA, người sử dụng có thể tìm và sử dụng một chứng chỉ khác có khoá công khai của CA này nhưng do CA khác phát hành, khoá công khai của CA này được người sử dụng giữ an toàn.

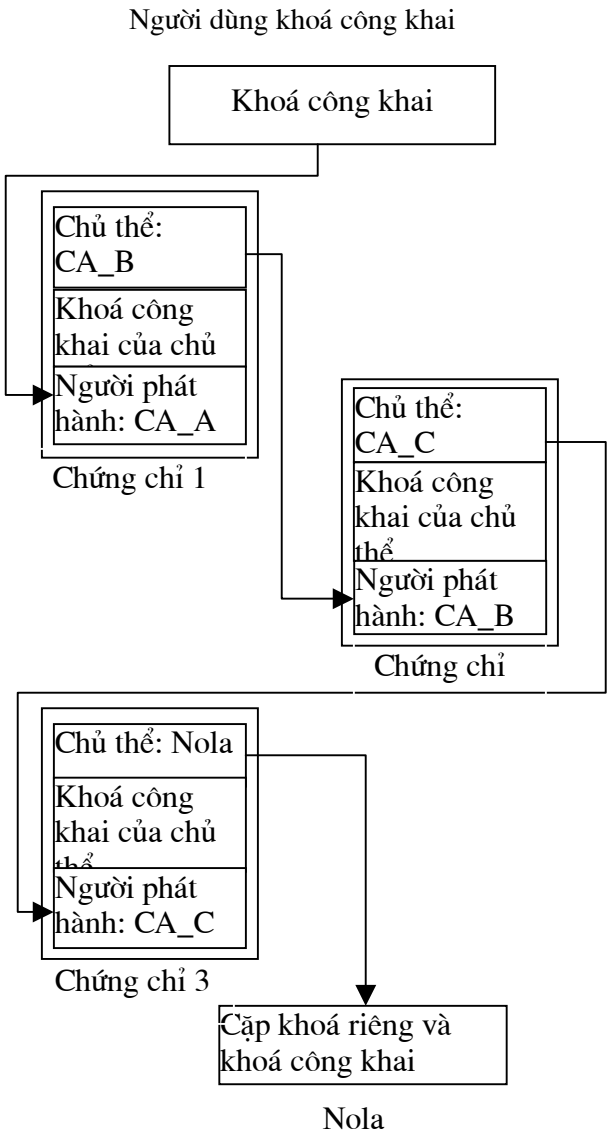
Vì vậy, một người sử dụng có thể áp dụng phương thức đệ quy chứng chỉ để nhận được khoá công khai của các CA và khoá công khai của những người sử dụng từ xa. Điều này dẫn đến một mô hình gọi là dây chuyền chứng thực hoặc đường dẫn chứng thực, dựa vào các hệ thống phân phối khoá công khai. Mô hình này được minh hoạ trong hình 4.2. Người sử dụng có thể lấy và sử dụng khoá công khai của một người giữ cặp khoá bất kỳ, ví dụ, Nola, cung cấp một đường dẫn chứng thực tin cậy từ một CA gốc của người sử dụng khoá công khai này tới Nola, thông qua một số các CA trung gian bất kỳ.

Ở đây chúng ta chưa nói đến bất kỳ giới hạn nào liên quan cấu trúc quan hệ giữa các CA. Khi tìm thấy một đường dẫn chứng thực, hệ thống sẽ làm việc.

4.1.2 Thời hạn hợp lệ và việc thu hồi

Chứng chỉ cơ bản và các mô hình đường dẫn chứng thực được trình bày ở trên được áp dụng riêng cho từng ứng dụng thực tế. Trước hết, phải thấy rằng, cặp khoá công khai và khoá riêng không phải hợp lệ mãi mãi.

Trong một hệ thống kỹ thuật, mỗi cặp khoá bất kỳ có thời gian tồn tại hạn chế để nhằm kiểm soát các cơ hội thám mã và các tấn công có thể gây ra tổn thất.



Hình 4.2 Đường dẫn chứng thực

Vì vậy, mỗi chứng chỉ có thời gian hợp lệ định trước, trên đó ghi ngày/giờ có hiệu lực và ngày/giờ hết hạn. Sau khi một chứng chỉ hết hạn, sự ràng buộc giữa khoá công khai và chủ thể của chứng chỉ có thể không còn hợp lệ nữa và chứng chỉ không còn được tin cậy. Một người sử dụng khoá công khai không nên sử dụng một chứng chỉ đã hết hạn, trừ khi muốn chứng thực lại hoạt động trước đó; Ví dụ như khi kiểm tra chữ ký trên một tài liệu cũ.

Dựa vào thời hạn kết thúc của chứng chỉ, nếu chủ thể của chứng chỉ này vẫn có một khoá công khai hợp lệ (hoặc cùng một khoá hoặc một khoá mới) thì CA có thể phát hành một chứng chỉ mới cho thuê bao này.

Hơn nữa, trong trường hợp phát hiện khoá bị lộ hoặc nghi ngờ có thể bị lộ, thời hạn kết thúc của một chứng chỉ có thể bảo vệ người sử dụng chống lại việc tiếp tục sử dụng khoá

công khai, thông qua một chứng chỉ đã được phát hành trước khi bị lộ. Ở đây có nhiều trường hợp trong đó một CA muốn huỷ bỏ hoặc thu hồi một chứng chỉ trước khi thời hạn sử dụng của nó kết thúc. Ví dụ, các chứng chỉ bị thu hồi trong trường hợp phát hiện hoặc nghi ngờ khoá riêng tương ứng bị lộ. Thủ tục thu hồi được trình bày trong mục 4.6.

4.1.3. Các mối quan hệ hợp pháp

Ở đây có hai kiểu quan hệ có thể tồn tại giữa CA và thuê bao của CA này:

(a) Cộng đồng khép kín : CA và các thuê bao của CA này là một thực thể hợp pháp (có thể không theo quy định). Ví dụ, giả thiết các thuê bao là một tập hợp các máy rút tiền tự động của một ngân hàng, nó sinh ra các chữ ký số cho các giao dịch tài chính và điều hành CA. Trong trường hợp này, mục đích của các chứng chỉ thuần tuý là kỹ thuật, có nghĩa là cho phép các ứng dụng tài chính kiểm tra tính toàn vẹn của các giao dịch, bằng một khoá công khai đã biết trước.

(b) Cộng đồng mở: CA là một thực thể hợp pháp, độc lập đối với các thuê bao riêng lẻ của nó. Chứng chỉ được các thực thể hợp pháp khác sử dụng. Ví dụ, một nhà cung cấp dịch vụ mạng thương mại hoặc nhà cung cấp dịch vụ CA phát hành các chứng chỉ cho những người thuê dịch vụ. Các thuê bao ký các giao dịch và các thành viên khác kiểm tra các giao dịch này dựa vào các chứng chỉ được CA phát hành (người được các thuê bao tin cậy). Trong trường hợp này, CA thường được coi như là một CA trung gian.

Không phải tất cả các trường hợp đều có thể thuộc một trong hai kiểu quan hệ trên một cách rõ ràng, các ví dụ có thể làm cầu nối giữa hai loại trên như: một công ty hoạt động như một CA đối với những người làm công của công ty, một cơ quan giáo dục hoạt động như là một CA đối với các sinh viên của mình, hoặc một câu lạc bộ hoạt động như là một CA đối với các thành viên của nó.

Trường hợp cộng đồng mở là một mối quan hệ đặc biệt quan trọng trong các mối quan hệ trên. Đặc biệt, sự an toàn của những người sử dụng khoá công khai phụ thuộc vào CA và các CA có nghĩa vụ đối với những người này. Thêm vào đó, CA và mỗi thuê bao có nghĩa vụ đối với các thuê bao khác.

Khi một khoá công khai đã chứng thực được sử dụng cho các mục đích chữ ký số, CA trung gian đôi khi bổ xung thêm các khả năng kỹ thuật nhằm tăng số lượng người sử dụng. Một chữ ký số được kiểm tra bằng cách sử dụng một chứng chỉ của một CA độc lập - có thể cung cấp bằng chứng thuyết phục hơn một chữ ký số được kiểm tra trên cơ sở phân phối khoá công khai thủ công không theo thể thức. Đó là vì một CA độc lập thực hiện một vai trò gần giống với vai trò của một công chứng viên. Công chứng viên có thể công nhận một tài liệu. Ví dụ luật chữ ký số Utah dựa vào giả thiết:

"Các chữ ký trên giấy tờ có một mối liên kết bên trong với một cá nhân riêng biệt bởi vì các chữ ký này được tạo ra bằng cách viết tay. Song một cặp khoá được sử dụng để tạo ra các chữ ký số không có mối liên kết bên trong với bất kỳ ai nên một mối liên kết như vậy phải

được tạo ra khi một CA nhận dạng một người có cặp khoá xác định. Sự tin cậy của mọi chữ ký số (được tạo ra bằng một khoá riêng) sẽ phụ thuộc vào sự tin cậy của liên kết (giữa khoá riêng này với một cá nhân) của một CA."

Không quan tâm đến người nào là CA, việc chứng thực chỉ có hiệu quả nếu hai kiểu kiểm soát cơ bản được đưa ra là thích hợp:

(a) Xác thực chủ thể: CA phải xác định một cách chắc chắn rằng đối tượng nắm giữ khoá riêng (tương ứng với khoá công khai đã được chứng thực) chính là người, thiết bị hoặc thực thể đã được nhận dạng trong chứng chỉ.

(b) Bảo vệ khoá riêng : Các kiểm soát phải tồn tại để đảm bảo rằng chỉ có chủ thể - người được xác thực trong (a) có thể thực hiện việc kiểm soát sau đó, thông qua khoá riêng.

4.2 Quản lý cặp khoá công khai và khoá riêng

Trong phần này chúng ta quan tâm đến các quá trình trong quản lý chứng chỉ như phát hành, cập nhật, tạm treo và thu hồi các chứng chỉ. Các quá trình này bị chi phối bởi các yêu cầu và các quá trình dành cho việc tự quản lý các cặp khoá công khai và khoá riêng. Trong thực tế, quá trình sinh cặp khoá và quá trình tạo chứng chỉ đôi khi được kết hợp chặt chẽ.

4.2.1 Quá trình sinh cặp khoá

Khi một khoá mới được sinh ra, cần chuẩn bị chuyển giao an toàn:

- Chuyển giao khoá riêng cho đối tượng nắm giữ cặp khoá của hệ thống. Nếu có yêu cầu sao chép dự phòng, cần chuyển giao khoá riêng cho hệ thống này, và
- Chuyển giao khoá công khai cho một hoặc nhiều CA sử dụng trong quá trình tạo chứng chỉ.

Một cặp khoá được sinh ra ở một trong hai nơi (là hai lựa chọn cơ bản):

- Hệ thống lưu giữ cặp khoá: Cặp khoá được sinh ra trong cùng một hệ thống (trong cùng một thẻ bài phần cứng hoặc modun phần mềm), sau đó khoá riêng sẽ được lưu giữ và sử dụng. Đối với các cặp khoá dùng cho chữ ký số, chúng được sử dụng để hỗ trợ cho các yêu cầu chống chối bỏ, đây là một bước chuẩn bị quan trọng vì khoá riêng không bao giờ bị tách ra khỏi môi trường tự nhiên của nó trong thời gian tồn tại, điều này tạo ra sự tin cậy, không một thành viên nào khác có thể có được thông tin về khoá riêng này.
- Hệ thống trung tâm: Cặp khoá được sinh ra trong một hệ thống trung tâm nào đó, có thể liên kết với một CA và khoá riêng được chuyển tới hệ thống lưu giữ cặp khoá (được trình bày ở trên) một cách an toàn. Hình thức này thuận lợi hơn việc sinh ra cặp khoá trong một hệ thống lưu giữ trên vì hệ thống trung tâm có thể có các nguồn tài nguyên rất lớn và các kiểm soát mạnh hơn, do đó có khả năng sinh ra một cặp khoá chất lượng tốt hơn (ít có khả năng phán đoán và tính toán). Nếu khoá riêng

của một cặp khoá được sao lưu trong một hệ thống trung tâm thì đây là một bước chuẩn bị thích hợp bởi vì một hệ thống tương tự hoặc các hệ thống liên quan chặt chẽ sẽ thực hiện các chức năng sinh khoá và sao lưu khoá.

Cả hai lựa chọn sinh khoá trên cần được làm cho phù hợp và cả hai có các thủ tục tạo ra chứng chỉ khác nhau. Trong thực tế, nó không giống với một CA và một thuê bao có thể có các cách tiếp cận khác nhau tới các kiểu cặp khoá khác nhau; Ví dụ, sinh một cặp khoá dùng cho chữ ký số trong hệ thống lưu giữ cặp khoá, sinh ra một cặp khoá dùng cho việc thiết lập khoá mã trong hệ thống trung tâm. Cũng lưu ý rằng, nó có thể chứng tỏ sự tiện lợi khi kết hợp tất cả các chức năng của CA, ví dụ như sinh cặp khoá và sao lưu cặp khoá vào trong một phương tiện trung tâm (hoặc một tập hợp các phương tiện liên quan).

4.2.2 Bảo vệ khoá riêng

Lưu ý rằng, việc sử dụng kỹ thuật và các chứng chỉ khoá công khai phụ thuộc vào khoá riêng chỉ con người, thiết bị hoặc thực thể (những đối tượng được nhận dạng thông qua một chứng chỉ khoá công khai) có khả năng sử dụng. Vì vậy, việc bảo vệ khoá riêng không bị truy nhập trái phép là hết sức quan trọng.

Các khoá riêng được bảo vệ thông qua các giải pháp sau:

(a) Lưu giữ trong một modul phần cứng thường trú hoặc thẻ bài. Ví dụ như một thẻ thông minh hoặc thẻ PCMCIA.

(b) Hoặc lưu giữ trên một file dữ liệu được mã hoá trong một hệ thống máy tính hoặc một thiết bị lưu giữ dữ liệu thông thường.

Trong trường hợp khác, cần tránh truy nhập vào khoá thông qua một hoặc nhiều kỹ thuật xác thực cá nhân. Nói chung, việc xác thực cá nhân cần có mật khẩu hoặc PIN. Ví dụ, đối với giải pháp (b), việc mã hoá cần sử dụng một khoá đối xứng, khoá này được tính toán từ một mật khẩu hoặc PIN và chỉ có đối tượng nắm giữ khoá công khai biết được. Các giải pháp xác thực cá nhân khác ví dụ như sở hữu một thẻ bài vật lý hoặc kiểm tra sinh trắc học, đặc biệt các giải pháp này được sử dụng kết hợp với giải pháp (a).

Nói chung, giải pháp (a) có thể cho an toàn cao hơn giải pháp (b) nhưng chi phí lại quá cao. Giải pháp (b) đôi khi được sử dụng để bảo vệ một hoặc nhiều khoá riêng và/hoặc thông tin nhạy cảm có trong một cơ sở dữ liệu

4.2.3 Cập nhật cặp khoá

Nếu đảm bảo an toàn tốt, việc cập nhật các cặp khoá công khai và khoá riêng sẽ được thực hiện một cách thường xuyên và định kỳ, đáp ứng các điều kiện đặc biệt, ví dụ khi nghi ngờ khoá riêng bị lộ. Khi một cặp khoá mới được sinh ra, cần phải tạo ra một chứng chỉ mới cho khoá công khai này. Tuỳ thuộc vào các điều kiện đặc biệt xung quanh việc cập nhật khoá, người ta có thể thu hồi chứng chỉ trước đó. Thời gian tồn tại của cặp khoá và một chứng chỉ được thảo luận chi tiết sau.

Các yêu cầu quản lý đối với các kiểu cặp khoá khác nhau:

Một người sử dụng sẽ thường xuyên có nhiều hơn một cặp khoá và do đó có nhiều hơn một chứng chỉ. Trong tương lai sẽ có nhiều khoá và nhiều chứng chỉ được chia xẻ thông qua các ứng dụng và mọi người có thể cần và sử dụng chúng ngoài thẻ tín dụng. Ngoài các lý do trên, người sử dụng có thể sử dụng các khoá và các chứng chỉ khác nhau cho các mục đích chữ ký số và mã hoá, thoả mãn hoàn toàn các nguyên tắc quản lý vòng đời của khoá.

Như chúng ta đã biết, thuật toán RSA có đặc tính hấp dẫn. ít nhất về mặt lý thuyết, một cặp khoá có thể được sử dụng cho cả hai mục đích là mã hoá (ví dụ sử dụng khi truyền một khoá đối xứng) và chữ ký số. Ví dụ, nếu các thành viên A và B muốn truyền thông an toàn với nhau và B có một cặp khoá RSA. A có thể gửi cho B một khoá đối xứng (khoá này đã được mã hoá bằng khoá công khai của B). Bằng cách sử dụng cùng một cặp khoá, B có thể ký một thông báo gửi cho A; B sinh ra một chữ ký bằng khoá riêng của B và A kiểm tra chữ ký bằng khoá công khai của B. Tuy nhiên, nếu quan sát kỹ các vấn đề xung quanh việc quản lý khoá, rõ ràng là việc tái sử dụng một cặp khoá là không khôn ngoan.

Bây giờ chúng ta xem xét các yêu cầu quản lý đối với các kiểu cặp khoá. Trước hết với các cặp khoá dùng cho chữ ký số, có các yêu cầu như sau:

(a) Khoá riêng của một cặp khoá (cặp khoá này được sử dụng cho các mục đích chữ ký số) phải được lưu giữ trong suốt thời gian tồn tại của nó, như vậy không một thành viên nào khác ngoài đối tượng lưu giữ được công nhận có thể truy nhập vào nó. Yêu cầu này là rất cần thiết nhằm hỗ trợ chống chối bỏ. Điều được khuyến nghị thường xuyên là một khoá riêng dùng cho chữ ký số không bao giờ được đưa ra khỏi thiết bị sử dụng nó - khoá được sinh ra, được sử dụng và thu hồi trong một môđun bí mật.

(b) Nói chung, chúng ta không cần sao lưu một khoá riêng dùng cho chữ ký số phòng trường hợp mất khoá - nếu một khoá bị mất, một cặp khoá mới có thể được sinh ra một cách dễ dàng. Hơn nữa việc sao lưu sẽ mâu thuẫn với yêu cầu (a).

(c) Một khoá riêng dùng cho chữ ký số không cần phải sao lưu và vì việc sao lưu này sẽ mâu thuẫn với yêu cầu (a). Trong thực tế, một khoá riêng dành cho chữ ký số phải được thu hồi một cách an toàn khi thời gian tồn tại của nó kết thúc. Nếu một khoá riêng bị lộ, thậm chí bị lộ sau khi không còn được sử dụng một thời gian dài, nó vẫn có thể được dùng để làm giả các chữ ký trên các tài liệu cũ đã được công khai thừa nhận. Việc gán nhãn thời gian an toàn đối với các tài liệu được ký có thể làm giảm các rủi ro làm giả mà không bị phát hiện, nhưng việc gán nhãn thời gian an toàn này lại không được sử dụng rộng rãi.

(d) Một khoá công khai dành cho chữ ký số cần phải sao lưu. Khoá này được dùng để kiểm tra các chữ ký cũ tại một thời điểm bất kỳ sau khi khoá riêng tương ứng được sinh ra và được sử dụng.

Đối với các cặp khoá được sử dụng để hỗ trợ cho việc mã hoá, cần bổ xung thêm các yêu cầu quản lý khoá khác như sau:

(e) Một khoá riêng được sử dụng để mã hoá cần được sao lưu. Bởi vì sao lưu là một cách để khôi phục lại thông tin đã được mã hoá. Nếu khoá bị mất (ví dụ, do lỗi thiết bị hoặc quên mật khẩu) thì tất cả thông tin được mã hoá bằng khoá này cũng bị mất.

(f) Do phụ thuộc vào thuật toán nên một khoá công khai được sử dụng để mã hoá có thể không cần sao lưu. Với khoá RSA, việc khôi phục lại dữ liệu đã được mã hoá không cần đến khoá công khai, vì vậy không cần phải sao lưu khoá công khai này. Theo thoả thuận khoá Diffie-Hellman, khi khôi phục lại dữ liệu (đã được mã hoá và được lưu giữ) cần sử dụng khoá công khai nên khoá công khai này cần được sao lưu.

(g) Khoá riêng (được sử dụng cho việc mã hoá) không cần phải huỷ bỏ khi thời gian tồn tại của nó đã kết thúc. Trái với (e), khoá riêng này không nên bị huỷ bỏ.

Rõ ràng là, các yêu cầu từ (a) đến (d) và các yêu cầu từ (e) đến (g) mâu thuẫn nghiêm trọng với nhau. Nếu một người cố gắng sử dụng cùng một cặp khoá cho cả hai mục đích là chữ ký số và thiết lập khoá mã, thì sẽ không thể thoả mãn tất cả các yêu cầu này. Khi sử dụng các cặp khoá khác nhau cho các mục đích chữ ký số và thiết lập khoá mã cần có thêm các yêu cầu sau:

 Các thực thi khoá công khai được sử dụng để mã hoá thường phải chịu nhiều kiểm soát xuất khẩu nghiêm ngặt hơn hơn so với các thực thi khoá công khai được sử dụng cho chữ ký số. Ví dụ, độ dài của khoá dùng cho mã hoá có thể bị hạn chế đến một giá trị nhỏ hơn, so với độ dài khoá cho phép dùng trong chữ ký số. Nếu sử dụng cùng một thuật toán cho cả hai mục đích, không cần thiết phải hạn chế sự phức tạp của quá trình ký số.

Hai cặp khoá có thể cần các chu kỳ mã khác nhau. Ví dụ, một cặp khoá với mục đích chia xẻ được sử dụng thường xuyên hơn trong việc thiết lập khoá (so với dùng trong chữ ký số). Cặp khoá có thể được cập nhật thường xuyên do các yêu cầu về chu kỳ mã hoá. Tuy nhiên, tất cả các khoá công khai cần được sao lưu do yêu cầu chữ ký số. Điều này dẫn đến kết quả là cần phải sao lưu nhiều hơn so với việc sử dụng các cặp khoá riêng lẻ cho các mục đích mã hoá và chữ ký số.

Không phải tất cả các thuật toán khoá công khai đều có tính chất như RSA. Ví dụ, thuật toán DSA có thể được sử dụng cho mục đích chữ ký số, nhưng không dùng cho mục đích thiết lập khoá. Nếu sử dụng thuật toán mềm dẻo, trong tương lai sẽ giúp ích cho việc thiết kế một hệ thống hiện tại, trong đó các thuật toán khác nhau và các cặp khoá khác nhau sẽ được sử dụng cho cả chữ ký số và thiết lập khoá.

Ở đây có thể có yêu cầu làm cho việc sử dụng các khoá riêng trong mã hoá có hiệu lực đối với các công chức chính phủ (như một phần của một hệ thống giao kèo khoá uỷ nhiệm). Các khoá riêng dùng cho chữ ký số không nên bị chính phủ phát hiện theo cách này. Nếu có lý lẽ thuyết phục đối với một cơ quan của chính phủ (được uỷ quyền để nghe trộm trên các cuộc truyền thông đã được mã hoá), thì việc yêu cầu một cơ quan của chính phủ cho phép làm giả chữ ký của mọi người có thể là yêu cầu bất hợp pháp.

Các yêu cầu trên nằm trong các thiết kế của các hệ thống gửi tin điện tử PEM và PGP ban đầu, trong đó sử dụng một cặp khoá RSA đơn lẻ cho cả hai mục đích là chữ ký số và thiết lập khoá mã.

4.3 Phát hành các chứng chỉ

4.3.1 Xin cấp một chứng chỉ

Trước khi CA có thể phát hành một chứng chỉ cho một thuê bao, thuê bao cần đăng ký với CA. Việc đăng ký gồm có thiết lập một mối quan hệ giữa thuê bao và CA, sau đó chuyển thông tin xác định của thuê bao cho CA.

Tuỳ vào từng trường hợp, việc đăng ký có thể là một hành động có ý thức hoặc không có ý thức của thuê bao. Ví dụ, trong trường hợp một ông chủ cấp chứng chỉ cho những người làm công của mình, quá trình đăng ký có thể tự động. Mối quan hệ rất dễ nhận ra. Ông chủ điều hành giống như một CA, tự động truy nhập vào cơ sở dữ liệu của một người làm công và từ đó có được bất cứ thông tin cần thiết nào về người làm công này.

Trong trường hợp của một CA trung gian, quá trình đăng ký rõ ràng là rất quan trọng, người cần chứng chỉ phải xin cấp và chấp nhận chứng chỉ.

Thêm vào đó, khi đăng ký với một CA, thuê bao cần xin cấp chứng chỉ một cách rõ ràng. Sự khác biệt giữa đăng ký và xin cấp một chứng chỉ là một yêu cầu chứng chỉ cần có các thông tin xác định cho từng chứng chỉ được phát hành, ví dụ như giá trị của khoá công khai và các trường xác định khác (được yêu cầu đối với chứng chỉ).

Có nhiều cách khác nhau để đăng ký và thực hiện các yêu cầu chứng chỉ. Trong môi trường Internet, quá trình này có thể được tiến hành trực tuyến. Tuy nhiên, CA cần xác thực thuê bao và đảm bảo rằng, khoá công khai và các thông tin của thuê bao có nguồn gốc từ chính thuê bao và không bị làm giả trong quá trình chuyển tiếp từ thuê bao tới CA. CA có thể biết thêm thông tin về thuê bao bằng cách đối thoại trực tiếp với thuê bao hoặc tra cứu một cơ sở dữ liệu của thành viên thứ ba. Trong nhiều trường hợp, việc truyền một thông tin nào đó phải thông qua các kênh truyền thống, không trực tuyến; Ví dụ, một người gửi tài liệu về nhận dạng cho một công chứng viên trong thời gian đăng ký và nhận một mật khẩu bí mật từ một cuộc trao đổi trực tuyến (yêu cầu và cấp một chứng chỉ).

4.3.2 Quá trình tạo chứng chỉ

Quá trình tạo ra một chứng chỉ bao gồm các bước sau đây:

1. CA nhận được các thông tin cần thiết cho chứng chỉ.

2. CA kiểm tra sự chính xác của các thông tin trong nội dung của chứng chỉ (phù hợp với các chuẩn và các chính sách áp dụng).

3. Chứng chỉ được ký bằng một thiết bị ký sử dụng khoá riêng của CA.

4. Một bản sao của chứng chỉ được chuyển tới thuê bao và nếu được yêu cầu, thuê bao sẽ gửi trả lại một xác nhận (cho biết thuê bao đã nhận được chứng chỉ).

5. Như một dịch vụ của CA, một bản sao của chứng chỉ có thể được đưa tới một kho chứa chứng chỉ (ví dụ như một dịch vụ thư mục) để công bố.

6. Như một dịch vụ tuỳ chọn của CA, một bản sao của chứng chỉ có thể được CA lưu giữ.

7. CA ghi lại các chi tiết thích hợp của quá trình tạo chứng chỉ trên một sổ nhật ký kiểm toán.

4.3.3 Xác thực chủ thể

Trước khi phát hành một chứng chỉ, CA cần xác nhận nhận dạng của người, thiết bị hoặc thực thể nắm giữ khoá riêng tương ứng với khoá công khai có trong chứng chỉ. CA hoặc thực thể nào đó được CA tin cậy phải tiếp cận các đặc điểm tiêu biểu xác định của người, thiết bị hoặc thực thể yêu cầu.

Việc xác nhận nhận dạng sử dụng một hoặc nhiều kỹ thuật và thủ tục như sau:

 Sự hiện diện cá nhân: Sự xuất hiện của một người trước khi một thực thể tin cậy được công nhận rộng rãi rất quan trọng đối với xác nhận nhận dạng. Nó không những cho phép một CA hoặc người uỷ nhiệm của nó truy nhập vào thông tin của người xin cấp chứng chỉ và các đặc điểm điển hình, mà còn cho phép đánh giá tư cách của một người và tuân theo các quy tắc và hành động thích hợp. Một khi thiết lập được nhận dạng (dựa vào sự hiện diện cá nhân), thì sự xuất hiện của một người sẽ không cần thiết cho các mục đích chữ ký số. Nhận dạng dựa vào sự hiện diện cá nhân thường được tiến hành kết hợp với các tài liệu nhận dạng.

 Các tài liệu nhận dạng : Một CA hoặc một người uỷ quyền của CA có thể sử dụng các tài liệu nhận dạng, hoặc sử dụng riêng lẻ hoặc sử dụng kết hợp với người xin cấp chứng chỉ, để xác nhận nhận dạng của người xin cấp chứng chỉ. Các tài liệu như vậy (thông thường các tài liệu này có chứa ảnh, ví dụ như một hộ chiếu, thẻ của người làm công, hoặc bằng lái xe) được công nhận rộng rãi để đảm bảo xác nhận nhận dạng tin cậy.

Các yêu cầu nhận dạng tài liệu trong thương mại và chính phủ được quan tâm khác nhau. Ví dụ, luật công chứng của một nước quy định rằng:

" bằng chứng thoả mãn/ nó gắn liền với việc nhận dạng dựa trên các tài liệu... có nghĩa là việc nhận dạng một cá nhân ít nhất dựa vào một tài liệu hiện thời được liên bang hoặc chính phủ của một nước phát hành gồm có ảnh, chữ ký và đặc điểm nhận dạng của cá nhân. Hoặc nhận dạng một cá nhân phải dựa vào ít nhất hai tài liệu do một cơ quan, thực thể kinh doanh, liên bang hoặc một nước phát hành (gồm có ít nhất chữ ký cá nhân)"

Việc sử dụng các tài liệu nhận dạng (phù hợp với mọi kỹ thuật xác nhận nhận dạng) sẽ kèm theo các rủi ro tiềm ẩn. Các CA và những người uỷ quyền của CA có thể nhận biết một cách dễ dàng các rủi ro này.

4.3.4 Cơ quan đăng ký địa phương

CA sẽ thường xuyên yêu cầu sự hiện diện cá nhân khi tương tác với các thuê bao; Chẳng hạn như, việc kiểm tra nhận dạng của người xin cấp chứng chỉ thông qua việc trình các tài liệu nhận dạng, trao đổi thẻ vật lý hoặc thực hiện các biện pháp sinh trắc học nếu có thể. Điều này gây khó khăn cho CA khi hỗ trợ một số lượng lớn các thuê bao, đặc biệt với các thuê bao phân tán về mặt địa lý. Một giải pháp khắc phục điều này là sử dụng những người trung gian phân tán, họ sẽ liên lạc trực tiếp với thuê bao cần thiết. Những người trung gian này được gọi là cơ quan đăng ký địa phương (LRA).

Cơ quan đăng ký địa phương là một người hoặc tổ chức hỗ trợ cục bộ cho một nhóm các thuê bao của CA, các thuê bao này có thể ở cách xa CA. Cơ quan đăng ký địa phương không tự mình phát hành các chứng chỉ, đúng hơn là cơ quan đăng ký địa phương phê chuẩn việc xin cấp chứng chỉ. Sau đó, CA phát hành các chứng chỉ. Các chức năng mà LRA cung cấp có thể gồm có:

(a) Đăng ký, xoá đăng ký và thay đổi các thuộc tính của các thuê bao.

(b) Nhận dạng và xác thực các thuê bao.

(c) Xem xét các yêu cầu về sinh cặp khoá và tạo chứng chỉ, hoặc khôi phục lại các khoá đã được sao lưu.

(d) Chấp nhận và xem xét các yêu cầu treo và huỷ bỏ chứng chỉ.

(e) Phân phối các thẻ cá nhân cho những người được uỷ quyền nắm giữ chúng và khôi phục lại các thẻ quá hạn do những người này gửi đến.

4.3.5 Cập nhật chứng chỉ

Mọi chứng chỉ đều có thời hạn, vấn đề này thuộc trách nhiệm của CA, ví dụ như xử lý thu hồi. Nói chung, các chứng chỉ có thể được thay thế dựa vào thời hạn kết thúc. Các cặp khoá cũng cần được thay thế định kỳ và từ đó, tạo ra một chứng chỉ mới. Việc thu hồi và cập nhật các chứng chỉ thường đi đôi với việc thu hồi và cập nhật các cặp khoá. (Ngoại trừ trường hợp, các CA có thể phát hành một chứng chỉ đã được cập nhật cho cặp khoá chưa hết hạn).

Đôi khi, việc cập nhật chứng chỉ được thực hiện như một quá trình trong suốt đối với thuê bao nếu mục đích của việc cập nhật chứng chỉ chỉ để cập nhật cặp khoá. Ví dụ, các sản phẩm mật mã có khả năng phát hiện tự động một cặp khoá đã hết hạn, cập nhật cặp khoá này và đối thoại truyền thông cần thiết với một CA để phát hành một chứng chỉ mới, tất cả những việc này không có sự tham gia của thuê bao.

Nếu như việc cập nhật một chứng chỉ có các kéo theo, ví dụ như nếu thông tin nhận dạng nào đó của thuê bao có trong chứng chỉ bị thay đổi, hoặc nếu CA có chính sách yêu cầu xác nhận các thông tin của chứng chỉ một cách định kỳ từ thuê bao, thì bắt buộc thuê bao tham gia vào quá trình cập nhật. Thuê bao được thông báo về sự cập nhật và có thể xác nhận chấp nhận một chứng chỉ mới một cách rõ ràng.

4.4 Phân phối chứng chỉ

Để mã hoá dữ liệu cho một thành viên từ xa, hoặc để một thành viên từ xa có thể kiểm tra một chữ ký số, một người sử dụng cần có bản sao chứng chỉ, từ đó có được khoá công khai của thành viên ở xa, các chứng chỉ của một CA bất kỳ phải tạo thành một đường dẫn chứng thực đầy đủ. Lưu ý rằng, đây không hoàn toàn là một vấn đề an toàn mà là vấn đề phổ biến dữ liệu, chứng chỉ không cần chuyển giao thông qua các hệ thống hoặc các giao thức an toàn bởi vì chứng chỉ tự bảo vệ. Mục này sẽ trình bày một số cách phân phối chứng chỉ khác nhau.

4.4.1 Chứng chỉ kèm theo chữ ký

Với một chữ ký số, chúng ta có nhiều cách phân phối chứng chỉ thích hợp. Nói chung, người ký sẽ có một bản sao chứng chỉ của mình và gắn kèm bản sao này với chữ ký số. Nếu thực hiện được điều này, bất cứ người nào muốn kiểm tra chữ ký phải có chứng chỉ trong tay. Tương tự, người ký có thể gắn kèm các chứng chỉ khác, chúng có thể cần cho việc phê chuẩn chứng chỉ của người ký. Ví dụ như các chứng chỉ dành cho CA của người ký nhưng lại do các CA khác phát hành. Hầu hết các giao thức truyền thông có sử dụng chữ ký số thường gắn kèm các chứng chỉ vào các chữ ký số theo cách này.

Việc gắn kèm các chứng chỉ vào các chữ ký số có thể gây lãng phí trong truyền thông và lãng phí khả năng lưu giữ vì người kiểm tra chữ ký có thể đã có chứng chỉ cần thiết trong tay (chứng chỉ này được lưu giữ cục bộ). Chính vì lý do này, người ký tự lựa chọn, nên hay không nên gắn kèm các chứng chỉ.

Tương tự, người ký sẽ không biết chính xác người kiểm tra sẽ cần một hay nhiều chứng chỉ, cho nên sẽ tồn tại nhiều đường dẫn chứng thực đi từ những người kiểm tra khác nhau đến một người ký. Do vậy, trừ khi tồn tại một cấu trúc không mềm dẻo của CA, nó đảm bảo rằng chỉ có một đường dẫn chứng thực đi từ tất cả những người kiểm tra đến một người ký thì việc người ký phải đảm bảo rằng tất cả các chứng chỉ yêu cầu được gắn kèm vào một chữ ký là không thực tế. Do vậy, người kiểm tra cần một giải pháp lưu trữ để lấy lại các chứng chỉ bị thất lạc, ví dụ như là một thư mục hoặc kho chứa.

4.4.2 Phân phối thông qua dịch vụ thư mục

Khi sử dụng kỹ thuật khoá công khai để mã hoá một thông báo, trước tiên người khởi tạo thông báo lấy các khoá công khai đã được chứng thực của tất cả những người nhận. Anh ta có được nó có thể do tình cờ có được các bản sao của chứng chỉ khoá công khai yêu cầu được lưu giữ cục bộ, chẳng hạn thông qua các tương tác với một thành viên. Trong trường hợp tổng quát, anh ta phải tìm kiếm các chứng chỉ cần thiết. Để giải quyết vấn đề này, một dịch vụ thư mục công cộng hoặc kho chứa (có thể phân phối các chứng chỉ) là đặc biệt thích hợp. Người khởi tạo thông báo lấy lại chứng chỉ của một người nhận thông qua một thư mục, có thể kết hợp với việc lấy thông tin, ví dụ như địa chỉ thư tín điện tử của người nhận.

Một kỹ thuật dịch vụ thư mục trực tuyến toàn diện đã và đang được phát triển thông qua các quá trình chuẩn hoá của Liên hiệp Viễn thông Quốc tế (ITU) và Tổ chức Tiêu chuẩn

Quốc tế (IOS). Các chuẩn thư mục được ITU thiết kế là X.500. X.500 này cung cấp cơ sở cho việc xây dựng một dịch vụ thư mục phân tán đa mục đích bằng cách liên kết các hệ thống máy tính thuộc quyền sở hữu của các nhà cung cấp dịch vụ, các chính phủ và các tổ chức tư nhân trên phạm vi toàn cầu. Nhiều ứng dụng lớn có thể được hỗ trợ, từ tìm kiếm đơn giản tên đến địa chỉ, duyệt qua hoặc tìm kiếm có khoá thuộc tính. Thư mục X.500 có thể là một nguồn thông tin cho tất cả mọi người, cho các thành phần của mạng truyền thông, cho các ứng dụng máy tính, hoặc cho các hệ thống tự động khác. Ví dụ, cho những người dùng của mạng máy tính, chức năng tìm kiếm tên của một người có thể đưa ra các thông tin như số điện thoại, địa chỉ thư tín điện tử và các thông tin chi tiết về các giao thức của ứng dụng được thiết bị của người này hỗ trợ.

Ban đầu, các chuẩn X.500 được phát triển từ năm 1984-1988, người ta cũng nhận ra xu hướng sử dụng các thư mục X.500 cho việc phân phối các chứng chỉ khoá công khai. Do đó, các chuẩn chứa đầy đủ các đặc tính của các mục dữ liệu được yêu cầu cho X.500, kết hợp với việc mô tả mức cao các thủ tục quản lý.

Nói chung, sự chấp nhận X.500 trên thị trường chậm hơn nhiều so với mong đợi. Do quá phức tạp, nó không tồn tại cho đến giữa những năm 1990. Như vậy, cần chọn lựa hợp lý các sản phẩm có chất lượng. Hơn nữa, các nhà cung cấp dịch vụ không chấp nhận việc liên kết các thư mục trực tuyến của họ, lý do là việc liên kết này cho phép các đối tượng cạnh tranh có cơ hội truy nhập trực tiếp vào danh sách thuê bao của họ. Tuy vậy, X.500 đang được đẩy mạnh phát triển trong các công ty lớn và một số tổ chức đang tìm kiếm các cách phân phối chứng chỉ khoá công khai.

Các hệ thống thư mục độc quyền cũng được sử dụng để phân phối các chứng chỉ khoá công khai trong các môi trường phần mềm riêng; Ví dụ như các thư mục Microsoft Exchange, Lotus Notes và Netware Directory Service.

LDAP là một giao thức truy nhập thư mục Internet, tương thích với mô hình thư mục X.500. LDAP đơn giản hơn nhiều và bổ xung thuận tiện hơn các giao thức của X.500. LDAP tạo thành một giao thức chuẩn hữu ích cho việc truy nhập vào các thông tin được lưu giữ trong một thư mục, bao gồm cả các chứng chỉ khoá công khai. Lưu ý rằng, LDAP không cần đến cơ sở dữ liệu thư mục cơ bản phụ thuộc vào kỹ thuật riêng biệt bất kỳ.

4.4.3 Các giải pháp phân phối khác

Ở đây có một số cách khác dùng cho việc phân phối các chứng chỉ. Như đã trình bày ở trên, các chứng chỉ không cần được bảo vệ đặc biệt và nó được phân phối thông qua các hệ thống không cần tin cậy và sử dụng các giao thức không an toàn. Ngay sau khi các chuẩn thích hợp và các quy ước được thiết lập, Web là một cách để phổ biến các chứng chỉ từ các máy chủ chuyên dụng. Các chứng chỉ được sử dụng lặp đi lặp lại nhiều lần cũng thường được lưu giữ cục bộ trong các hệ thống sử dụng các khoá công khai.

4.5 Khuôn dạng chứng chỉ X.509

Khuôn dạng chứng chỉ khoá công khai được chấp nhận rộng rãi nhất được định nghĩa trong chuẩn X.509 của ISO/IFC/ITU.

4.5.1 Khuôn dạng chứng chỉ cơ bản

Khuôn dạng chứng chỉ X.509 gồm có 3 phiên bản, phiên bản 1 ra đời vào năm 1988, phiên bản 2 ra đời vào năm 1993 và phiên bản 3 ra đời vào năm 1996. Các khuôn dạng của phiên bản 1 và 2 được trình bày sau đây, chúng được sử dụng trong tất cả các bổ xung của X.509 cho đến năm 1996. Các yếu tố cơ bản được trình bày trong hình 4.3.

Các trường của chứng chỉ như sau:

(a) Phiên bản (Version): Chỉ ra dạng phiên bản 1,2,3.

(b) Số hiệu (Serial Number): Số hiệu nhận dạng duy nhất của chứng chỉ này. Nó được CA phát hành gán cho.

(c) Tên thuật toán ký (Signature): Tên thuật toán ký được CA sử dụng để ký chứng chỉ (sẽ được trình bày chi tiết hơn trong mục "Đăng ký đối tượng").

(d) Người phát hành (Issuer): Tên theo chuẩn X.500 của CA phát hành (được trình bày chi tiết hơn trong mục "Tên trong X.500").

(e) Thời gian hợp lệ (Validity): Ngày/giờ có hiệu lực và hết hạn của một chứng chỉ.

(f) Chủ thể (Subject): Tên X.500 của đối tượng nắm giữ khoá riêng (tương ứng với khoá công khai được chứng thực).

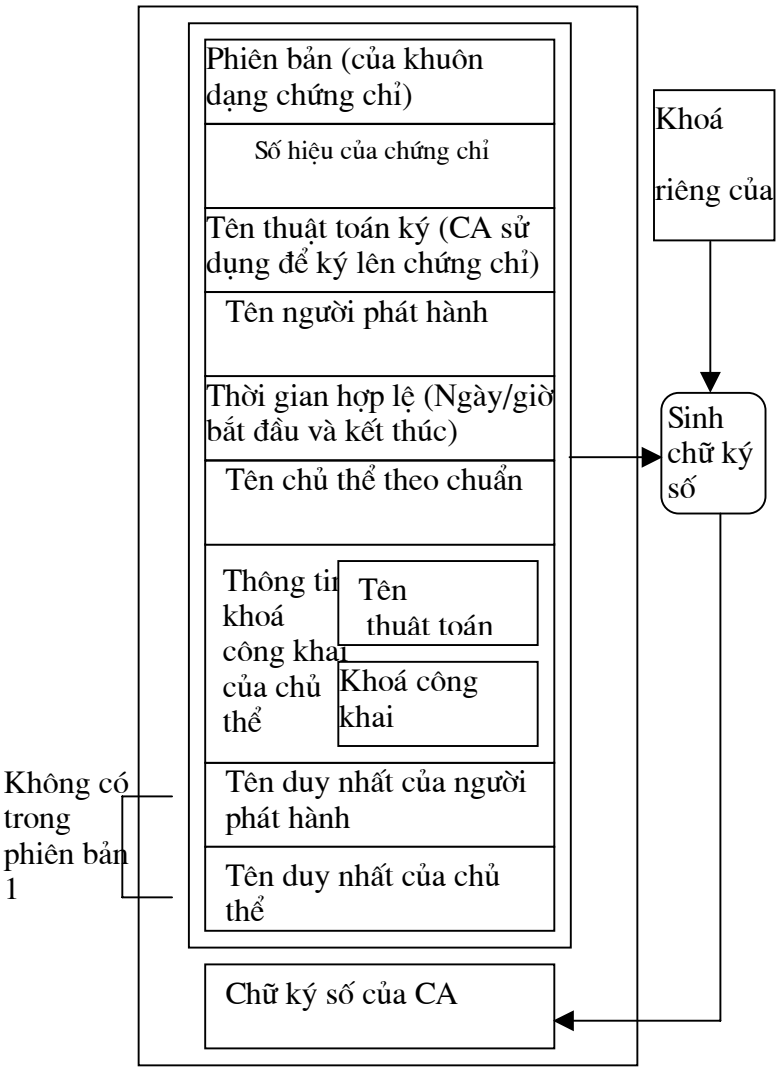
(g) Thông tin về khoá công khai của chủ thể (Subject Public-key Information): Gồm có khoá công khai của chủ thể cùng với một tên thuật toán sử dụng khoá công khai này.

(h) Tên duy nhất người phát hành (Issuer unique identifier): Là một chuỗi bít tuỳ chọn, được sử dụng để chỉ ra tên rõ ràng của CA phát hành, trong trường hợp cùng một tên được gán cho các thực thể khác nhau trong cùng thời gian (xem mục "Tên trong X.509").

(i) Tên duy nhất của chủ thể (Subject unique identifier): Là một chuỗi bít tuỳ chọn, được sử dụng để chỉ ra tên rõ ràng của chủ thể, trong trường hợp cùng một tên được gán cho các thực thể khác nhau trong cùng thời gian.

4.5.2 Tên trong X.509

Khi các chứng chỉ không bị hạn chế sử dụng kết hợp với các hệ thống thư mục X.509, các chứng chỉ của phiên bản 1 và 2 sử dụng cách đặt tên theo X.509 để nhận dạng các chủ thể và người phát hành.

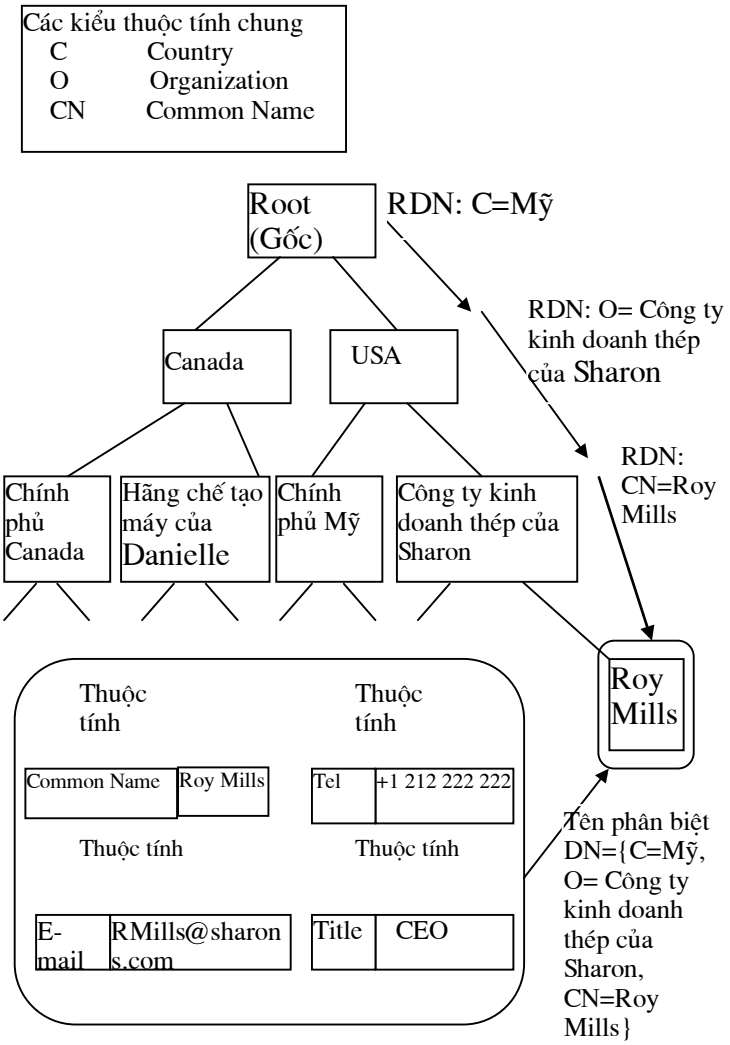


Hình 4.3 Khuôn dạng chứng chỉ trong phiên bản 1 và 2 của X.509

Thông tin được lưu giữ trong các thư mục X.509 gồm có một tập hợp các đầu vào (entry). Mỗi đầu vào liên quan tới một đối tượng thực, ví dụ một người, một tổ chức, hoặc một thiết bị. Đối tượng này có một tên rõ ràng, được gọi là tên phân biệt (DN). Đầu vào thư mục của một đối tượng có chứa các giá trị của một tập hợp các thuộc tính, gắn liền với đối tượng này. Ví dụ như thông tin đầu vào về một người có thể chứa các giá trị của các thuộc tính như tên, số điện thoại và địa chỉ thư tín điện tử. Để hỗ trợ yêu cầu đặt tên rõ ràng, tất cả các đầu vào của X.509 được tổ chức hợp lý thành một cấu trúc cây, được gọi là cây thông tin thư mục (DIT). DIT có một gốc và không hạn chế số đỉnh. Tất cả các đỉnh này (trừ gốc) phụ thuộc vào các đỉnh xa hơn. Mỗi đỉnh (trừ gốc) tương ứng với một đầu vào thư mục và có một tên phân biệt (tên phân biệt của gốc là null).

Tên phân biệt của một đầu vào được tạo ra bằng cách kết hợp tên phân biệt của đầu vào cấp trên gần nó nhất (ở trên cây) cùng với tên phân biệt liên quan (RDN), nó phân biệt đầu vào phụ thuộc với các cấp dưới trực tiếp khác của cùng một thực thể cấp trên.

RDN biểu diễn các giá trị của một (hoặc nhiều) thuộc tính của một thực thể. Chính xác hơn, đây là một tập hợp các xác nhận về giá trị của thuộc tính, mỗi xác nhận phải hoàn toàn chính xác, liên quan đến các giá trị phân biệt của một thực thể (đây là các giá trị của thuộc tính được cung cấp duy nhất). Ví dụ như một người có thể có RDN như sau *Common Name=Roy Mills*.



Hình 4.4 Ví dụ về cấu trúc tên X.500

Hình 4.4 trình bày một ví dụ về một cấu trúc tên toàn cầu của X.500. Tầng ở dưới gốc gồm có nhiều đỉnh, mỗi đỉnh liên kết với một nước. Tầng tiếp theo (ở dưới tầng các nước) có các đỉnh liên kết với các tổ chức của nước này. Các đầu vào của cá nhân và các đối tượng khác mà liên kết với một tổ chức phụ thuộc vào đầu vào của tổ chức. Cấu trúc của tên phân biệt (ví dụ như Roy Mills, người đứng đầu công ty kinh doanh thép Sharon tại Mỹ) cũng được minh hoạ trong hình 4.4.

Khuôn dạng chứng chỉ X.509 theo phiên bản 2 có hai trường tên không phải là theo tên trong X.500, các trường như tên duy nhất của người phát hành và tên duy nhất của chủ thể. Mục đích chính của việc bổ xung thêm các trường này vào phiên bản 1 để hỗ trợ các khả năng kiểm soát truy nhập của X.500. Các trường này giải quyết vấn đề việc một tên X.500 có thể bị tái sử dụng. Ví dụ, giả thiết rằng một nhân viên của công ty kinh doanh thép Sharon có tên X.500 {*Country = US, Organization = Sharon's Steelcorp.Inc, Common Name = John Smith*}. Giả thiết tiếp theo là John Smith rời khỏi công ty và tên X.500 không được gán nữa nhưng một năm sau đó công ty mời John Smith trở lại công ty và tiếp tục gán tên X.500 cũ. Điều này làm cho việc xác thực trên các danh sách kiểm soát truy nhập trở nên không rõ ràng, các danh sách kiểm soát truy nhập này được gắn vào các đối tượng dữ liệu của X.500 và việc quản lý trở nên lỏng lẻo. (Nói riêng, nếu một người sử dụng của X.500 bị loại khỏi hệ thống thì không có cách nào để tìm được tất cả các danh sách kiểm soát truy nhập đã cấp các đặc quyền cho người sử dụng này). Nói cách khác, John Smith mới có thể ngẫu nhiên gán lại các đặc quyền truy nhập của John Smith cũ. Ý tưởng của trường tên duy nhất là một giá trị mới sẽ được đặt vào trường này bất cứ khi nào tên X.500 được tái sử dụng.

Rất tiếc là các tên duy nhất không phải là giải pháp đáng tin cậy cho vấn đề này bởi vì chúng rất khó quản lý, có xu hướng che dấu không cho xem và rất dễ bị bỏ qua hoặc quên khi bổ xung. Có một giải pháp tốt hơn nhiều, có thể đảm bảo rằng tất cả các tên X.500 đều rõ ràng. Trên một RDN, chỉ cần lấy một giá trị thuộc tính duy nhất trong toàn bộ thời gian. Ở đây có một vấn đề đối với tên chung, ví dụ như công ty kinh doanh thép Sharon có thể có một hoặc nhiều người làm công với cái tên John Smith. Các tổ chức thường có một hệ thống số hiệu dành cho người làm công, hệ thống số hiệu này cũng gặp phải sự không rõ ràng như trên và khó có thể đảm bảo rằng các số hiệu của người làm công không bị tái sử dụng trong toàn bộ thời gian. Vì vậy, một dạng RDN tốt hơn cho người làm công của Sharon có thể như sau: {*Common Nam e= John Smith, Employee Number = 0012345*}. Giải pháp (không cần các trường tên duy nhất) được nhiều tổ chức (sử dụng X.500 và/hoặc X.509) chấp nhận.

4.5.3 Đăng ký đối tượng

Khuôn dạng chứng chỉ X.509 được trình bày trong hình 4.3 có các tên thuật toán. Các tên này được sử dụng để nhận dạng thuật toán ký (dùng cho chữ ký của người phát hành) và

thuật toán sử dụng khoá công khai được chứng thực. Ví dụ, các tên thuật toán khác nhau có thể được định rõ:

(a) Chữ ký số, sử dụng DSS với hàm băm SHA.

(b) Chữ ký số, sử dụng RSA với hàm băm MD5.

(c) Thiết lập khoá mã hoá, sử dụng truyền khoá RSA.

(d) Thiết lập khoá mã hoá, sử dụng kỹ thuật Diffie- Hellman.

Các tên thuật toán này là một ví dụ về một lớp các đối tượng yêu cầu đăng ký, hay là việc gán các tên của đối tượng duy nhất.

Một hệ thống đăng ký của đối tượng được sử dụng cho các tên thuật toán và cho các lớp đối tượng khác liên quan tới thương mại điện tử, chính là cơ chế tên đối tượng, được định rõ trong các chuẩn và được sự hỗ trợ của rất nhiều các cơ quan đăng ký đối tượng quốc gia.

Tên đối tượng là một giá trị, bao gồm một dãy các số nguyên. Giá trị này có thể được gán cho một đối tượng đã đăng ký. Các tên đối tượng hoàn toàn khác nhau hay một tên đối tượng là duy nhất. Các tên đối tượng dựa vào một cấu trúc phân cấp của các cơ quan gán giá trị riêng biệt. Mỗi mức của hệ thống phân cấp được gán một số nguyên phân biệt. Các nguyên tắc dành cho các mức cao hơn của hệ thống phân cấp được định rõ trong các phụ lục dành cho *ASN.1* và trong thủ tục chuẩn của cơ quan đăng ký.

Các giá trị được gán ở mức cao nhất như sau:

- 0 (dành cho ITU)

- 1 (dành cho ISO)

- 2 (dành cho cả ITU và ISO)

Theo ISO, mức thứ hai lấy các giá trị như sau: 0 (dành cho các chuẩn của ISO), 1 (dành cho các nước công nhận ISO), 2 (dành cho các tổ chức quốc tế được công nhận). Theo ISO-ITU, các giá trị khác nhau được gán cho mức thứ hai nhằm thoả mãn các yêu cầu của các chuẩn khác nhau. Một giá trị quan trọng là 16 (quốc gia - country) được sử dụng cho các cơ quan đăng ký quốc gia.

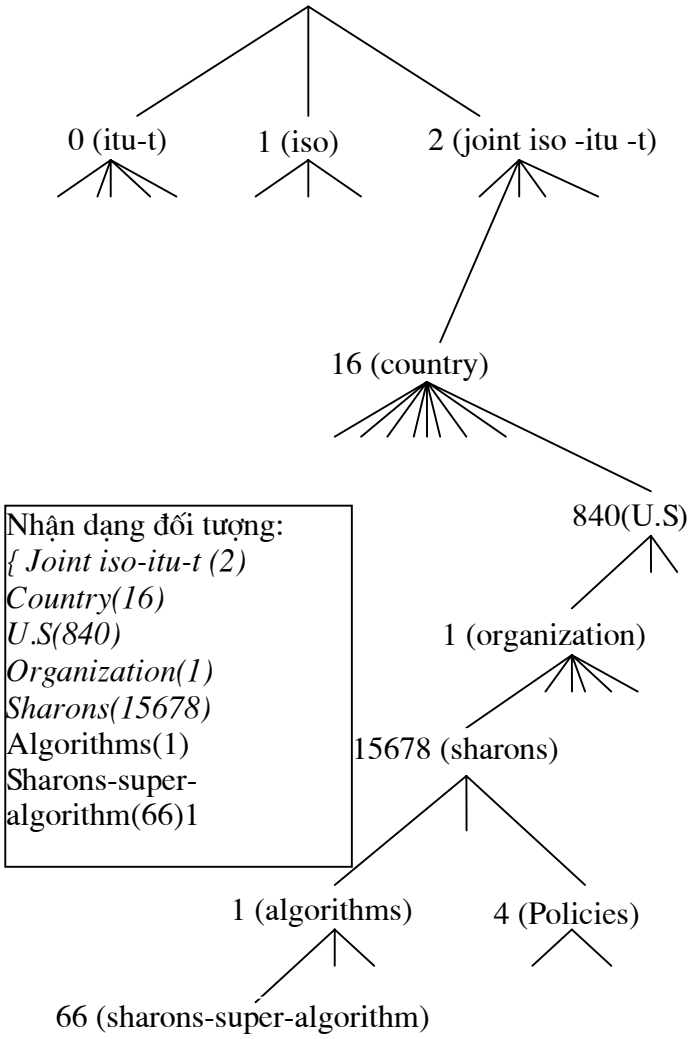
Với country = {2 16} là đặc biệt quan trọng. Tại mức kề dưới, các mã quốc gia (có 3 số) được sử dụng để nhận dạng quốc gia. Mỗi quốc gia chỉ định một tổ chức làm cơ quan đăng ký quốc gia. Ví dụ, mã quốc gia của Mỹ là 840. Mỹ chọn ANSI làm cơ quan đăng ký quốc gia của mình. ANSI gán cho các tổ chức mà đăng ký với nó ở mức dưới là 1.

Ví dụ, ANSI gán cho công ty kinh doanh thép Sharon một giá trị là 15678. Dùng cho tất cả các thành phần, điều này có nghĩa là công ty kinh doanh thép Sharon chỉ được gán (duy nhất) cho tên đối tượng với các thành phần là {2 16 840 1 15678}. Sau đó, công ty kinh doanh thép Sharon có quyền gán các giá trị của thành phần tại các mức thấp hơn tuỳ theo

mục đích của mình, ví dụ giá trị {2 16 840 1 15678 1} dành cho cây của các thuật toán mã hoá và giá trị {2 16 840 1 15678 1 66} dành cho thuật toán mã hoá riêng đặc biệt.

Hình 4.5 minh hoạ về việc gán các tên đối tượng này. Lưu ý rằng, việc gán các số này rất quan trọng. Mỗi số liên quan đến một chuỗi văn bản ngắn có thể đọc được, nhưng hệ thống tên đối tượng không phải là một hệ thống gán tên. Ví dụ, tên đối tượng cho công ty kinh doanh thép Sharon có thể được viết như sau:

{ Joint iso-itu-t (2) Country(16) U.S (840) Organization(1) Sharons(15678) Algorithms(1) Sharons-super-algorithm(66)}.



Hình 4.5 Ví dụ về tên đối tượng

Bảng sau trình bày một số ví dụ về các tên thuật toán được đăng ký, chúng được sử dụng phổ biến cho các chứng chỉ X.509.

Tên của đối tượng	Thuật toán	Nguồn của đặc tính
{iso(1) identified-organization(3) oiw(14) secsig (3) algorithm(2) 29}	Digital signature: RSA với SHA-1	NIST Open Systems Environment Implementors' Workshop (OIW) agreements
{iso(1) member-body(2) us (840) x9-57(10040) x9algorithm (4) dsa-with-sha1}	Digital signature: DSA với SHA-1	ANSI X9.57
{joint-iso-ccitt(2) country(16) us(840) organization(1) us-goverment(101) dod(2) infosec(1) algorithms(1) 2}	Digital signature: DSA với SHA-1	U.S.Department of Defense MISSI program
{iso(1) member-body(2) us (840) rsadsi(113549) pkcs(1) pkcs-1(1) md5WithRSAEncryption (4)}	Digital signature: RSA với MD5	RSA Data Security,Inc. PKCS#1

4.5.4 Khuôn dạng chứng chỉ X.509 mở rộng (phiên bản 3)

Vào khoảng những năm 1993-1994, mọi cố gắng nhằm triển khai các chứng chỉ X.509 trên một phạm vi đủ lớn được đẩy mạnh. Người ta nhận thấy rằng, các khuôn dạng chứng chỉ trong phiên bản 1 và 2 không đáp ứng được tất cả các yêu cầu. Dưới đây là các lý do giải thích việc bổ xung thêm thông tin:

(a) Giả thiết chủ thể của một chứng chỉ bất kỳ có các chứng chỉ khác nhau với các khoá công khai khác nhau (các khoá này được sử dụng cho các mục đích khác nhau) và giả thiết rằng, các cặp khoá cần được cập nhật định kỳ, do vậy cần phải có cách để phân biệt các chứng chỉ khác nhau của đối tượng này một cách dễ dàng.

(b) Một tên trong X.500 trở thành tên duy nhất của chủ thể nhưng không có đủ thông tin cho những người sử dụng chứng chỉ khác nhận dạng chủ thể, vì thế cần chuyển thêm thông tin nhận dạng chủ thể ngoài tên X.500.

(c) Một số các ứng dụng cần nhận dạng những người sử dụng thông qua các dạng tên xác định ứng dụng, ngoài các tên X.500. Ví dụ, trong an toàn thư tín điện tử, việc gắn một khoá công khai với một địa chỉ thư tín điện tử quan trọng hơn nhiều so với việc gắn với một tên X.500.

(d) Các chứng chỉ khác nhau có thể được phát hành theo các chính sách và các hoạt động chứng thực khác nhau. Các chính sách và các hoạt động chứng thực này thường chi phối mức tin cậy của người sử dụng đối với một chứng chỉ. Ví dụ, nếu một chứng chỉ được phát hành cho một thuê bao với hy vọng rằng, đôi khi nó sẽ được sử dụng cho mục đích mã hoá thư tín điện tử, CA sẽ không phải thực hiện tất cả các kiểm tra nhận dạng và xác thực thích hợp nếu chứng chỉ đã được sử dụng cho việc kiểm tra các chữ ký số trong các giao dịch tài chính giữa các tổ chức. Những người sử dụng chứng chỉ cần biết rằng, các đảm bảo và các hoạt động sẽ được áp dụng cho việc phát hành từng chứng chỉ.

(e) Các đường dẫn chứng thực không được dài tuỳ tiện và phức tạp. Khi một CA (CA phát hành) chứng thực CA khác (CA của một chủ thể), CA phát hành có thể chỉ muốn chấp nhận một tập hợp con các chứng chỉ được CA của một chủ thể phát hành (ví dụ, các chứng chỉ này bao phủ lên không gian tên của chủ thể riêng biệt).

Trong thực tế, để thoả mãn các yêu cầu (đã biết hoặc chưa biết) trong tương lai, cần bổ xung thêm các trường vào khuôn dạng của chứng chỉ. Các tổ chức chuẩn (như ISO/IEC, ITU và ANSI 19) chấp nhận bổ xung thêm vào chứng chỉ X.509 một cơ chế mở rộng chung. Kết quả là X.509 có 3 khuôn dạng chứng chỉ được định nghĩa.

Chứng chỉ trong phiên bản 3 có cùng khuôn dạng với các chứng chỉ trong phiên bản 1 và 2 nhưng có bổ xung thêm các trường mở rộng, được trình bày trong hình 4.6.

Mỗi trường mở rộng có một kiểu (cần được đăng ký). Giống với cách đăng ký một thuật toán, kiểu của trường mở rộng được đăng ký bằng cách gán cho nó một tên đối tượng. Về nguyên tắc, các kiểu của trường mở rộng được một người nào đó xác định. Trong thực tế, để làm được điều này, các kiểu của trường mở rộng thông thường phải được biết rộng rãi thông qua các thiết lập khác nhau, chính vì vậy các kiểu quan trọng của trường mở rộng phải được chuẩn hoá. Tuy nhiên, các cộng đồng quan tâm có thể xác định các kiểu của trường mở rộng để đáp ứng các nhu cầu riêng của họ.

Trong phiên bản 3, mỗi trường mở rộng chứa một giá trị tên đối tượng (chỉ ra kiểu của trường, một chỉ báo thiết yếu và một giá trị). Kiểu của mục dữ liệu trong trường con (ví dụ như chuỗi văn bản, ngày hoặc cấu trúc dữ liệu phức tạp) và ngữ nghĩa liên quan đến giá trị này do kiểu của trường mở rộng chi phối. Điều này có thể xảy ra như là kết quả của việc định nghĩa các chứng chỉ nhằm hỗ trợ cho các nhu cầu của nhiều ứng dụng, hoặc là kết quả của việc đưa ra các trường mở rộng mới thông qua việc di trú kỹ thuật.

Chỉ báo thiết yếu là một cờ. Cờ này sẽ báo khi sự xuất hiện của trường mở rộng là thiết yếu (critical) hoặc không thiết yếu (non-critical). Nếu cờ này báo sự xuất hiện của trường mở rộng là không thiết yếu thì một hệ thống sử dụng chứng chỉ được phép bỏ qua trường mở rộng nếu nó không chấp nhận kiểu của trường mở rộng. Nếu cờ này báo sự xuất hiện của trường mở rộng là thiết yếu thì một hệ thống sẽ không an toàn nếu sử dụng một phần bất kỳ của chứng chỉ, trừ khi hệ thống này chấp nhận kiểu của trường mở rộng và thiết lập chức năng liên quan.

Ví dụ, giả sử rằng trường mở rộng được xác định để chuyển một dạng tên lựa chọn cho đối tượng của chứng chỉ sử dụng, thông qua một tập hợp các ứng dụng đặc thù. Một trường như vậy có thể được báo là không thiết yếu vì các ứng dụng khác không sử dụng dạng tên lựa chọn vẫn được phép sử dụng chứng chỉ dựa vào trường tên chủ thể nguyên thuỷ ngay cả khi các ứng dụng này không có sự thoả thuận về việc mở rộng tên lựa chọn. Hoặc, giả thiết có một trường mở rộng chuyển thông tin, nó hạn chế các mục đích mà một CA có thể được đáp ứng khi sử dụng chứng chỉ. Nếu một hệ thống sử dụng chứng chỉ không hiểu trường mở rộng này hoặc bỏ qua nó thì hệ thống này có thể hoạt động không an toàn. Trong trường hợp sau, trường mở rộng phải được CA chỉ báo.

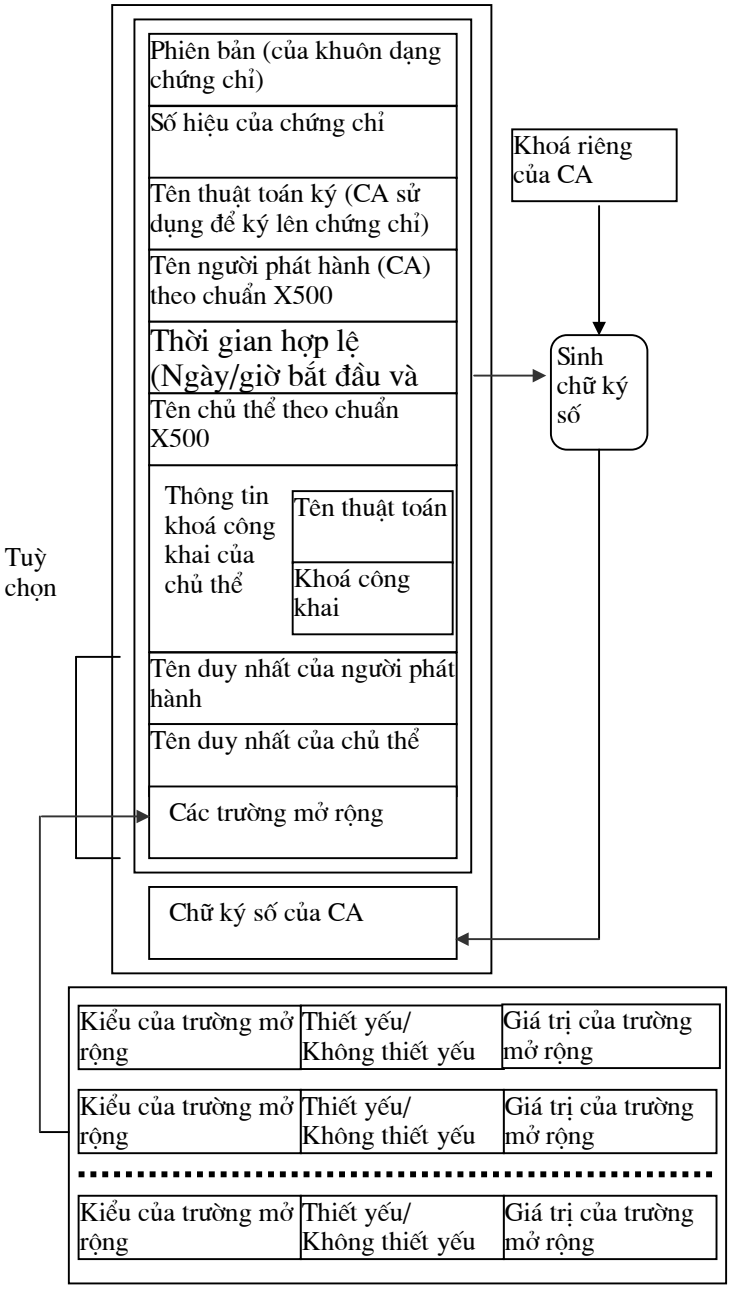
Khái niệm “thiết yếu” thường xuyên bị hiểu sai. Một trường mở rộng có thể quan trọng với người sử dụng chứng chỉ nhưng không nhất thiết phải lật cờ thiết yếu. Một hệ thống sử dụng chứng chỉ có thể yêu cầu các trường mở rộng nào đó xuất hiện trong một chứng chỉ hoặc thông tin nào đó phải có trong các trường của chứng chỉ trước khi chứng chỉ được chấp nhận. Một yêu cầu như vậy không liên quan đến tính thiết yếu, hệ thống sử dụng chứng chỉ có thể yêu cầu sự xuất hiện của các trường mở rộng không thiết yếu chẳng khác gì với yêu cầu sự xuất hiện của các trường mở rộng thiết yếu nào đó.

Các trường mở rộng không thiết yếu giúp cho việc chia xẻ chứng chỉ thông qua các ứng dụng khác nhau trở nên dễ dàng hơn và giúp cho sự di trú trở nên đơn giản hơn thông qua việc bổ xung dần dần các kiểu mới cho trường mở rộng. Các trường mở rộng thiết yếu dẫn đến các vấn đề về khả năng liên hoạt động và cần phải tránh, trừ khi giải quyết các mối quan tâm về an toàn. Thông thường khi sử dụng, đa số các trường mở rộng được lật cờ không thiết yếu.

4.5.5 Đặt tên trong phiên bản 3 của X.509

Một trong các điểm khác nhau quan trọng nhất giữa phiên bản 3 của X.509 và các phiên bản trước là việc đặt tên. Phiên bản 3 khó có thể hạn chế hệ thống đặt tên X.500.

Trong phiên bản 3 của X.509, các thực thể khác nhau được chấp nhận, các ví dụ về các thực thể là các chủ thể và người phát hành chứng chỉ. Một thực thể bất kỳ được nhận dạng thông qua một hoặc nhiều tên (có các dạng khác nhau).



Hình 4.6 Khuôn dạng chứng chỉ trong phiên bản 3 của X.509

Các ví dụ về các dạng tên như các tên X.500, các tên vùng của Internet, các địa chỉ thư tín điện tử trên Internet và các URL. Ví dụ, một thực thể có thể là một người mang tên là

Roy Mills và người này là chủ thể của chứng chỉ. Thực thể này có thể được nhận dạng bằng nhiều tên khác nhau, ví dụ như sau:

- Tên X.500: {Country=US, Organization=Sharon's Steelcorp,Inc., Common Name=Roy Mills};
- Tên X.500: {Country=US, Organization=Sharon's Steelcorp,Inc., Title=CEO};
- Địa chỉ thư tín điện tử: RMills@sharons.com.

Mỗi tên rõ ràng (được trình bày ở trên) nhận dạng một chủ thể. Vì vậy, không có lý do gì không phát hành một chứng chỉ có chứa tất cả các tên trên và bất cứ người nào cũng có thể sử dụng chứng chỉ nếu biết ít nhất một trong các tên này. Một chứng chỉ như vậy rất tiện lợi. Ví dụ, đối với một ứng dụng thư điện tử hoàn toàn không liên kết với X.500 và đơn giản chỉ muốn liên kết một khoá công khai với một địa chỉ thư điện tử. Cùng lược đồ áp dụng cho tất cả những người phát hành của chứng chỉ – một CA có thể có một hoặc nhiều tên theo các dạng khác nhau và các tên rõ ràng này nhận dạng cùng một thực thể.

Các dạng tên được chấp nhận trong chuẩn X.509 là:

- Địa chỉ thư điện tử;
- Tên domain của Internet;
- Địa chỉ thư điện tử X.400;
- Tên thư mục X.500;
- Tên thành viên EDI (gồm có tên của cơ quan gán tên, cộng với tên của thành viên được cơ quan này gán cho);
- Tên của Web Uniform Resource (trong đó URL là một kiểu phụ);
- Địa chỉ IP trên Internet (tạo thành một tên đối tượng, được trình bày chi tiết trong mục đăng ký đối tượng);
- Tên được đăng ký (theo dạng tên bất kỳ – dạng tên được đăng ký như là một đối tượng (như đã được trình bày trong mục "Đăng ký đối tượng").

Yêu cầu thiết yếu của một hệ thống đặt tên bất kỳ là tên phải rõ ràng và tên này nhận dạng một thực thể trong phạm vi một hệ thống đặt tên đang sử dụng.

4.5.6 Các trường mở rộng chuẩn của chứng chỉ

Một tập hợp các trường mở rộng chuẩn (dành cho chứng chỉ trong phiên bản 3 của X.509) được các tổ chức chuẩn ISO/IEC, ITU và ANSI 19 phát triển. Các trường mở rộng của ISO/IEC và ITU giống hệt nhau và được công bố theo dạng đã bổ xung cho chuẩn X.509. Các trường mở rộng của ANSI giống các trường mở rộng của ISO/IEC/ITU về mặt kỹ thuật nhưng tập trung vào các ứng dụng kinh doanh tài chính.

Các trường mở rộng có thể được chia nhỏ thành các nhóm như sau:

(1) Thông tin về khoá và chính sách;

(2) Các thuộc tính của chủ thể và người phát hành;

(3) Các ràng buộc đối với đường dẫn chứng thực;

(4) Các trường mở rộng liên quan đến danh sách các chứng chỉ bị thu hồi (các CRL).

Các trường mở rộng nhóm (1) chuyển thêm các thông tin về các khoá của chủ thể và người phát hành, ví dụ như các tên khoá và các chỉ báo về việc sử dụng khoá được phê chuẩn. Nó cũng chuyển các chỉ báo về chính sách của chứng chỉ (Các chính sách liên quan đến các hoạt động của CA), giúp cho việc thiết lập cơ sở hạ tầng khoá công khai trở nên dễ dàng và cho phép các nhà quản trị hạn chế các mục đích sử dụng các chứng chỉ và các khoá đã được chứng thực. Các trường mở rộng này bao gồm:

(a) Trường Authority Key Identifier: Trường này được sử dụng để phân biệt các khoá khác nhau được CA phát hành sử dụng khi ký chứng chỉ (ví dụ như các khoá khác nhau được sử dụng trong các khoảng thời gian khác nhau). Các khoá này có thể được nhận diện bằng cách:

 Thông qua một tên khoá rõ ràng;

 Thông qua một con trỏ trỏ tới một chứng chỉ khác, trong đó một CA khác chứng thực khoá của người phát hành chứng chỉ này (chứng chỉ khác được nhận dạng thông qua tên của người phát hành và số hiệu của chứng chỉ); hoặc

 Thông qua tên khoá rõ ràng và một con trỏ chứng chỉ.

Trường này giúp cho các hệ thống (các hệ thống này sử dụng chứng chỉ) tìm kiếm các chuỗi chứng chỉ một cách hiệu quả, vì vậy các CA sẽ cập nhật các cặp khoá của họ một cách định kỳ như là một phần trong quản lý vòng đời khoá.Trường này giúp cho các CA tiếp theo tìm kiếm chính xác chứng chỉ trong chuỗi chứng chỉ.

(b)Trường Subject Key Identifier: Trường này được sử dụng để phân biệt các khoá mà chủ thể của một chứng chỉ sử dụng. Ví dụ, chủ thể có thể thiết lập một cặp khoá mới một cách định kỳ và trường này chỉ ra khoá công khai nào (của một chứng chỉ xác định) được chứng thực.

(c) Trường Key Usage: Trường này được sử dụng để chỉ ra mục đích sử dụng khoá, ví dụ như cho chữ ký số (ngoài chống chối bỏ, ký chứng chỉ hoặc ký CRL), cho chống chối bỏ, mã hoá khoá, mã hoá dữ liệu, thoả thuận khoá Diffie-Hellman, ký chứng chỉ hoặc ký CRL. Trường này có hai biến thể. Biến thể đầu tiên được chỉ ra khi trường được lật cờ 'thiết yếu'. Trong biến thể này, CA giới hạn chỉ được sử dụng chứng chỉ và khoá vào các mục đích được chỉ rõ. Nếu một người đã sử dụng chứng chỉ vào các mục đích khác thì coi như vi phạm chính sách của CA và không nên tin tưởng vào chứng chỉ này. Biến thể thứ hai của trường được chỉ ra khi trường được lật cờ 'không thiết yếu'. Trong trường hợp này, trường

không khác gì một chỉ báo, người sử dụng chứng chỉ có thể sử dụng nó để tìm ra chứng chỉ đúng. Ví dụ, một người sử dụng có thể có các khoá và các chứng chỉ khác nhau, chúng được sử dụng cho các mục đích chữ ký số và thiết lập khoá mã, và cả hai chứng chỉ này được lưu giữ trong đầu vào thư mục của người sử dụng, trường này có thể giúp một người sử dụng chứng chỉ tìm ra chứng chỉ đúng. Hai biến thể của trường này có mục tiêu sử dụng riêng, nhưng sử dụng nhiều nhất là các CA sẽ chọn và sử dụng biến thể thiết yếu để hạn chế việc đưa ra trách nhiệm pháp lý của mình.

(d) Trường Private-key Usage Period: chỉ ra thời hạn sử dụng của một khoá riêng cho mục đích ký số (khoá riêng này tương ứng với khoá công khai dùng trong ký số và đã được chứng thực). Việc sử dụng trường này góp phần hạn chế khả năng lộ khoá riêng.

(e) Trường Certificate policies: chỉ ra các chính sách hoặc các hoạt động liên quan đến chứng chỉ.

(f) Trường Policy Mapping: (chỉ được sử dụng khi chủ thể của chứng chỉ cũng là một CA) cho phép người phát hành chứng chỉ chỉ ra một hoặc nhiều chính sách (cho chứng chỉ của người phát hành này), có thể được quan tâm ngang bằng với chính sách khác (như các chính sách được sử dụng trong domain của CA).

Các mở rộng Subject và Issuer Attributes hỗ trợ các tên lựa chọn dành cho các chủ thể và người phát hành chứng chỉ. Chúng cũng có thể mang thêm các thông tin thuộc tính của chủ thể để giúp cho người sử dụng chứng chỉ có được sự tin cậy đối với chứng chỉ (áp dụng cho một người, một tổ chức hoặc một thiết bị xác định). Các trường mở rộng này gồm:

(a) Trường Subject Alternative Name: Trường này chứa một hoặc nhiều tên lựa chọn phân biệt. Các chủ thể của chứng chỉ sử dụng nhiều dạng tên khác nhau. Nó cho phép chứng chỉ hỗ trợ các ứng dụng như thư tín điện tử hoặc EDI, sử dụng các dạng tên của mình và không nhất thiết phải sử dụng các thư mục X.500. Các dạng tên này được liệt kê trong mục "Đặt tên trong phiên bản 3 của X.509".

(b) Trường Issuer Alternative Name: Trường này chứa một hoặc nhiều tên lựa chọn dành cho những người phát hành của chứng chỉ. Các dạng tên dành cho người phát hành cũng giống như các dạng tên dành cho trường Subject Alternative Name. Trường này chỉ ra các CA không tuân theo X.500, ví dụ như các CA được truy nhập thông qua Web hoặc thư tín điện tử.

(c) Trường Subject Directory Attributes: Trường này chuyển cho chủ thể mọi giá trị thuộc tính của X.500 mà chủ thể mong muốn. Nó đưa ra một cách thức chung để có thể chuyển thêm thông tin nhận dạng về chủ thể, ngoài những thông tin có trong các trường tên. Các ví dụ về các thông tin nhận dạng hữu ích như vị trí của chủ thể trong một tổ chức, số điện thoại hoặc địa chỉ thư tín.

Nhóm các trường mở rộng Certification Path Constraints có thể giúp cho các tổ chức khác nhau liên kết các cơ sở hạ tầng của họ với nhau. Khi một CA chứng thực một CA

khác, trong chứng chỉ có thể có nhiều thông tin được sử dụng để chỉ báo cho người sử dụng chứng chỉ biết các giới hạn về các kiểu đường dẫn chứng thực xuất phát từ điểm này. Các trường mở rộng này gồm:

(a) Basic Constraints: Trường này chỉ ra chủ thể của chứng chỉ có thể là một CA hoặc chỉ là một thực thể cuối. Sự chỉ báo này rất quan trọng, được sử dụng để ngăn chặn những người dùng cuối cạnh tranh gian lận với các CA. Nếu chủ thể là một CA, cũng có thể định rõ sự ràng buộc đối với độ dài của đường dẫn chứng thực. Ví dụ, trường này có thể chỉ ra rằng người sử dụng chứng chỉ không được chấp nhận các đường dẫn chứng thực có đường đi dài hơn tính từ chứng chỉ này, họ có thể sử dụng các chứng chỉ của thực thể cuối (các chứng chỉ được CA của chủ thể phát hành), nhưng không nên chấp nhận các chuỗi dài hơn, trong đó CA của chủ thể đã chứng thực CA khác.

(b) Name Constraints: Trường này giới hạn không gian tên có thể chấp nhận được trong các chứng chỉ có trong một đường dẫn chứng thực.

(c) Policy constraints: Trường này xác định một tập hợp các ràng buộc cho việc nhận diện chính sách chứng chỉ và ánh xạ chính sách rõ ràng.

4.5.7 Ký hiệu và mã của ASN.1

Các khuôn dạng dữ liệu của X.509 được biểu diễn trong tập ký hiệu được gọi tắt là ASN.1, nó được phát triển như một phần của chương trình chuẩn hoá OSI. Tuy ASN.1 rất mạnh nhưng không phổ biến trong một số lĩnh vực vì nó rất phức tạp, thực tế là các đặc tính của nó không thuật tiện và chất lượng không cao, chi phí cho việc thiết lập các công cụ thấp. Tuy nhiên, ASN.1 được sử dụng trong các giao thức (ví dụ như S/MIME và SET) nên các nhà đầu tư mong muốn các ký hiệu này trở nên phổ biến và thu được các công cụ thích hợp.

4.6 Việc thu hồi chứng chỉ

Thời gian tồn tại của một chứng chỉ khoá công khai bị giới hạn, có thể biết được thời gian này thông qua giờ/ngày bắt đầu có hiệu lực và giờ/ngày hết hạn của một chứng chỉ, tất cả những thông tin này nằm trong phần được ký của chứng chỉ. Khoảng thời gian hợp lệ này kéo dài bao lâu là do chính sách của CA phát hành, thông thường thời gian tồn tại kéo dài từ vài tháng đến vài năm.

Khi một chứng chỉ được phát hành, nó có thể được sử dụng trong suốt thời gian hợp lệ của mình. Tuy nhiên, trong một số trường hợp, những người sử dụng không nên tiếp tục tin tưởng vào một chứng chỉ mặc dù thời hạn hợp lệ của chứng chỉ này chưa kết thúc. Những trường hợp đó bao gồm phát hiện hoặc nghi ngờ khoá riêng tương ứng bị lộ, thay đổi tên và thay đổi mối quan hệ giữa chủ thể và CA (ví dụ như một người làm công kết thúc hợp đồng làm thuê với một tổ chức). Trong những trường hợp như vậy, CA có thể thu hồi chứng chỉ. Do có thể thu hồi được nên khoảng thời gian hoạt động của một chứng chỉ có thể ngắn hơn so với khoảng thời gian hợp lệ được định trước.

4.6.1 Yêu cầu thu hồi

Quyết định thu hồi một chứng chỉ thuộc trách nhiệm của một CA, nói chung để đáp ứng một yêu cầu từ một người có quyền nào đó. Người có quyền thu hồi chứng chỉ dựa vào các hoạt động của một CA, thuê bao phải được biết các hoạt động này. Nói chung, thuê bao có quyền yêu cầu thu hồi chứng chỉ của mình. Những người có trách nhiệm của CA cũng có quyền thu hồi chứng chỉ của một thuê bao trong các trường hợp bắt buộc, ví dụ như vi phạm nghiêm trọng vào những điều khoản bắt buộc trong hoạt động chứng thực (CPS) do thuê bao đưa ra. Ngoài ra, những người khác có thể có quyền yêu cầu thu hồi, ví dụ những người làm công của thuê bao có thể yêu cầu thu hồi chứng chỉ liên quan đến hợp đồng làm thuê.

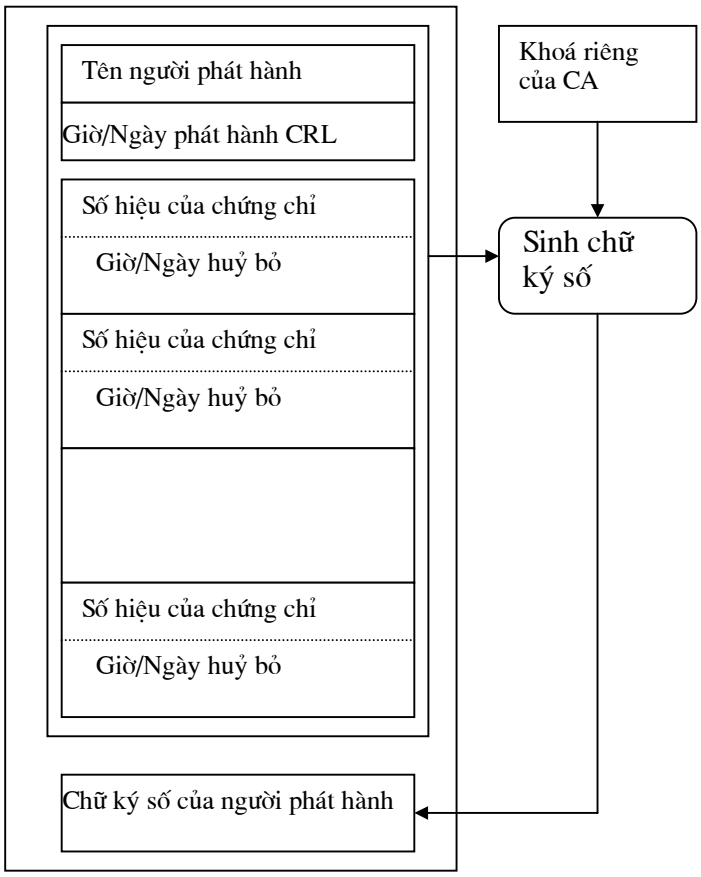
CA sẽ xác thực nguồn gốc của bất cứ yêu cầu thu hồi nào. Khi có cơ quan đăng ký địa phương, trách nhiệm tiếp nhận và phê chuẩn các yêu cầu thu hồi được uỷ thác cho các cơ quan này.

4.6.2 Danh sách các chứng chỉ bị thu hồi (CRL)

Sau khi quyết định thu hồi một chứng chỉ, CA cần làm cho những người sử dụng chứng chỉ nhận biết được sự thu hồi này. Giải pháp thông dụng nhất là có một chỉ báo về sự thu hồi, CA phát hành một cách định kỳ một cấu trúc dữ liệu được gọi là danh sách các chứng chỉ bị thu hồi (CRL). Khái niệm CRL được trình bày trong chuẩn X.509. CRL là một danh sách các chứng chỉ bị thu hồi được gán nhãn thời gian, danh sách này được CA ký và làm nó có hiệu lực đối với những người sử dụng chứng chỉ. CRL có thể phân tán, ví dụ gửi nó đến một địa chỉ Web xác định hoặc thông qua đầu vào (entry) thư mục X.500 của CA. Mỗi chứng chỉ bị thu hồi được CRL nhận dạng thông qua số hiệu của nó, mỗi chứng chỉ có một số hiệu duy nhất, số hiệu này do CA phát hành sinh ra và nó nằm trong chứng chỉ. Các thông tin chính của một CRL đơn giản được trình bày trong hình 4.7.

Khi một hệ thống sử dụng một khoá công khai được chứng thực (ví dụ để kiểm tra chữ ký số của người sử dụng khác), hệ thống sử dụng chứng chỉ không những kiểm tra chữ ký và thời gian hợp lệ của chứng chỉ mà còn phải có một CRL phù hợp gần nhất và xác thực rằng số hiệu của chứng chỉ không có trong CRL này. CRL phù hợp gần nhất không được chuẩn hoá và có thể thay đổi theo chính sách cục bộ; nhưng trong hầu hết các chính sách, điều này có nghĩa là một CRL được phát hành trong khoảng thời gian gần nhất.

Một CA phát hành các CRL thường kỳ, thời gian phát hành kế tiếp có thể tính theo giờ, ngày hoặc tuần. Khoảng thời gian này do chính sách của CA quyết định. Một CRL mới được phát hành theo từng giai đoạn khác nhau mà không cần để ý đến quyết định thu hồi mới được bổ xung thêm vào danh sách trong khoảng thời gian cuối cùng, điều này rất cần thiết, do đó một hệ thống sử dụng chứng chỉ có thể chắc chắn rằng đây là một CRL mới cập nhật. Một đặc điểm hấp dẫn của giải pháp thu hồi là các CRL có thể được phân phối cùng một cách thức như đã dùng để phân phối chứng chỉ khoá công khai, tức là thông qua truyền thông và các hệ thống máy chủ không cần đảm bảo chặt chẽ tính toàn vẹn của dữ liệu (một khi CRL đã được ký). Vì vậy, cách thức này trở nên kinh tế hơn khi cài đặt và thực hiện (ở đây không cần các máy chủ tin cậy đắt tiền hoặc các kênh truyền thông an toàn).



Hình 4.7 Danh sách các chứng chỉ bị huỷ bỏ

Một hạn chế của giải pháp này là thời gian định kỳ, nó hạn chế khoảng thời gian phát hành CRL. Ví dụ, khi có một thông báo thu hồi không được chuyển tới các hệ thống sử dụng chứng chỉ một cách tin cậy cho đến khi thời gian phát hành CRL kế tiếp bắt đầu (ví dụ, có thể khoảng 1 giờ, 1 ngày, 1 tuần hoặc lâu hơn). Lưu ý rằng, không có gì ngăn cản được một CA sinh ra và gửi đi một CRL mới ngay khi có một thu hồi mới xuất hiện (hoặc đã trở nên rõ ràng). Tuy nhiên, không gì có thể đảm bảo rằng các CRL không định kỳ (off cycle CRL) như vậy có đến được các hệ thống sử dụng chứng chỉ hay không. Ví dụ, nếu một đối tượng truy nhập trái phép xoá một off-cycle CRL từ một máy chủ không tin cậy và thay thế vào đó là một CRL đã được phát hành trước đó, tất nhiên hệ thống sử dụng chứng chỉ không thể phát hiện ra được.

4.6.3 Việc quảng bá các CRL

Một đặc tính quan trọng của giải pháp "đưa ra danh sách các chứng chỉ bị thu hồi một cách định kỳ" là nó có thể được dùng theo một chế độ, do đó hệ thống sử dụng chứng chỉ lấy lại các CRL từ một thư mục khi nó cần. Đôi khi, giải pháp này còn được gọi là một giải pháp "kéo" (pull) dành cho phân phối CRL. Một giải pháp phân phối lựa chọn là giải pháp

"đẩy" (push), trong đó một CA quảng bá các danh sách CRL cho các hệ thống sử dụng chứng chỉ (như các thông báo thu hồi mới được gửi đi). Việc quảng bá này cần sử dụng các phương tiện truyền thông có bảo vệ, như thư điện tử an toàn hoặc một giao thức giao dịch được bảo vệ. Nói cách khác, đối tượng tấn công có thể chặn và xoá bỏ các thông báo về sự thu hồi. Thuận lợi chính của giải pháp push chính là các thu hồi thiết yếu hơn (ví dụ như các thu hồi là kết quả của việc lộ khoá hoặc do lỗi của CA) có thể được phân phối một cách nhanh nhất mà không cần để ý đến thời gian định kỳ.

Tuy nhiên, còn một số vấn đề gắn liền với giải pháp này. Vấn đề thứ nhất đòi hỏi một giải pháp phân tán có bảo vệ để đảm bảo các CRL đến được các đích chủ định. Vấn đề thứ hai là sẽ sinh ra một số lượng lớn các thông tin nếu như giải pháp này được sử dụng để thông báo tất cả các thu hồi, do vậy trong thực tế, chỉ cần thông báo các thu hồi thiết yếu hơn. Vấn đề thứ ba là quyết định các huỷ bỏ nào cần được thông báo cho các hệ thống sử dụng chứng chỉ nào (trong một môi trường của cơ sở hạ tầng lớn tuỳ ý). Vấn đề thứ tư là sự ra đời của các chuẩn (dành cho các giải pháp này) làm giảm bớt việc sử dụng rộng rãi các giải pháp này.

Chương trình MISSI của Bộ quốc phòng Mỹ cung cấp một cơ sở hạ tầng khoá công khai dành cho DMS (Hệ thống thông báo dùng trong Bộ Quốc Phòng). Cơ sở hạ tầng này sử dụng giải pháp " đưa ra danh sách các thu hồi một cách định kỳ" để thông báo về các thu hồi. Tuy nhiên có thêm một giải pháp kiểu quảng bá, được sử dụng để thông báo một danh sách các thu hồi do khoá bị lộ, được gọi là danh sách khoá bị lộ (CKL). Một CKL trung tâm được duy trì cho toàn bộ mạng domain gốc. Mạng này được các CA thông báo về các khoá này. CKL được phân phối thông qua thư tín điện tử an toàn và được bảo vệ thông qua các phương tiện DMS thông thường. Với sự ra đời của khuôn dạng CRL trong phiên bản 2 của X.509 vào giữa những năm 1996, MISS đang di trú việc sử dụng đặc tính mới của X.509, đặc tính này được gọi là các CRL gián tiếp nhằm thiết lập chức năng CKL.

Trong trường hợp DMS, tất cả các vấn đề của giải pháp quảng bá được giải quyết. Tính sẵn sàng của giải pháp phân phối (được bảo vệ) không phải là một vấn đề cần quan tâm vì ứng dụng đích được hỗ trợ là thư điện tử an toàn. Nhờ đó, tất cả các hệ thống đều có truy nhập vào các dịch vụ thư điện tử an toàn. Do giải pháp quảng bá chỉ được sử dụng cho việc thông báo các khoá bị lộ và do điều này rất hiếm khi xảy ra trong môi trường được kiểm soát tốt của DMS, nên CKL chưa bao giờ có được kích thước đầy đủ. CKL được phát hành cho toàn bộ mạng.

Tuy nhiên, giải pháp CKL của MISSI không phổ biến trong các môi trường của ứng dụng khác. Nói riêng, nó không thể hỗ trợ các yêu cầu của toàn quốc và tất nhiên nó không phải là một cơ sở hạ tầng mang tính toàn cầu và thương mại mở.

4.6.4 Sự huỷ bỏ ngay lập tức

Một mối quan tâm thường xuyên đối với giải pháp "đưa ra danh sách các thu hồi một cách định kỳ" là các hệ thống sử dụng chứng chỉ không thể chấp nhận sự chậm trễ các

thông báo thu hồi vì lý do thời gian định kỳ. Tuỳ thuộc vào môi trường ứng dụng, sẽ có nhiều thiệt hại nếu khoá bị lộ trong một ngày. Trong một thế giới lý tưởng, thông tin về một chứng chỉ bị thu hồi có giá trị ngay lập tức đối với người sử dụng chứng chỉ khi anh ta muốn sử dụng chứng chỉ đó.Vì vậy, các cách thu hồi ngay lập tức cũng được quan tâm.

Với việc kiểm tra thu hồi trong thời gian thực (real-time revocation checking) và kiểm tra tình trạng trực tuyến (online status checking), một hệ thống sử dụng khoá công khai muốn xác nhận thời gian hợp lệ của một chứng chỉ (sử dụng trong một giao dịch trực tuyến với một máy chủ đang liên kết với CA phát hành). Cuộc giao dịch sẽ trả lại một thông báo về tình trạng thu hồi hiện thời của chứng chỉ. Nó phải được tiến hành an toàn, đảm bảo được tính đúng lúc và nguồn của nó cho hệ thống sử dụng khoá công khai. Các yêu cầu đặc thù này có trong từng cuộc giao dịch, khi CA sinh một chữ ký số và khi hệ thống sử dụng khoá công khai kiểm tra chữ ký số này. CA phải thực hiện các dịch vụ trực tuyến có giá trị cao, tiếp cận được tất cả những người sử dụng và dịch vụ này phải được thực hiện trong một môi trường an toàn.

Kiểm tra thu hồi trong thời gian thực có thể hiệu quả trong một số môi trường, đặc biệt trong các cộng đồng khép kín gồm các chủ thể và những người sử dụng khoá công khai. Chi phí cũng cần được quan tâm. Chi phí mua và hoạt động của các máy chủ trực tuyến tin cậy có thể rất cao. Dễ nhận thấy rằng, một máy chủ như vậy cần tạo ra chữ ký số cho mỗi cuộc giao dịch hỏi đáp và các nguồn tài nguyên cần cho quá trình xử lý mật mã có thể rất đắt. Chi phí hoạt động cho một máy chủ an toàn (gồm cả chi phí thiết lập tất cả các kiểm soát an toàn cần thiết) cũng rất cao.

Ở đây có bao nhiêu giải pháp thu hồi khác có thể giúp chúng ta đạt được mục đích "thu hồi ngay lập tức" mà không phải chịu các chi phí trong giải pháp kiểm tra thu hồi trong thời gian thực? Sau đây có một số giải pháp có thể, được đề xuất từ các nguồn khác nhau:

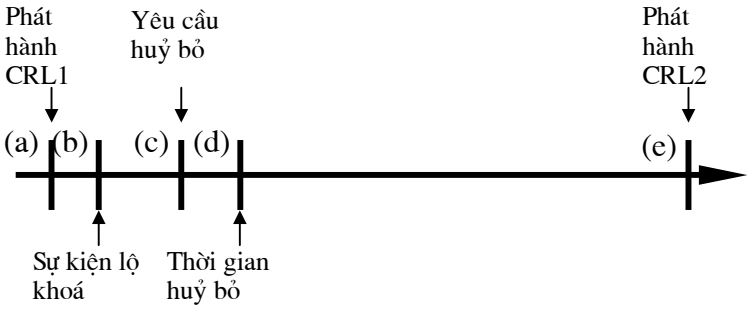
(a) Loại bỏ khỏi nơi lưu giữ (Removal from repository): Đây là một giải pháp đơn giản vì CA có thể loại bỏ ngay lập tức một chứng chỉ từ đầu vào thư mục của chủ thể khi chứng chỉ bị thu hồi; Các hệ thống sử dụng khoá công khai (có mối quan tâm riêng về tính đúng lúc) có thể lấy được một chứng chỉ mới hoàn toàn bất cứ khi nào họ muốn sử dụng một chứng chỉ. Giải pháp này rất dễ thực hiện nhưng lại không an toàn do các máy chủ thư mục và việc truyền thông với các máy chủ thư mục này không đủ tin cậy. Ví dụ, một đối tượng truy nhập trái phép có thể chèn một bản sao của chứng chỉ cũ vào kênh truyền thông trong một giao dịch với máy chủ thư mục, ngay cả khi chứng chỉ này đã bị thu hồi. Hơn nữa, việc phân phối các chứng chỉ không cần các giao thức đặc biệt, thông thường chúng được phân phối bằng cách gắn vào các thông báo được ký, các thông báo này yêu cầu phải sử dụng khoá được chứng thực trong các quá trình kiểm tra.

(b) Máy chủ hoặc thư mục lưu giữ chứng chỉ tin cậy (Trusted certificate server or directory): Để tăng cường cho giải pháp (a), chúng ta cần đảm bảo rằng máy chủ

lưu giữ chứng chỉ được thiết lập như một hệ thống tin cậy và đáp ứng giao dịch (được máy chủ này ký số) và có gắn thêm một tem thời gian. Ví dụ, một giao dịch Web có thể được sử dụng, trong đó SSL quy định phải bảo vệ đáp ứng giao dịch theo yêu cầu. Như một sự lựa chọn, các giao thức của thư mục X.500 chứa một đặc tính tuỳ chọn, được sử dụng để bảo vệ đáp ứng giao dịch. Có thể sử dụng cách này để thu được sự thu hồi ngay lập tức. Nó quy định cho tất cả các máy chủ và máy khách có thiết lập giao thức bảo vệ, hay các hệ thống sử dụng chứng chỉ có sự tin cậy, vì vậy thư mục hay các máy chủ lưu giữ chứng chỉ hoạt động tuỳ thuộc vào các điều kiện tin cậy và theo chính sách của CA. Giải pháp này không thể thoả mãn tất cả các yêu cầu, ít nhất về yêu cầu giá cả, nó tốn kém ngang với giải pháp kiểm tra huỷ bỏ trong thời gian thực.

(c) Chu kỳ phát hành CRL đủ nhỏ (Fine granularity periodic CRLs): Như đã biết, CA quyết định chu kỳ phát hành của các CRL, có thể khởi tạo khoảng thời gian này vừa đủ ngắn nhưng các thông báo thu hồi vẫn kịp thời sử dụng giải pháp CRL cơ bản mà không yêu cầu các máy chủ tin cậy hoặc các giao thức bảo vệ? Vấn đề chính ở đây không phải là tạo chu kỳ phát hành CRL một ngày, một giờ hoặc 10 phút, mà là quy định rằng các danh sách không được quá lớn (sao cho chi phí xử lý và truyền thông có thể chấp nhận được) và hệ thống thư mục có khả năng đáp ứng được việc phân phối. Thời gian định kỳ này nên phù hợp cho nhiều ứng dụng, có thể tính theo giờ hoặc thậm chí theo ngày nhưng khi một CA thông báo 'nghi ngờ lộ khoá' thì chu kỳ phát hành này trở nên vô nghĩa.

Các giải pháp thu hồi khác nhau (với các mức độ trực tiếp khác nhau) có thể có ứng dụng trong các môi trường khác nhau. Giải pháp thích hợp nhất sẽ tuỳ thuộc vào các rủi ro (được ước tính trước) và chi phí. Các giải pháp mới vẫn tiếp tục được tìm kiếm và phát triển.



Hình 4.8 Dòng thời gian hủy bỏ

4.6.5 Dòng thời gian xử lý thu hồi

Để hiểu được một số các liên kết giữa các CRL và các phát hành hợp pháp liên quan, chúng ta có thể xem xét dòng thời gian xảy ra các sự kiện trong hình vẽ 4.8.

Chuỗi sự kiện như sau:

a/ Phát hành CRL1: Một CRL được phát hành trước khi xảy ra thu hồi.

b/ Sự kiện lộ khoá: Một sự kiện xảy ra dẫn đến việc thu hồi, ví dụ có một thông báo 'nghi ngờ khoá riêng bị lộ'. Không nhất thiết phải biết chính xác thời gian nhưng cần biết khoảng thời gian của sự kiện này. Sự kiện này có thể xảy ra trước sự kiện (a).

c/ Yêu cầu thu hồi: Một người có quyền gửi một yêu cầu thu hồi tới cho CA hoặc cơ quan đăng ký địa phương (đại diện cho CA). Sự kiện này có thể xảy ra trước hoặc sau sự kiện (a).

d/ Thời gian thu hồi: CA chính thức chấp nhận thu hồi.

e/ Phát hành CRL2: CRL (có chứa chứng chỉ bị thu hồi) được phát hành và công bố.

Một chứng chỉ được sử dụng bất kỳ thời gian nào sau khi sự kiện (b) phê chuẩn một khoá công khai. Rõ ràng là, thành viên mà người sử dụng chứng chỉ mong muốn - có thể không kiểm soát được khoá riêng tương ứng, có khả năng gây thiệt hại đáng kể cho người sử dụng chứng chỉ và/hoặc đối tượng nắm giữ khoá công khai hợp pháp (thuê bao). Để giải quyết được tình trạng này, rủi ro giữa các thành viên cần được chia nhỏ. Rủi ro lớn nhất nên để thành viên có khả năng kiểm soát tốt nhất chống đỡ. Để thực hiện được điều này quả là không dễ dàng, đặc biệt từ khi tình trạng của các thành viên biến đổi tại các thời điểm khác nhau (các điểm này đã được chỉ rõ trong dòng thời gian). Ví dụ, sự thu hồi liên quan đến khoá riêng bị lộ. Các phân nhánh trong các giai đoạn khác nhau có thể là:

 Giai đoạn (b)-(c): Tình trạng lộ khoá xảy ra nhưng CA không được thông báo. Người sử dụng chứng chỉ không thể trông chờ để biết tình trạng lộ khoá. Thuê bao có thể biết hoặc không biết điều này. Đây có thể là lý do để thuê bao phải chịu rủi ro lớn (do bị lạm dụng khoá riêng) trong giai đoạn này.

 Giai đoạn (c)-(d): Tình trạng lộ khoá được thông báo nhưng CA không gửi đi một thu hồi nào. Người sử dụng chứng chỉ không thể trông chờ để biết điều này. Đây có thể là lý do CA phải chịu rủi ro lớn (do bị lạm dụng khoá riêng) trong giai đoạn này.

 Giai đoạn (d)-(e): Thông báo thu hồi chính thức được gửi đi nhưng người sử dụng chứng chỉ có thể không có cách nào biết được sự thu hồi này. Tình trạng chia nhỏ rủi ro sẽ phụ thuộc vào việc sử dụng giải pháp thu hồi nào (và có thể được thoả thuận giữa các thành viên). Với việc phát hành các CRL định kỳ, người sử dụng chứng chỉ sẽ không biết có sự thu hồi cho đến khi CRL2 được phát hành. Do có thu hồi trực tiếp, nên đây có thể là lý do ta muốn người sử dụng chứng chỉ biết được sự thu hồi trong giai đoạn này. Đây có thể là mối quan tâm hàng đầu của người sử dụng chứng chỉ - chờ cho đến khi CRL2 được phát hành mới tiến hành giao dịch hỏi đáp có sử dụng khoá.

 Giai đoạn sau (e): Lúc này, CA đã hoàn thành trách nhiệm của mình trong việc thông báo các thông tin về sự thu hồi. Do người sử dụng chứng chỉ có thể sử dụng một chứng chỉ

đã bị thu hồi trong giai đoạn này, nên cần gắn trách nhiệm cao hơn cho những người sử dụng này.

Việc giải quyết các tranh cãi về sự thu hồi cũng phụ thuộc phần lớn vào thời gian chính xác của các sự kiện. Tình trạng này được cải thiện đáng kể nếu các giao dịch được ký hoặc các thông báo có gắn nhãn thời gian tin cậy.

Nghĩa vụ của CA, thuê bao và người sử dụng chứng chỉ đối với một tình trạng thu hồi, chia nhỏ trách nhiệm pháp lý, chống lại tình trạng lộ khoá và tập trung vào việc thiết lập các hoạt động của CA và các thoả thuận giữa các thành viên, là nhất thiết phải thiết lập và thoả thuận các quy tắc rõ ràng nhằm kiểm soát các sự kiện thu hồi.

4.7 CRL theo X.509

Bổ xung thêm vào khuôn dạng chứng chỉ đã được trình bày trong mục 4.5, chuẩn X.509 của ISO/IEC/ITU cũng định nghĩa một khuôn dạng CRL chuẩn.

4.7.1 Khuôn dạng CRL

Cũng giống như khuôn dạng chứng chỉ, khuôn dạng CRL của X.509 liên tục được phát triển từ khi nó xuất hiện vào năm 1988. Nói riêng, từ khi cơ chế trường mở rộng được thêm vào chứng chỉ để tạo ra phiên bản 3, kiểu cơ chế này cũng được thêm vào CRL để tạo ra phiên bản 2 của CRL. Khuôn dạng CRL này được trình bày trong hình 4.9.

Các trường này gồm:

a/ Phiên bản (Version): Chỉ ra khuôn dạng CRL thuộc phiên bản 1 hoặc 2, tính cho cả các phiên bản trong tương lai. Đối với phiên bản 1, trường này được bỏ qua và các trường (h) và (i) không được phép.

b/ Tên thuật toán ký (Signature): Chỉ ra thuật toán được sử dụng trong khi ký CRL.

c/ Người phát hành (Issuer): Tên của cơ quan phát hành CRL này.

d/ Thời gian cập nhật hiện thời (This Update): Ngày và giờ phát hành CRL này.

e/ Thời gian cập nhật tiếp theo (Next Update): Ngày và giờ phát hành CRL tiếp theo. Đây là một trường tuỳ chọn, có thể được bỏ qua nếu tất cả những người sử dụng của CRL biết được chu kỳ phát hành. Tuy nhiên, trường này được khuyến nghị không nên bỏ qua.

f/ Số hiệu chứng chỉ của người sử dụng (User Certificate): Số hiệu của chứng chỉ bị huỷ bỏ hoặc bị treo.

g/ Ngày thu hồi (Revocation): Ngày bắt đầu có hiệu lực huỷ bỏ hoặc treo một chứng chỉ.

h/ Các trường mở rộng của CRL entry (CRL Entry Extensions): Đây là các trường bổ xung, kiểu của các trường này phải được đăng ký và có thể được gán cho mỗi mục đưa vào.

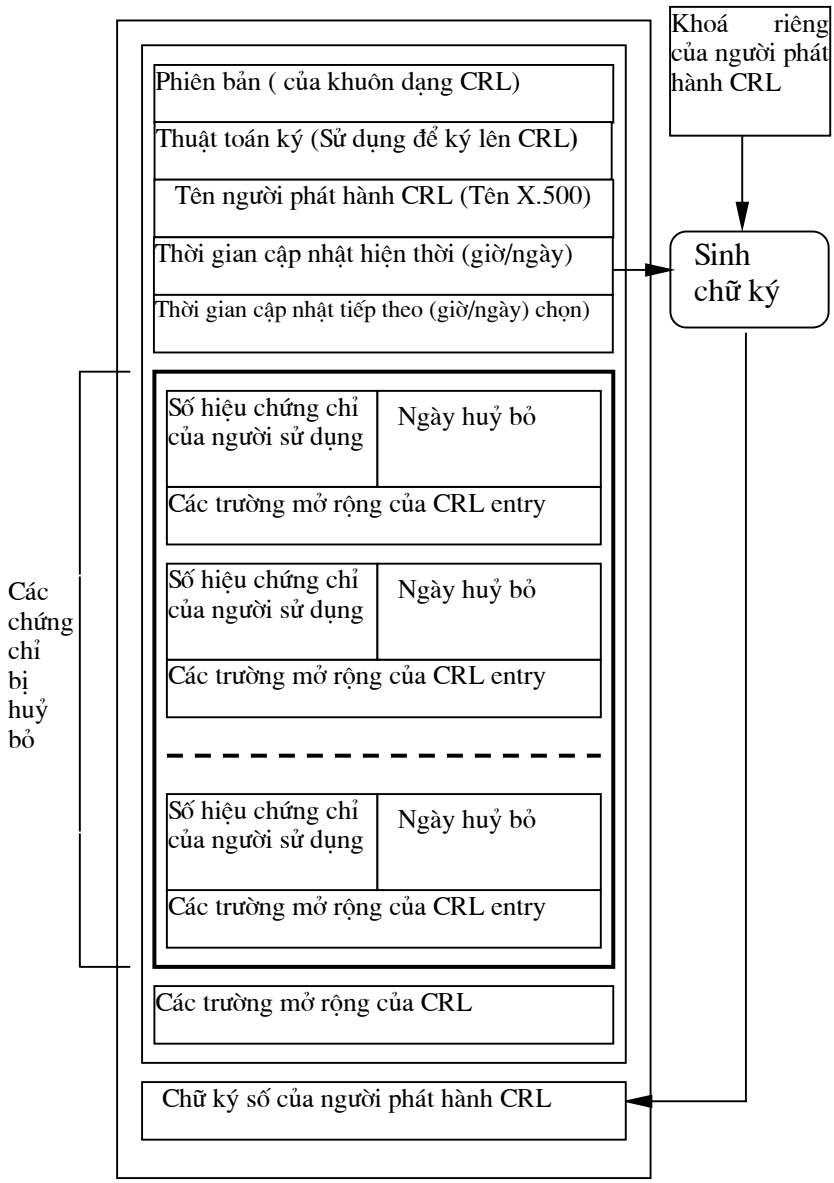
i/ Các trường mở rộng của CRL (CRL Extensions): Đây là các trường bổ xung, kiểu của các trường này phải được đăng ký và có thể được gán cho CRL đầy đủ.

Cơ chế trường mở rộng được sử dụng cho (h) và (i) tương tự với cơ chế trường mở rộng đã được sử dụng cho khuôn dạng X.509, nó cũng có chỉ báo thiết yếu.

Một tập hợp các trường mở rộng của CRL và các trường mở rộng của CRL entry được các tổ chức ISO/IEC, ITU và ANSI 19 phát triển. Chúng được công bố song song với các trường mở rộng chuẩn của chứng chỉ.

Các trường mở rộng chuẩn có thể được chia nhỏ thành các mảng sau đây:

- Các trường mở rộng chung;
- Các điểm phân tán CRL;
- Các Delta-CRL;
- Các CRL gián tiếp;
- Việc treo chứng chỉ.



Hình 4.9 Khuôn dạng CRL của X.509

4.7.2 Các trường mở rộng chung

Các trường mở rộng chung như sau:

 Số thứ tự CRL (CRL number): trường mở rộng của CRL. Trường này chứa một số thứ tự tăng dần, gán cho mỗi CRL khi nó được phát hành. Nó giúp cho người sử dụng chứng chỉ biết được nếu thiếu một trong các CRL cũ; nó cũng hỗ trợ cho đặc tính delta-CRL (xem phần sau)

 Mã lý do (Reason Code): trường mở rộng của CRL entry. Trường này đưa ra lý do của việc thu hồi chứng chỉ. Một số ứng dụng có thể sử dụng trực tiếp lý do thu hồi này bằng cách thông tin phản hồi cho người sử dụng, hoặc bằng cách phản ứng khác nhau với các lý do khác nhau.

 Ngày hết hiệu lực (Invalidity Date): trường mở rộng của CRL entry. Trường này chỉ ra ngày mà một khoá bị thu hồi vì lý do lộ.

Đối với trường mở rộng Reason code, nó có các giá trị được định nghĩa như sau:

 Lộ khoá (Key Compromise): Chứng chỉ của một thực thể cuối bị thu hồi vì lý do lộ khoá hoặc nghi ngờ lộ khoá.

 Lộ khoá của CA (CA Compromise): Chứng chỉ của một CA bị thu hồi vì lý do lộ khoá hoặc nghi ngờ lộ khoá.

 Thông tin gốc bị thay đổi (Affiliacation Changed): Tên của chủ thể hoặc các thông tin khác về chủ thể (có trong chứng chỉ) bị thay đổi.

 Chuyển nhượng (Superceded): Chứng chỉ đã được chuyển nhượng.

 Chấm dứt hoạt động (Cessation of Operation): Chứng chỉ không còn cần thiết cho mục đích ban đầu.

Trường mở rộng Reason code có hai giá trị đặc biệt:

+ Remove from CRL được trình bày trong mục Delta-CRL.

+ Certificate Hold được trình bày trong mục "Treo chứng chỉ".

Cả hai trường mở rộng: Authority Key Identifier và Issuer Alternative Name được sử dụng như các trường mở rộng của chứng chỉ (đã trình bày trong mục 4.5), cũng có thể được sử dụng như trường mở rộng của CRL. Chúng được sử dụng để nhận dạng khoá dùng khi ký và cho phép nhận dạng người phát hành CRL thông qua các dạng tên không theo tên X.500.

4.7.3 Các điểm phân tán CRL

Kích cỡ tối đa của một CRL rất quan trọng. Với các CRL được phát hành định kỳ, khi một hệ thống sử dụng một chứng chỉ, hệ thống này cần tìm về một CRL và xử lý nó (như kiểm chữ ký trên CRL đầy đủ). Nếu các CRL quá lớn, sẽ nảy sinh các vấn đề về tính hiệu quả do các chi phí truyền thông và các chi phí xử lý trong các hệ thống sử dụng chứng chỉ.

Các entry (thông tin thu hồi đưa vào danh sách) được thêm vào CRL (khi có sự thu hồi). Một entry có thể được loại bỏ khi hiệu lực của một chứng chỉ hết hạn. Tốc độ thông báo thu hồi không thể đoán trước được nhưng có một điều rõ ràng là nó phụ thuộc vào số lượng các chủ thể. Hai yếu tố chính được sử dụng để kiểm soát kích cỡ của các CRL, đó là số lượng các chủ thể và thời gian hợp lệ của một chứng chỉ.

Ở đây sẽ nảy sinh vấn đề rắc rối nếu chúng ta muốn hạn chế kích cỡ của các CRL bằng cách rút ngắn thời gian tồn tại của một chứng chỉ thì sẽ vấp phải các vấn đề như chi phí hoạt động cao, sự bất tiện cho người sử dụng và không gian lưu trữ cho các nguồn tài nguyên lưu trữ lớn hơn.

Trong các phiên bản của X.509 vào năm 1988 và 1993, mỗi CA có hai CRL: một CRL cho tất cả các chủ thể của người sử dụng cuối, một CRL cho các CA khác và cả hai đều được chứng thực. CRL sau được kỳ vọng là rất ngắn (thường là trống rỗng). Điều này rất có giá trị vì nó làm giảm các chi phí xử lý CRL khi kiểm tra đường dẫn chứng thực. Tuy nhiên, ở đây vẫn còn một mối quan tâm là CRL dành cho chứng chỉ của người sử dụng cuối phải bao trùm lên toàn bộ số lượng người sử dụng cuối của một CA. Ở đây sẽ nảy sinh vấn đề rắc rối nếu số lượng những người sử dụng cuối này lên tới hàng ngàn, hàng triệu hoặc hàng tỷ. Như vậy rủi ro sẽ tăng nếu CRL của người sử dụng cuối có quy mô không phù hợp.

Vấn đề này đã được giải quyết trong phiên bản 3 của chứng chỉ và phiên bản 2 của CRL. Các khuôn dạng mới này có thể chia nhỏ các chứng chỉ của một CA thành một số nhóm riêng, mỗi nhóm riêng liên kết với một điểm phân tán CRL. Vì vậy, kích cỡ tối đa của một CRL có thể nhỏ hơn và CA có thể kiểm soát được kích cỡ này. Các điểm phân tán CRL có thể được nhận dạng thông qua một trong các dạng tên/địa chỉ sau: các tên X.500, các URL hoặc các địa chỉ thư tín điện tử.

Các trường mở rộng của X.509 cũng cho phép tồn tại các điểm phân tán CRL riêng lẻ (tuỳ thuộc vào các lý do thu hồi khác nhau), với các thu hồi thông thường (ví dụ do việc thay đổi tên) có thể được xếp vào một CRL khác so với các thu hồi do lộ khoá. Tuỳ thuộc vào môi trường ứng dụng và chính sách, một số ứng dụng chỉ được phép kiểm tra danh sách các thu hồi do lộ khoá. So với các CRL thông thường, danh sách các thu hồi do lộ khoá được cập nhật thường xuyên hơn. Chúng ta có thể tạo ra một cơ sở hạ tầng, trong đó kích cỡ của các CRL bao trùm lên các tình trạng lộ khoá có thể được giữ ở mức nhỏ và các CRL này được phát hành với chu kỳ ngắn hơn, ví dụ như tính theo giờ hoặc thậm trí thường xuyên hơn. Với các danh sách thu hồi thông thường, nếu kích cỡ của chúng quá lớn, có thể phát hành chúng với chu kỳ dài hơn, ví dụ tính theo ngày.

Các trường mở rộng được định nghĩa như sau:

- Các điểm phân tán CRL (CRL Distribution Points): là trường mở rộng của chứng chỉ, nó nhận dạng một hoặc nhiều điểm phân tán CRL, các điểm phân tán này phân tán các CRL khi xuất hiện một thông báo về một chứng chỉ bị thu hồi. Để có thể kiểm tra thu hồi, một hệ thống sử dụng chứng chỉ phải tìm kiếm và kiểm tra một

CRL từ một trong các điểm phân tán hoặc từ một nguồn khác, ví dụ như từ đầu vào thư mục của CA phát hành. Một điểm phân tán có thể phân tán một CRL chứa các thông báo thu hồi (không quan tâm đến các lý do thu hồi), hoặc nó có thể phân tán một CRL chứa các entry thu hồi (dành cho một tập hợp có hạn các lý do thu hồi). Trường mở rộng này không cần lật cờ thiết yếu. Nếu một hệ thống sử dụng chứng chỉ không chấp nhận trường này, hệ thống chỉ nên chấp nhận chứng chỉ nếu hệ thống có thể kiểm tra tình trạng thu hồi bằng cách khác.

 Issuing Distribution Points: là một trường mở rộng của CRL, nó chỉ ra tên của các điểm đã phân tán CRL riêng biệt này và chỉ cho biết, có lưu giữ hay không lưu giữ danh sách các chứng chỉ bị thu hồi của thực thể cuối, của CA hoặc các chứng chỉ bị thu hồi do một tập hợp hữu hạn các lý do. Tất cả các trường này cần nằm trong phần được ký của CRL và người sử dụng cần kiểm tra nó, ngăn không cho những đối tượng tấn công thay thế CRL giả tại một điểm phân phối. Ví dụ, nếu không có các kiểm tra này, tại điểm phân tán B một đối tượng tấn công có thể thay thế một CRL rỗng từ điểm phân tán A bằng một CRL không rỗng, và vì vậy một số chứng chỉ bị thu hồi lại trở thành hợp lệ. CRL được người phát hành CRL ký (thông thường, các CA tự làm điều này) các điểm phân tán CRL không có các cặp khoá của riêng mình.

4.7.4 Các Delta-CRL

Sử dụng Delta-CRL là cách giảm kích cỡ của các CRL. Delta-CRL là danh sách các thay đổi xảy ra từ khi phát hành CRL trước và danh sách này được ký. Các Delta-CRL được thiết kế để giảm các chi phí truyền thông cho các hệ thống. Delta-CRL có thể duy trì các cơ sở dữ liệu (của riêng nó) chứa các thông tin về chứng chỉ bị hủy bỏ. Các Delta-CRL được sử dụng để cập nhật tình trạng hiện thời của cơ sở dữ liệu mà không cần cho việc xử lý một CRL rỗng. Trong chế độ này, việc thực hiện đòi hỏi sử dụng các phương tiện lưu giữ an toàn, nên khó có thể thực hiện trong môi trường máy tính để bàn, nhưng có thể thích hợp trong một môi trường máy chủ lớn.

Việc sử dụng các Delta-CRL phụ thuộc vào một trường mở rộng của CRL là trường Delta-CRL Indicator, nó nhận diện một Delta-CRL. Delta-CRL chỉ chứa các cập nhật mới của CRL tính từ thời điểm phát hành CRL trước. Trường này chứa số hiệu của CRL gốc và chỉ chứa các thay đổi của CRL này chứ không lưu toàn bộ danh sách các thu hồi của nó.

Các Delta-CRL cũng sử dụng một giá trị đặc biệt trong trường mở rộng Reason code. Giá trị Remove from CRL cho biết cần loại bỏ một đầu vào (entry) xuất hiện trong CRL gốc do thời gian hợp lệ của nó đã hết hoặc ngừng treo một chứng chỉ.

4.7.5 Các CRL gián tiếp

Đặc tính của một CRL gián tiếp là cho phép một CRL được phát hành thông qua một cơ quan khác. Hệ quả quan trọng nhất của đặc tính này là một CRL có thể chứa các thu hồi của nhiều CA.

Đặc tính quan trọng này có thể mang lại hiệu quả do giảm được số lượng các CRL. Các sử dụng đặc thù gồm có:

(a) Trong một cộng đồng có nhiều CA, các thông báo thu hồi do lộ khoá (khác với các thu hồi thông thường, ví dụ như thu hồi do thay đổi tên, .v.v) có thể được đưa vào trong danh sách dành cho toàn bộ cộng đồng. Danh sách này cần được phân tán, kiểm tra thường xuyên và kích cỡ của nó không nên quá lớn.

(b) Khi xử lý một đường dẫn chứng thực bất kỳ, mọi chứng chỉ trên đường dẫn này được kiểm tra thông qua một CRL. Việc tạo ra CRL gián tiếp (có chứa tất cả các chứng chỉ bị thu hồi của CA) đã cải thiện đáng kể hiệu quả trong một xí nghiệp lớn hoặc trong một cộng đồng.

Các CRL gián tiếp được chỉ ra bằng cách sử dụng các trường mở rộng của chứng chỉ và trường CRL Distribution Points. Trường mở rộng CRL Distribution Points là trường tuỳ chọn, được sử dụng để nhận diện người phát hành CRL (người phát hành CRL này khác với những người phát hành chứng chỉ). Trường này (được người phát hành chứng chỉ ký) dùng như một phương tiện để người phát hành chứng chỉ ủy quyền cho người phát hành CRL đưa ra các thông báo thu hồi. Điều này rất quan trọng bởi người sử dụng chứng chỉ có thể kiểm tra bất kỳ một CRL nào khi chúng được ký bởi người phát hành CRL uỷ quyền.

Trong một CRL gián tiếp, một chỉ báo đặc biệt được thiết lập trong trường mở rộng Issuing Distribution Point. Nó cho biết người sử dụng chứng chỉ cần kiểm tra người phát hành chứng chỉ đối với mọi entry có trong CRL. Anh ra không thể tin tưởng rằng, người phát hành CRL phát hành tất cả các entry (gắn liền với các chứng chỉ) như với các CRL thông thường. Để hỗ trợ chức năng này, một trường mở rộng của CRL entry được bổ xung thêm và được định nghĩa như sau:

 Certificate Issuer: Trường này chỉ ra người phát hành chứng chỉ tương ứng (đối với mỗi CRL entry). Nếu trường này không xuất hiện trong entry đầu tiên của một CRL gián tiếp, đối với entry này, người phát hành chứng chỉ mặc định là người phát hành CRL. Trên các entry tiếp theo của một CRL gián tiếp, nếu trường này không xuất hiện, người phát hành chứng chỉ được mặc định là người phát hành chứng chỉ dành cho entry trước đó. Các quy tắc ngầm định là một cách thích hợp để tạo ra một CRL gián tiếp.

4.7.6 Treo chứng chỉ

Đôi khi, một câu hỏi được đặt ra là "có nên huỷ bỏ một chứng chỉ hay không?". Ví dụ, giả thiết rằng có một nhà băng hoạt động như là một CA đối với các khách hàng của nó và giả thiết rằng, có một hệ thống giám sát tự động, hệ thống này phát hiện các hoạt động khả nghi trong tài khoản của một khách hàng nào đó và sẽ thông báo nếu xảy ra tình trạng lộ khoá riêng của khách hàng. Trong các trường hợp như vậy, nhà băng có thể không muốn huỷ bỏ chứng chỉ của khách hàng vì nó có thể ảnh hưởng đến mối quan hệ với khách hàng, rồi sau đó phải tiến hành cấp lại chứng chỉ không cần thiết. Tuy nhiên, người sử dụng chứng

chỉ này cần phải được thông báo về tình trạng này và thậm chí, họ phải chịu trách nhiệm cho việc tin cậy chứng chỉ này.

Để thoả mãn các yêu cầu này, uỷ ban ANSI 19 đưa ra một cơ chế treo chứng chỉ. Trong CRL có một mục, có thể là "held" (bị treo). Tình trạng của entry trong CRL có thể được chuyển thành '"revoked" (bị thu hồi) hoặc entry dành cho chứng chỉ có thể bị loại bỏ hoàn toàn khỏi CRL (ngừng treo).

Tình trạng treo được thông báo qua một giá trị đặc biệt, Certificate Hold, giá trị này nằm trong trường Reason code (đây là một trường mở rộng của CRL entry). Ở đây có thêm một trường mở rộng của CRL entry (liên quan đến việc treo chứng chỉ), đó là:

 Mã chỉ dẫn (Instruction code): Trường này cung cấp tên của một chỉ dẫn đã được đăng ký. Chỉ dẫn đưa ra hoạt động cần phải thực hiện khi gặp một chứng chỉ bị treo. Các chỉ dẫn có thể là "liên lạc với CA trước khi sử dụng chứng chỉ " hoặc "tái sở hữu thẻ/thẻ bài của người sử dụng".

4.8 Cặp khoá và thời hạn hợp lệ của chứng chỉ

Như đã biết, các cặp khoá (được sử dụng cho các mục đích khác nhau) sẽ được cập nhật định kỳ. Đây là cách hiệu quả để hạn chế các cửa sổ thời gian trong các tấn công thám mã và hạn chế lộ khoá trong một khoảng thời gian định trước. Các chứng chỉ cần có các thời gian hợp lệ, chúng phản ánh thời gian tồn tại của các khoá công khai được chứng thực.

Khoảng thời gian hợp lệ của một chứng chỉ cho người sử dụng chứng chỉ (đây là một thành viên tin cậy) biết, trong khoảng thời gian này:

a/ Khoá công khai là hợp lệ, có thể sử dụng khoá này cho các mục đích xác định.

b/ Khoá công khai và các thông tin khác trong chứng chỉ (đặc biệt là thông tin nhận dạng) là hợp lệ.

c/ Các thông báo về sự thu hồi sẽ được CA phát hành.

Giả thiết rằng, các cặp khoá được cập nhật định kỳ, chúng ta hãy xem mối quan hệ giữa khoảng thời gian hợp lệ của chứng chỉ và khoảng thời gian trong đó một cặp khoá cho trước (gồm khoá công khai và khoá riêng) được sử dụng. Các cặp khoá được sinh ra tuỳ thuộc vào mục đích sử dụng nó.

4.8.1 Các cặp khoá liên quan đến mã hoá

Với một cặp khoá được sử dụng cho các mục đích mã hoá và thiết lập khoá mã, khoá công khai chỉ nên được sử dụng trong khoảng thời gian hợp lệ của một chứng chỉ. Nếu khoá công khai được sử dụng (chẳng hạn được một hệ thống mã hoá sử dụng) mà không kiểm tra sự hợp lệ chứng chỉ, người nhận dữ liệu sẽ gặp rủi ro, làm ảnh hưởng đến sự tin cậy. Khoảng thời gian - trong đó một khoá riêng tương ứng được sử dụng (ví dụ, được một hệ thống giải mã sử dụng) hơi khác một chút. Ví dụ, khoá riêng có thể được sử dụng để giải mã trong

một khoảng thời gian dài sau khi tất cả các chứng chỉ (có khoá công khai tương ứng) đã hết hạn, đây là một vấn đề cục bộ dành cho đối tượng nắm giữ khoá riêng.

4.8.2 Các cặp khoá dùng cho ký số

Với một cặp khoá được sử dụng cho các mục đích ký số, xuất hiện hai tình trạng sau:

a/ Sự phê chuẩn mang tính thời điểm: Trong một số tình huống, người sử dụng chứng chỉ (là người kiểm tra chữ ký hoặc thành viên tin cậy) không quan tâm đến các thu hồi chứng chỉ xảy ra trước thời điểm một chữ ký được tạo ra bằng khoá riêng. Nói riêng, trong trường hợp chống chối bỏ cần lưu giữ bằng chứng (một tập hợp đầy đủ các thông tin về tình trạng của chứng chỉ kết hợp với một chữ ký, có nghĩa là tất cả các chứng chỉ trong chuỗi có thể được áp dụng, cộng với các CRL hoặc các thông tin khác về tình trạng thu hồi), bằng chứng này tồn tại ở thời điểm ký, không quan tâm đến các thu hồi xảy ra sau thời điểm ký. Trong trường hợp này, khoảng thời gian hợp lệ của chứng chỉ không cần kéo dài hơn khoảng thời gian sử dụng của khoá riêng.

b/ Sự phê chuẩn trong thời gian thực : Trong một số trường hợp khác, người sử dụng chứng chỉ cần quan tâm đến các thông báo thu hồi xảy ra trước thời điểm kiểm tra chữ ký, không chú ý đến thực tế là quá trình ký có thể đã xảy ra tại một thời điểm quan trọng nào đó trước đó. Ví dụ về các trường hợp này là khi kiểm tra một chữ ký của người phát hành phần mềm trên một bản sao phần mềm, bản sao này được phân phối điện tử từ một máy chủ Internet, khi kiểm tra một chữ ký của CA trên một chứng chỉ khoá công khai; hoặc khi kiểm tra một tem thời gian của một máy chủ có gán nhãn thời gian trên một tài liệu của thành viên thứ ba. Trong các trường hợp này, thông thường người kiểm tra chữ ký muốn kiểm tra xem, chứng chỉ hiện tại có hợp lệ và có bị thu hồi hay không. Khi đó, khoảng thời gian hợp lệ của chứng chỉ nói chung kéo dài hơn một chút so với khoảng thời gian sử dụng khoá riêng cho mục đích ký.

Tình huống (b), đôi khi có lợi cho các chứng chỉ khoá công khai có mang theo một chỉ báo về khoảng thời gian đối với khoá riêng mà trong khoảng thời gian này, mọi sử dụng khoá riêng cho mục đích ký đều hợp lệ (lưu ý rằng khoảng thời gian này có thể ngắn hơn một chút so với khoảng thời gian hợp lệ của chứng chỉ). Để đáp ứng mục đích này, chứng chỉ trong phiên bản 3 của X.509 có chứa một trường mở rộng được gọi là trường Private-key Usage Period.

Đôi khi, trường này có thể tạo thêm sự an toàn cho người sử dụng khoá công khai. Chúng ta quan tâm đến một trường hợp, trong đó một cặp khoá (được sử dụng để ký số) được cập nhật hàng năm (có nghĩa là khoá riêng chỉ được sử dụng trong vòng một năm), nhưng thời hạn phát hành các chứng chỉ (có khoá công khai tương ứng) kéo dài hai năm (vì CA cam kết sẽ thông báo về các tình trạng thu hồi của chứng chỉ trong 2 năm). Trong trường hợp này, khoảng thời gian hợp lệ của một chứng chỉ là 2 năm, nhưng trường Private-key Usage Period chỉ cho phép sử dụng khoá riêng chỉ trong năm đầu tiên. Tuỳ thuộc vào ứng dụng, điều này có thể làm giảm bớt tình trạng lộ khoá riêng. Một số ứng dụng có thể áp dụng một

kiểm tra độc lập như sau: chỉ chấp nhận các chữ ký được sinh ra trong khoảng thời gian hợp lệ của khoá riêng. Ví dụ, khoá riêng của năm 1995 bị lộ. Một đối tượng nào đó chỉ có thể làm giả các chữ ký năm 1995, mặc dù chứng chỉ vẫn được lưu hành trong năm 1995 và năm 1996.

4.8.3 Cặp khoá dùng cho mục đích ký của CA

Thực chất, cặp khóa dùng để ký của CA là chỉ một trong các trường hợp về các cặp khoá dùng cho mục đích ký số. Tuy nhiên, chữ ký của chứng chỉ có khả năng làm cầu nối giữa hai viễn cảnh chữ ký số nêu trong mục trên. "Sự phê chuẩn mang tính thời điểm" sẽ được sử dụng để giải quyết các tranh cãi. Tuy nhiên, sự phê chuẩn hiện thời cũng rất cần thiết. Những người sử dụng chứng chỉ thường yêu cầu và có quyền nhận được các thông tin thu hồi mới nhất đối với tất cả các chứng chỉ đang được sử dụng tích cực của CA. Vì vậy, việc sử dụng trường Private-key Usage Period có thể là cách thích hợp cho các CA nhằm hạn chế lộ khoá (và hạn chế trách nhiệm pháp lý).

Lưu ý rằng, thời gian tồn tại hợp lệ của một chứng chỉ khoá công khai không những bị hạn chế bởi khoảng thời gian hợp lệ đã công bố, mà còn bị hạn chế bởi tính hợp lệ của chữ ký của CA. Vì vậy, một CA cần đảm bảo rằng, thời gian hợp lệ cho khoá công khai của CA (và chứng chỉ tương ứng nào đó) kéo dài hơn thời gian hợp lệ định trước của chứng chỉ bất kỳ khi nó đang ký.

4.9 Chứng thực thông tin uỷ quyền

Mục đích cơ bản của một chứng chỉ khoá công khai là gắn một khoá công khai với một người, một thiết bị hoặc một thực thể bằng cách đưa tên hoặc các thông tin nhận diện khác vào chứng chỉ. Khi sử dụng khoá công khai để kiểm tra một chữ ký số, đôi khi người ta cũng cần sử dụng các thông tin khác về người ký trước khi đặt sự tin cậy vào chữ ký và để biết chắc rằng, người ký có được phép ký theo một mục đích riêng biệt hay không. Ví dụ:

 Một cá nhân riêng biệt có thể được một công ty uỷ quyền để chi tiêu một lượng đôla (theo quy định) hay không? Có được quyền ký hay không?

 Đây có phải là chữ ký của người có quyền ký trên thông báo hồi âm của bản kê khai thuế?

 Đây có phải là chữ ký của người có quyền chứng thực sự hợp pháp của file phần mềm nhận được hay không? (như một dạng bảo vệ bản quyền phần mềm).

Việc phân tán các thông tin uỷ quyền cũng có thể thực hiện được nhờ dùng các chứng chỉ, một cơ quan (được công nhận) có thể phát hành một chứng chỉ để công bố một người hoặc đối tượng nào đó có quyền sở hữu các đặc quyền riêng. Phần còn lại của mục này sẽ trình bày các cách phân tán thông tin uỷ quyền thông qua các chứng chỉ.

4.9.1 Thông tin uỷ quyền trong các chứng chỉ X.509

Trong một môi trường, các chứng chỉ khoá công khai được sử dụng để gắn kết các khoá công khai với người, thiết bị hoặc các thực thể khác, các chứng chỉ như nhau cũng có thể có chuyển các thông tin uỷ quyền về chủ thể của chứng chỉ. Trong thực tế, một số trường mở rộng của chứng chỉ X.509 đều mang các thông tin uỷ quyền; ví dụ, trường ràng buộc cơ bản (Basic Constraint field) uỷ quyền cho các thực thể cụ thể hoạt động như các CA. Rõ ràng là các chứng chỉ đều chứa thông tin uỷ quyền của chủ thể, ví dụ, các thuộc tính trong trường "Subject Directory Attributes" hoặc các trường mở rộng phi chuẩn được được định nghĩa đặc biệt cho mục đích này.

Tuy nhiên, ở đây có hai lý do lý giải tại sao nên sử dụng các chứng chỉ khoá công khai để chuyển thông tin uỷ quyền.

 Thông thường, người có thẩm quyền (người thích hợp nhất cho việc chứng thực nhận dạng của người có liên kết với một cặp khoá) không thích hợp cho việc chứng thực thông tin uỷ quyền. Ví dụ, bộ phận an toàn của một tổ chức có thể chỉ là người có thẩm quyền, anh ta thích hợp cho việc chứng thực: quyền được ký thay mặt cho công ty. Đôi khi, "việc chia nhỏ trách nhiệm" là một yêu cầu chính sách của một công ty.

 Động lực của hai kiểu chứng thực có thể không tương thích với nhau. Ví dụ, trong một tổ chức, những người được uỷ quyền để thực hiện một chức năng đặc thù nào đó có thể được thay đổi hàng tháng, hàng tuần hoặc thậm chí hàng ngày. Tuy nhiên, các chứng chỉ khoá công khai thường được thiết kế với thời gian tồn tại kéo dài hàng năm hoặc nhiều hơn. Việc thu hồi và tái phát hành các chứng chỉ khoá công khai thường xuyên rất cần thiết khi thay đổi các uỷ quyền. Điều này ảnh hưởng rất nhiều đến các tính hiệu quả của một hệ thống chứng chỉ khoá công khai.

Ở đây có một số trường hợp, trong đó các vấn đề trên không được áp dụng và việc thực thi hệ thống có thể tận dụng các điểm mạnh của chứng chỉ khoá công khai để chuyển thông tin uỷ quyền. Một ví dụ rõ ràng là trong Bộ quốc phòng Mỹ, các trường của chứng chỉ khoá công khai được sử dụng để chuyển các thông tin ở một mức thông tin an toàn nào đó đối với chủ thể của chứng chỉ. CA có thể được tin cậy một cách dễ dàng, do đó nó có thể chứng thực độ chính xác của thông tin ở một mức an toàn nào đó và, do các thông tin này không thay đổi thường xuyên nên khó có thể gây ra các vấn đề liên quan đến sự thay đổi của toàn bộ hệ thống chứng chỉ.

4.9.2 Các chứng chỉ thuộc tính

Thừa nhận rằng, các chứng chỉ khoá công khai không phải lúc nào cũng là phương tiện tốt nhất cho việc phân tán thông tin uỷ quyền. Vì thế, uỷ ban ANSI 19 phát triển một giải pháp lựa chọn, gọi là chứng chỉ thuộc tính. Giải pháp này hợp nhất các chuẩn của ANSI 19 với X.509. Một chứng chỉ thuộc tính ràng buộc một hoặc nhiều phần thông tin thuộc tính với chủ thể của chứng chỉ. Một người bất kỳ có thể định nghĩa, đăng ký các kiểu thuộc tính và sử dụng chúng trong các chứng chỉ thuộc tính. Một chứng chỉ được ký số và phát hành

thông qua một cơ quan cho phép gán thuộc tính. Ngoài sự khác nhau về nội dung, một chứng chỉ thuộc tính được quản lý theo cách như đã được sử dụng để quản lý chứng chỉ khoá công khai. Nói riêng, cơ chế thu hồi dựa vào CRL của X.509 được cơ quan cho phép gán thuộc tính sử dụng để thu hồi các chứng chỉ thuộc tính.

Các trường có trong một chứng chỉ thuộc tính như sau:

a/ Phiên bản (Version) dùng để thông báo của khuôn dạng chứng chỉ (ban đầu là phiên bản 1), có thể sử dụng cho các phiên bản trong tương lai.

b/ Chủ thể (Subject): Trường này nhận dạng người hoặc thực thể với các thuộc tính liên quan. Thông tin nhận diện này có thể là tên hoặc chỉ dẫn đến chứng chỉ khoá công khai (chỉ dẫn này gồm tên người phát hành và số hiệu chứng chỉ của X.509).

c/ Người phát hành (Issuer): Tên của bộ phận hay cơ quan cho phép gán thuộc tính phát hành chứng chỉ thuộc tính này.

d/ Tên thuật toán ký (Signature): được sử dụng để ký chứng chỉ.

e/ Số hiệu (Serial Number): số hiệu duy nhất dành cho chứng chỉ này, số hiệu này được cơ quan cho phép gán thuộc tính gán cho, nó được sử dụng trong một CRL để nhận dạng chứng chỉ này.

f/ Thời gian hợp lệ (Validity): Ngày/giờ bắt đầu có hiệu lực và hết hạn của một chứng chỉ. Trường này định rõ thời gian tồn tại hợp lệ của chứng chỉ, trừ khi chứng chỉ bị thu hồi trước thời hạn kết thúc của nó.

g/ Các thuộc tính (Attributes): Thông tin liên quan đến thực thể (được nói đến trong trường owner) hoặc thông tin liên quan đến xử lý chứng thực. Các thông tin này có thể được chủ thể, cơ quan cho phép gán thuộc tính hoặc thành viên thứ ba cung cấp, tuỳ thuộc vào kiểu thuộc tính đặc thù.

h/ Tên duy nhất của người phát hành (Issuer Unique Identifier): Là một chuỗi tuỳ chọn, được sử dụng để chỉ ra một cách rõ ràng tên cơ quan cho phép gán thuộc tính.

i/ Các mở rộng (Extensions): Trường này cho phép bổ xung thêm các trường mới vào khuôn dạng của chứng chỉ. Cơ chế bổ xung các trường mở rộng giống với cơ chế được sử dụng trong chứng chỉ khoá công khai của X. 509.

Các chứng chỉ thuộc tính tạo thành một cơ chế mục đích chung, có nhiều sử dụng. Sự phân tán các thông tin uỷ quyền (được chứng thực) là một trong các sử dụng này. Để hỗ trợ việc sử dụng các chứng chỉ thuộc tính, ANSI 19 đang phát triển một chuẩn, trong đó định nghĩa một tập hợp các thuộc tính liên quan đến việc uỷ quyền, phù hợp với các chứng chỉ thuộc tính. Chuẩn này cũng mô tả cách để có thể chuyển thông tin thuộc tính nằm trong các tài liệu được ký và cách để một người kiểm tra chữ ký có thể theo dõi hai tập hợp thông tin thuộc tính nếu một chữ ký mang sự uỷ quyền thích hợp.

Ví dụ, nếu một tài liệu (đã được ký) có một giá trị thuộc tính và giá trị thuộc tính này tương ứng với một mức chi tiêu của một tổ chức là $100,000 và nếu chứng chỉ thuộc tính của người ký chỉ báo rằng, tổ chức này cho phép người ký chỉ được ký đến $10,000 thì khi một thành viên bên ngoài nhận được tài liệu đã được ký, anh ta có thể suy luận ra đây không phải là sự uỷ quyền thích hợp.

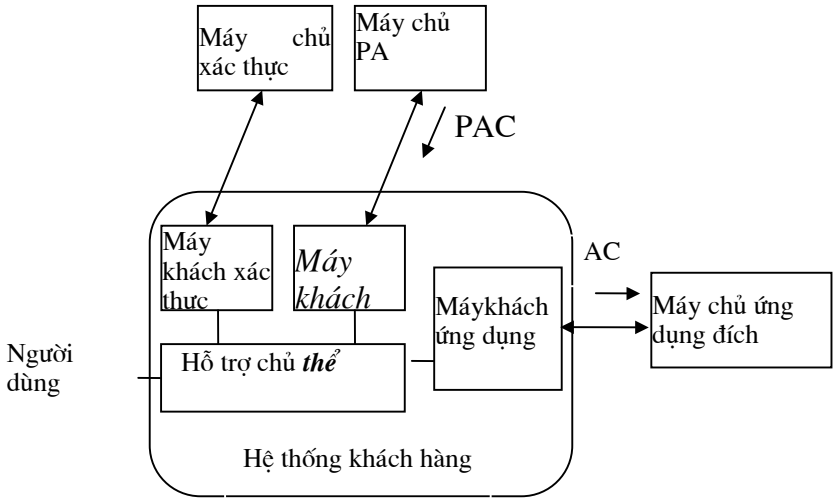
Các chứng chỉ thuộc tính đặc trưng cho một mảng rất quan trọng, đó là kỹ thuật thương mại điện tử, mảng này đang được phát triển và khai thác triệt để.

4.9.3 Các chứng chỉ thuộc tính đặc quyền

Khái niệm "phân tán thông tin uỷ quyền được chứng thực" đã được sử dụng từ đầu những năm 1990 trong môi trường hơi khác một chút. Trong môi trường này, các nhà cung cấp phân tán tính toán theo mô hình khách- chủ. Hình thức phân tán thông tin uỷ quyền này được ECMA (Hội các nhà sản xuất máy tính Châu Âu) xây dựng đầu tiên, sau đó nó bị ảnh hưởng gần như hoàn toàn vào các thiết kế hệ thống của OSF, OSF/DCE và dự án SESAME.

Hình thức này giải quyết vấn đề là một người sử dụng máy tính tương tác truy nhập vào các phương tiện của nhiều hệ thống máy chủ, do các hệ thống này hỗ trợ nhiều ứng dụng cần thiết. Các tổ chức khác nhau điều hành các hệ thống máy chủ này. Cấu hình được minh hoạ trong hình 4.10. Việc xác thực sử dụng kỹ thuật xác thực máy khách-máy chủ, cơ chế Kerberos. Cơ chế này như sau: Bên máy khách tiến hành trao đổi trực tuyến với một máy chủ xác thực. Sau khi xác thực (hoặc cùng kết hợp xác thực), phía máy khách tiến hành trao đổi trực tuyến với một máy chủ thuộc tính đặc quyền (PAserver) để có được một chứng chỉ thuộc tính đặc quyền (PAC). PAC có chứa các thông tin uỷ quyền của người sử dụng. Sau đó, PAC được chuyển tới các máy chủ ứng dụng đích, máy khách thay mặt cho người sử dụng truy nhập vào các máy chủ này. Máy chủ đích sử dụng PAC để ra các quyết định như: người sử dụng có yêu cầu có thể truy nhập vào các tài nguyên nào và các dạng truy nhập nào thì được phép.

PAC là một cấu trúc dữ liệu, cấu trúc này được một máy chủ tin cậy sinh ra trong domain của người sử dụng, nó gắn thông tin đặc quyền (hoặc uỷ quyền) vào thông tin nhận dạng của người sử dụng này hoặc phiên đăng nhập, theo một dạng có thể được chứng thực thông qua các máy chủ đích mà anh ta muốn truy nhập vào. Thông tin đặc quyền đầu tiên liên quan đến việc kiểm tra người sử dụng có thể là một thành viên trong một nhóm riêng biệt (ví dụ, một thành viên trong nhóm tái thiết kế các hệ thống quản trị của công ty thép Sharon), hoặc có một vai trò riêng (người được uỷ quyền ký). Mô hình này có thể được mở rộng ra nhiều mô hình uỷ quyền khác, ví dụ mô hình an toàn kiểu quân sự.



Hình 4.10 Kiểm soát truy nhập và xác thực khách- chủ của ECMA

Một PAC được bảo vệ, cho nên một máy chủ đích khi nhận được PAC có thể tin tưởng rằng chứng chỉ:

- được tạo ra từ một nguồn chính xác;
- không bị sửa đổi trong quá trình phân phối;
- không bị một đối tượng nào khác xem xét trừ người giữ hợp lệ.

Trong các môi trường này, các thiết kế ban đầu đều sử dụng mật mã đối xứng. Trong các phát triển mới đây, các kỹ thuật khoá công khai và chữ ký số đã được giới thiệu từng bước và người ta có thể nhận thức được một PAC là một cấu trúc được ký số, cấu trúc này gắn các thông tin đặc quyền vào một tập thông tin nhận dạng. Do vậy, sự tương thích giữa các PAC và các chứng chỉ thuộc tính hướng xác thực (được ANSI 19 phát triển) ngày càng tăng.

4.9.4 Cơ sở hạ tầng an toàn được phân tán đơn giản

Vào năm 1996, Ron Rivest và Butler Lampson đưa ra một đề xuất về việc thiết kế chứng chỉ khoá công khai, được gọi là cơ sở hạ tầng an toàn được phân tán đơn giản (SDSI). Giải pháp SDSI không nhất trí với sự phức tạp ngày càng nhiều của X.509 và cho rằng, nó cần đơn giản hơn để có thể đáp ứng nhiều môi trường ứng dụng. SDSI định nghĩa một tập hợp nhỏ chức năng của X.509, bỏ qua một số đặc tính phức tạp của X.509, ví dụ các chính sách của chứng chỉ, các ràng buộc và quản lý vòng đời của khoá. Một môi trường ứng dụng đơn giản hơn có thể thực hiện mà không cần các đặc tính này. Nó sử dụng cách biểu diễn và cú pháp mã đơn giản hơn, được ký hiệu là ASN.1 và sử dụng trong X.509.

SDSI cũng định rõ một cách sắp xếp cấu trúc tên riêng biệt, dựa vào các không gian tên cục bộ được liên kết với nhau. Ví dụ, công ty chế tạo máy của Danielle có thể gán tên cho

tất cả những người làm công của công ty, ví dụ với một tên là Ali. Tổ chức khác (công nhận công ty Danielle là một thực thể duy nhất và tin tưởng rằng công ty Danielle đã gán các tên duy nhất cho tất cả những người làm công của họ) có thể nhận ra Ali thông qua một tên rõ ràng là Danielle's Ali. Hình thức này có thể được sử dụng một cách đệ quy để xây dựng các tên rõ ràng theo ngữ cảnh sử dụng chúng, không cần phải sử dụng đến cấu trúc tên có thứ bậc.

Dựa vào X.509, SDSI cũng giải quyết phát hành uỷ quyền nhờ các định nghĩa về một số kiểu chứng chỉ uỷ quyền đơn giản. Ví dụ, một chứng chỉ của SDSI có thể chứa một định nghĩa của một nhóm cá nhân. Chứng chỉ gán một tên cho nhóm, tên này có thể được sử dụng trong các danh sách kiểm soát truy nhập vào các tài nguyên. SDSI cũng định nghĩa một chứng chỉ uỷ quyền, chứng chỉ này cho phép cho một thành viên ký các tuyên bố về các kiểu xác định, thay mặt người uỷ quyền.

4.9.5 Cơ sở hạ tầng khoá công khai đơn giản

Một lược đồ chứng chỉ xác thực khác được phát triển trong IETF, trong một nhóm được gọi là nhóm cơ sở hạ tầng khoá công khai đơn giản (SPKI). Giải pháp SPKI còn rất mới, trong đó một chứng chỉ I cho phép xác định các uỷ quyền, hoặc các đặc quyền đối với một khoá công khai mà không yêu cầu nhận dạng gắn với một người hoặc một thực thể giữ khoá riêng tương ứng. Ví dụ, một chứng chỉ SPKI có thể cho phép một khoá công khai xác thực các đăng nhập Internet bằng giao thức Telnet với tên người sử dụng riêng biệt, vào một máy chủ được chọn trong khoảng thời gian xác định.

Giống như SDSI, SPKI cũng tạo một thiết lập "đơn giản" bằng cách chấp nhận một lược đồ mã dữ liệu nghèo nàn và chi phí thiết lập thấp hơn so với ký hiệu ASN.1 (được sử dụng trong X.509).

Giải pháp SPKI có một khả năng cần được quan tâm, đặc biệt khi được sử dụng để bảo vệ truy nhập vào các nguồn tài nguyên. Tuy nhiên, hiện nay nó vẫn chưa trả lời được một số câu hỏi về các giới hạn trách nhiệm và khả năng kiểm toán trong các môi trường thương mại điện tử mở.

Việc phân tán các thông tin xác thực được chứng thực là một mảng đang được phát triển tích cực.

4.10 Tóm tắt

Khi một khoá công khai được sử dụng để mã hoá thông báo, hoặc để kiểm tra chữ ký số, việc sử dụng này mang tính thiết yếu vì nó có thể đảm bảo cho người sử dụng biết khoá công khai mà họ sử dụng đúng là khoá của người nhận thông báo hoặc từ người ký. Một chứng chỉ khoá công khai là một cấu trúc dữ liệu, liên kết một khoá công khai với một người, thiết bị hoặc thực thể khác một cách an toàn. Chứng chỉ được một CA ký số và nó chứng thực nhận dạng của chủ thể.

Với các đường dẫn chứng thực, các chứng chỉ được sử dụng để chứng thực dần dần các khoá công khai của các CA, sau đó mới đến các khoá công khai của các thực thể cuối. Do

vậy, một hệ thống chứng chỉ cho phép một người sử dụng khoá công khai thu được các khoá công khai của một số lớn các thành viên khác một cách đáng tin cậy, mà chỉ cần biết các thông tin về khoá công khai của một CA.

Hệ thống chứng chỉ phụ thuộc vào khoá riêng tương ứng với khoá công khai (khoá này được chứng thực và được bảo vệ bằng cách chỉ cho phép chủ thể của chứng chỉ đã xác thực sử dụng khoá này). Tương tự, một thực thể cuối nên sử dụng các cặp khoá khác nhau cho các mục đích mã hoá và ký số.

Khi muốn có một chứng chỉ, một người hoặc một thực thể hợp pháp khác cần đăng ký với một CA. Việc phát hành chứng chỉ có thể sử dụng các thủ tục trực tuyến. Ví dụ, truyền các thông tin xác thực, hay mật khẩu bí mật. Việc chứng thực nhận dạng có thể đòi hỏi sự hiện diện của cá nhân, hoặc tài liệu nhận dạng. Cơ quan đăng ký địa phương là một người hay tổ chức có thể hỗ trợ cục bộ cho các thuê bao của CA. Các chứng chỉ được phân tán cho những người dùng cuối thông qua các dịch vụ thư mục, các máy chủ hoặc kho chứa, hoặc được gắn vào các mục dữ liệu đã được ký.

Việc phát hành chứng chỉ có thể sử dụng các thủ tục trực tuyến. Khuôn dạng chứng chỉ khoá công khai chuẩn được công nhận rộng rãi nhất được định nghĩa trong chuẩn X.509 của ISO/IEC/ITU. Khuôn dạng chứng chỉ X.509 có 3 phiên bản; Phiên bản 3 (được hoàn thành năm 1996) giới thiệu nhiều đặc tính mới và tuỳ chọn. Khi các phiên bản trước chỉ hỗ trợ hệ thống tên X.500, phiên bản 3 hỗ trợ nhiều dạng tên khác nhau, ví dụ như địa chỉ thư tín điện tử và các URL. Phiên bản 3 cung cấp các trường mở rộng cho chứng chỉ, bao gồm các trường mở rộng chuẩn và các trường mở rộng được định nghĩa riêng hoặc dành cho một cộng đồng nào đó. Các trường mở rộng chuẩn được định nghĩa cho nhiều mục đích khác nhau, bao gồm thông tin về chính sách và khoá, các thuộc tính của chủ thể và người phát hành, các bắt buộc đối với đường dẫn chứng thực.

Một chứng chỉ được phát hành trong một khoảng thời gian định trước và nó chỉ hợp lệ trong khoảng thời gian đó. Tuy nhiên, trong một số trường hợp, ví dụ như xảy ra lộ khoá riêng tương ứng, chứng chỉ cần bị thu hồi. Giải pháp thông báo huỷ bỏ phổ biến nhất như sau: CA ký lên một CRL (danh sách các chứng chỉ bị thu hồi, được gán nhãn thời gian) và phát hành CRL một cách định kỳ. Các giải pháp thông báo huỷ bỏ khác cũng có thể được sử dụng, ví dụ truyền trực tiếp với một máy chủ tin cậy để xác thực tình trạng hiện thời của một chứng chỉ.

Chuẩn X.509 có định nghĩa một khuôn dạng CRL chuẩn. Khuôn dạng CRL chuẩn (có trong phiên bản 2 của CRL) có cơ chế trường mở rộng giống với cơ chế mở rộng trong khuôn dạng chứng chỉ X.509 của phiên bản 3 và nó cũng có các trường mở rộng chuẩn, các trường này tương thích với các trường mở rộng chuẩn của chứng chỉ X.509 trong phiên bản 3. CRL chuẩn này thông báo về tình trạng thu hồi tạm thời (treo), hoặc thu hồi vĩnh viễn của một chứng chỉ.

Việc phân tán các thông tin uỷ quyền là một yêu cầu khác với yêu cầu gắn kết một khoá công khai vào một nhận dạng, nhưng yêu cầu này cũng có thể thoả mãn bằng cách sử dụng các chứng chỉ. Một cơ quan được công nhận có thể phát hành một chứng chỉ, công bố rằng một người riêng biệt hoặc một đối tượng nào đó có quyền hoặc đặc quyền riêng. Như một sự lựa chọn, các đặc quyền hoặc quyền có thể được liên kết trực tiếp với một khoá công khai, không cần nhận dạng người hoặc đối tượng được liên kết. Các cách khác để nhận ra các chứng chỉ uỷ quyền bao gồm các thích ứng của các chứng chỉ X.509 có trong phiên bản 3, các chứng chỉ thuộc tính (được ANSI định nghĩa), các chứng chỉ thuộc tính đặc quyền (PAC được ECMA định nghĩa), giải pháp cơ sở hạ tầng an toàn được phân tán đơn giản (SDSI) và giải pháp cơ hạ tầng khoá công khai đơn giản (SPKI).

Chương 5:

CƠ SỞ HẠ TẦNG KHOÁ CÔNG KHAI

Các sở hạ tầng khoá công khai (PKI) bao gồm nhiều dịch vụ hỗ trợ. Các dịch vụ hỗ trợ này rất cần thiết khi các kỹ thuật khoá công khai được sử dụng trên phạm vi rộng. Các cơ quan chứng thực (CA) và các phương tiện quản lý chứng chỉ tạo thành hạt nhân của các cơ sở hạ tầng khoá công khai. Tuy nhiên, khi chúng ta cố gắng áp dụng các khái niệm quản lý chứng chỉ này vào trong môi trường thực, đặc biệt trong các môi trường có nhiều tổ chức và các cộng đồng khác nhau, chúng cần làm việc với nhau theo các cách thức phức tạp và làm nảy sinh nhiều vấn đề nhạy cảm cần được quan tâm. Nhiều ứng dụng hỗ trợ khác nhau (mang tính kỹ thuật và pháp lý) cần được sử dụng để khai thác một cách có hiệu quả các kỹ thuật khoá công khai. Trong phần này chúng ta tìm hiểu một số vấn đề trong việc xây dựng các PKI nhằm hỗ trợ một số lượng lớn những người sử dụng khác nhau. Các mục được trình bày bao gồm các cách xây dựng cấu trúc quan hệ giữa các CA, các cách kết hợp các chính sách và các hoạt động chứng thực khác nhau cùng với các khái niệm về đường dẫn chứng thực và các ràng buộc đối với tên, các cách tìm và phê chuẩn các đường dẫn chứng thực và các giao thức quản lý chứng chỉ. Chúng ta có thể tìm hiểu các hoạt động gần đây, nhằm ban hành hợp pháp các PKI, hỗ trợ các chữ ký số trong các giao dịch kinh doanh của chính phủ và thương mại. Ở đây cũng giới thiệu hai mô hình PKI là SET của MasterCard/Visa (được sử dụng trong thanh toán sử dụng thẻ ngân hàng trên Internet) và MISSI của Bộ quốc phòng Mỹ (được sử dụng trong gửi tin điện tử).

5.1 Các yêu cầu

Các PKI rất cần thiết cho sự tồn tại của thương mại điện tử trong phạm vi rộng. Tuy nhiên, chi phí cho chúng rất lớn và rất dễ xảy ra rủi ro khi triển khai và điều hành, việc phát triển chúng gặp một số trở ngại. Bởi vậy, khi thiết kế một PKI cần tuân theo một số yêu cầu như sau:

(a) Khả năng mở rộng: Các PKI cần có khả năng mở rộng. Điều cốt yếu của khả năng mở rộng là đảm bảo tính kinh tế trong triển khai và điều hành, tối giản các vấn đề, giúp cho người sử dụng cuối có được sự tiện lợi và an toàn, bằng cách công nhận một tập hợp các dữ liệu uỷ nhiệm của người sử dụng để hỗ trợ cho việc truyền thông với các thành viên từ xa khác nhau.

(b) Hỗ trợ cho nhiều ứng dụng : Vì sự tiện lợi, an toàn và kinh tế cho người sử dụng cuối, các cơ sở hạ tầng nên hỗ trợ nhiều ứng dụng. Ví dụ, một người sử dụng Internet có thể đăng ký với một nhà cung cấp PKI trên Internet và có thể có được các dịch vụ dành cho thư tín điện tử, truy nhập Web và truyền file.

(c) Khả năng liên vận hành của các cơ sở hạ tầng được quản trị tách biệt : Để có một cơ sở hạ tầng ở khắp mọi nơi và nó được điều hành thông qua một đầu mối quản

lý duy nhất - là điều không thực tế. Tuy nhiên, khả năng liên vận hành của các cơ sở hạ tầng có thể thực hiện được và phụ thuộc vào yêu cầu (a).

(d) Hỗ trợ nhiều chính sách: Các đường dẫn chứng thực thích hợp với một ứng dụng, không nhất thiết phải thích hợp với ứng dụng khác. (Ví dụ, ta có thể tin cậy một CA trong việc chứng thực các máy chủ Web thương mại, nhờ đó chúng ta có thể tiến hành các giao dịch kinh doanh giá trị thấp, nhưng không thể giao phó cho CA này những thông tin có khả năng làm lộ các bí mật kinh doanh). Do vậy, để thoả mãn các yêu cầu (a) và (b), cần kết hợp các chính sách khác nhau với các đường dẫn khác nhau, làm cho các chính sách này có hiệu lực, cho phép người sử dụng khác công nhận các chính sách khác, ví dụ như các chính sách được chấp nhận trong các ứng dụng khác nhau.

(e) Quản lý rủi ro đơn giản : Một tổ chức bất kỳ (hoạt động và sử dụng một PKI) cần có sự hiểu biết về các rủi ro liên quan và chia nhỏ các rủi ro cho các thành viên.

(f) Giới hạn trách nhiệm pháp lý của CA (Limitation of CA liability): Như một trường hợp quan trọng của yêu cầu (e), một CA trung gian cần được đảm bảo rằng trách nhiệm pháp lý của CA này có thể được chia nhỏ và được giới hạn để bao trùm lên các rủi ro xác định. Ví dụ, một CA cần được đảm bảo rằng nó sẽ không phải chịu trách nhiệm pháp lý đối với các thiệt hại là kết quả do sử dụng một chứng chỉ cho các mục đích không dự tính trước.

(g) Chuẩn hoá: Tất cả các yêu cầu trên chỉ ra sự cần thiết phải thiết lập các chuẩn thích hợp, trong phạm vi của các PKI.

5.2 Các cấu trúc quan hệ của CA

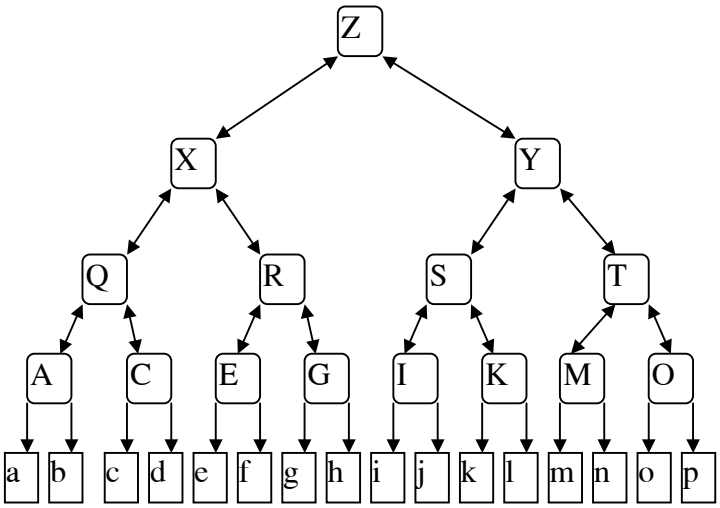
Khi sử dụng khoá công khai của một thành viên từ xa, cần phải tìm và phê chuẩn một đường dẫn chứng thực đầy đủ, đường dẫn chứng thực này đi qua nhiều CA, từ khoá công khai này tới một CA gốc, khoá công khai của các CA trên đường dẫn được lưu giữ trong một khuôn dạng tin cậy. Để xây dựng các PKI lớn và có khả năng mở rộng, một trong các vấn đề chính cần giải quyết là làm cho việc tìm và phê chuẩn các đường dẫn chứng thực trở nên thuận tiện. Có nghĩa là thiết lập các quy ước cấu trúc quản lý, trong đó các CA chứng thực các CA khác như thế nào, các quy ước cấu trúc này đôi khi được gọi là các mô hình tin cậy. Tuy nhiên, sự tin cậy không phải là câu hỏi duy nhất được đặt ra. Tiếp theo sau, chúng ta tìm hiểu các chuẩn bị cấu trúc chính, các chuẩn bị này đã được đề xuất và được sử dụng trong việc phát triển các PKI.

5.2.1 Cấu trúc phân cấp tổng quát

Để quy gọn vấn đề cơ bản về một dạng đơn giản nhất, chúng ta cần liên kết một cách có hệ thống các cặp khoá của các thành viên (nằm trong một cộng đồng lớn) thông qua các đường dẫn ngắn có thể chấp nhận được, với mỗi đường dẫn đi qua các CA tin cậy. Theo lý

thuyết đồ thị toán học, thông qua cấu trúc cây hoặc phân cấp, chúng ta tìm ra một cách giải quyết hiệu quả và hệ thống đối với vấn đề này.

Khi xem xét cấu trúc trong hình 5.1, các thực thể có tên bằng chữ hoa (ví dụ như **Z**, **X** và **Y**) là các CA. Các thực thể có tên bằng chữ thường (ví dụ như **a**, **b** và **c**) là các thực thể cuối, hoặc các thuê bao. Các mũi tên một chiều chỉ ra rằng thực thể nguồn đã phát hành một chứng chỉ, chứng chỉ này có chứa khoá công khai của thực thể đích; các mũi tên hai chiều chỉ ra rằng mỗi cặp CA phát hành các chứng chỉ cho nhau.



Hình 5.1 Cấu trúc phân cấp tổng quát

Theo cấu trúc này, chúng ta có thể dễ dàng xây dựng được một đường dẫn chứng thực giữa các cặp thực thể cuối bất kỳ, không quan tâm đến việc mỗi thực thể cuối làm thế nào để xác định CA (hoặc nhiều CA) được chấp nhận như là một CA gốc (root CA). Lưu ý rằng, mỗi thực thể cuối thiết lập một mối quan hệ gần gũi với một CA và quyết định chấp nhận nó như một CA gốc. Ví dụ, thực thể cuối a thiết lập một mối quan hệ gần gũi với CA A và chấp nhận khoá công khai của A như là khoá công khai gốc. Sau đó a có thể có được (một cách có hệ thống) một bản sao khoá công khai (đã được phê chuẩn) của các thực thể cuối khác trong cấu trúc, từ đó tồn tại một đường dẫn chứng thực cho tất cả các thực thể cuối.

Ví dụ, để có thể có được một bản sao khoá công khai của c (bản sao khoá công khai này đã được phê chuẩn), a phải xử lý một đường dẫn chứng thực của 3 chứng chỉ như sau:

- *Chứng chỉ của **A** dành cho CA **Q** , chứng chỉ này được CA **A** phát hành (lưu ý rằng **a** luôn tin tưởng vào khoá công khai của **A**);*
- *Chứng chỉ của **A** dành cho CA **C** , chứng chỉ này được CA **Q** phát hành;*
- *Chứng chỉ của **A** dành cho thực thể cuối **c**, chứng chỉ này được CA **C** phát hành.*

Để ***a*** có được một bản sao khoá công khai của ***g*** cần sử dụng một đường dẫn chứng thực gồm có 5 chứng chỉ. Để ***a*** có được một bản sao khoá công khai của ***m***, cần sử dụng một đường dẫn chứng thực gồm có 7 chứng chỉ.

Mô hình này thực sự hợp lý. Ở đây có thể có nhiều hơn hai thực thể là mức dưới (hoặc lệ thuộc) của một thực thể khác. Ví dụ, giả thiết rằng mọi CA có thể chứng thực tới 100 CA hoặc các thực thể cuối mức dưới. Trong trường hợp này, 4 mức CA (như đã được trình bày trong hình 5.1), có thể cho phép tới 100 triệu thực thể cuối phê chuẩn các khoá công khai của mỗi thực thể, với độ dài của các đường dẫn chứng thực không bao giờ vượt quá 7 chứng chỉ. Nếu chúng ta thêm vào một mức các CA khác và cho trước độ dài đường dẫn tối đa là 9 chứng chỉ, thì có tới 10 tỷ thực thể cuối được hỗ trợ.

Mô hình này có thể cho chúng ta cách xây dựng các đường dẫn chứng thực có độ dài ngắn hợp lý giữa một số lượng lớn các thực thể cuối, nhưng có một vấn đề cần quan tâm đó là sự tin cậy. Khi sử dụng một đường dẫn chứng thực cho trước, người sử dụng chứng chỉ phải tin cậy mọi CA trên đường dẫn và tiến hành các biện pháp phòng ngừa nhằm đảm bảo rằng không một thành viên nào khác có thể làm giả các chứng chỉ, có nghĩa là khoá riêng được sử dụng để ký chứng chỉ phải được bảo vệ chặt chẽ và không bị lộ.

Một vấn đề xuất hiện trong cấu trúc phân cấp này là nhiều đường dẫn chứng thực mong muốn được đi qua các CA ở mức cao hơn, đặc biệt là CA mức cao nhất, đó là ***Z***. Vì vậy, tất cả các thành viên trong cơ sở hạ tầng cần tin cậy ***Z***. Nếu một đối tượng tấn công có được khoá riêng của Z (nhờ thoả hiệp) thì đối tượng tấn công này có thể làm giả các chữ ký số của những người ký trong cấu trúc và làm cho người kiểm tra chữ ký số (người này sử dụng đường dẫn chứng thực đi qua Z) tin rằng chữ ký giả là hợp lệ.

Đôi khi, một mô hình được coi là thích hợp với cấu trúc phân cấp, trong đó CA ***Z*** là một cơ quan chứng thực quốc tế; mức tiếp theo là các cơ quan chứng thực quốc gia, ví dụ: ***X*** và ***Y*** là các cơ quan chứng thực quốc gia của Mỹ và Anh; mức CA thấp hơn tương ứng với các tổ chức của quốc gia, các nhà kinh doanh, cơ quan và cộng đồng của các cá nhân. Các mối quan tâm về sự tin cậy trở nên rõ ràng hơn. Nếu cơ quan chứng thực của Mỹ bị thỏa hiệp (để lộ khoá), điều này cho phép một đối tượng tấn công:

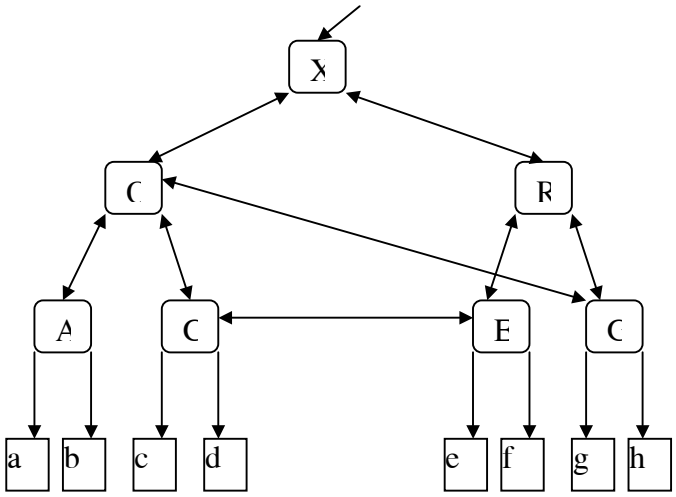
- *Làm giả các chữ ký số của bất cứ người nào trên nước Mỹ và làm cho mọi người trên thế giới tin rằng các chữ ký là hợp lệ;*
- *Làm giả các chữ ký số của bất cứ người nào ở bên ngoài nước Mỹ và làm cho mọi người trên nước Mỹ tin rằng các chữ ký là hợp lệ.*

Đối với ***Z,*** các hậu quả của việc lộ khoá rất nghiêm trọng. Một đối tượng tấn công có thể làm giả các chữ ký số của bất cứ người nào trên thế giới và làm cho mọi người ở các nước khác tin rằng các chữ ký đều hợp lệ. (Nếu các quy tắc ràng buộc có thể giới hạn các đường dẫn chứng thực trong nước, không được mở rộng tới cơ quan chứng thực mức cao nhất, các đường dẫn chứng thực trong một nước không nên bị co ngắn lại). Do các mối quan tâm về độ tin cậy, việc sử dụng cấu trúc phân cấp này không được chấp nhận và thực thi trong một số các lĩnh vực kinh doanh xác định hoặc trong các cộng đồng khép kín khác.

5.2.2 Cấu trúc phân cấp với liên kết bổ xung

Cấu trúc phân cấp mang lại cho chúng ta một cách thích hợp tìm các đường dẫn chứng thực trong một cộng đồng lớn gồm có nhiều thực thể cuối, đôi khi các đường dẫn chứng thực này có thể dài hơn mong muốn.

Với một cấu trúc phân cấp xác định, có thể bổ xung thêm một liên kết chứng thực trực tiếp giữa hai CA bất kỳ trong cấu trúc. Ví dụ, hình 5.2 trình bày một phần cấu trúc phân cấp (đã được trình bày trong hình 5.1), với một số liên kết bổ xung. Các cơ quan chứng thực ***C*** và ***E*** được chọn để chứng thực lẫn nhau sẽ rất thuận lợi khi các thực thể mức dưới của ***C*** và ***E*** cần sử dụng thường xuyên khoá công khai của các CA này, ví dụ, do mối quan hệ làm việc gần gũi giữa các cộng đồng liên quan.



Hình 5.2 Cấu trúc phân cấp với các liên kết bổ xung

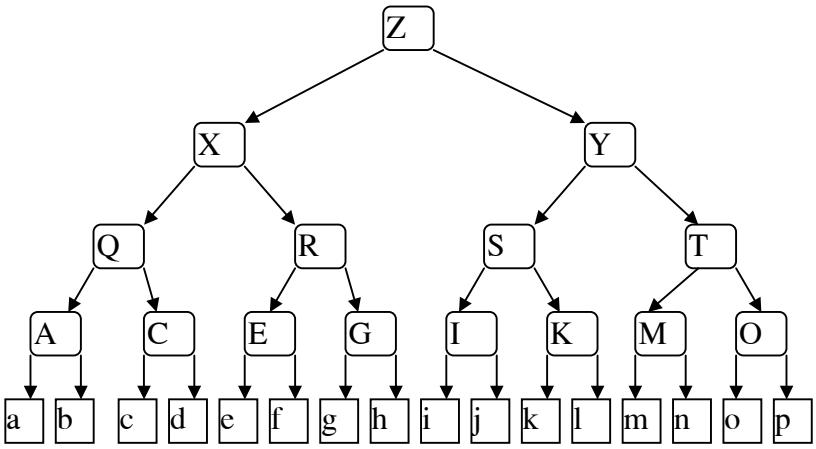
Các liên kết bổ xung kiểu như vậy không phải là một phần của cấu trúc phân cấp cơ bản, đôi khi chúng được gọi là các chứng chỉ chéo. Liên kết giữa ***C*** và ***E*** có nghĩa là ở đây hiện có một đường dẫn chứng thực, độ dài của đường dẫn chứng thực là 5 (giống như cấu trúc đã đưa ra). Tương tự, CA ***Q*** đã phát hành một chứng chỉ cho CA ***G,*** qua đó các thực thể cuối ví dụ như ***a*** và ***c*** có thể sử dụng các khoá công khai của các thực thể khác, ví dụ như ***g*** và ***h*** , với một đường dẫn chứng thực có độ dài là 3 chứ không phải là 5. Lưu ý rằng, các liên kết bổ xung có thể là hai chiều (ví dụ như ***C*** và ***E***), hoặc có thể một chiều (ví dụ như ***Q*** và ***G***), sự lựa chọn này phụ thuộc vào các mối quan hệ tin cậy và các yêu cầu hoạt động.

X.509 không quy định các CA cần quan hệ với nhau theo một cấu trúc đặc thù nào; Đúng hơn, nó mô tả mô hình phân cấp tổng quát với các liên kết bổ xung và khuyến khích sự ngầm định này.

5.2.3 Cấu trúc phân cấp top-down

Đây là một biến thể của cấu trúc phân cấp tổng quát. Cấu trúc này được Bộ quốc phòng Mỹ phát triển cho cơ sở hạ tầng khoá công khai của mình, sử dụng trong gửi tin quân sự an toàn. Cấu trúc này được gọi là cấu trúc phân cấp top-down, được minh hoạ trong hình 5.3.

Cấu trúc này khác với cấu trúc phân cấp tổng quát ở chỗ: cấu trúc này chỉ có các quan hệ đi xuống, có nghĩa là các CA không phát hành các chứng chỉ cho các CA mức cao hơn. Vì vậy, tất cả các đường dẫn chứng thực đều bắt đầu từ cơ quan chứng thực mức cao nhất (top-level CA). Tất cả những người sử dụng chứng chỉ phải có các cơ quan chứng thực mức cao nhất như các cơ quan gốc của họ, nói cách khác, họ nắm giữ một bản sao khoá công khai của cơ quan chứng thực mức cao nhất, khoá công khai này đã được phân phối theo các cách riêng (có nghĩa là được phân phối bằng các cách khác, không thông qua các chứng chỉ).



Hình 5.3 Cấu trúc phân cấp top-down

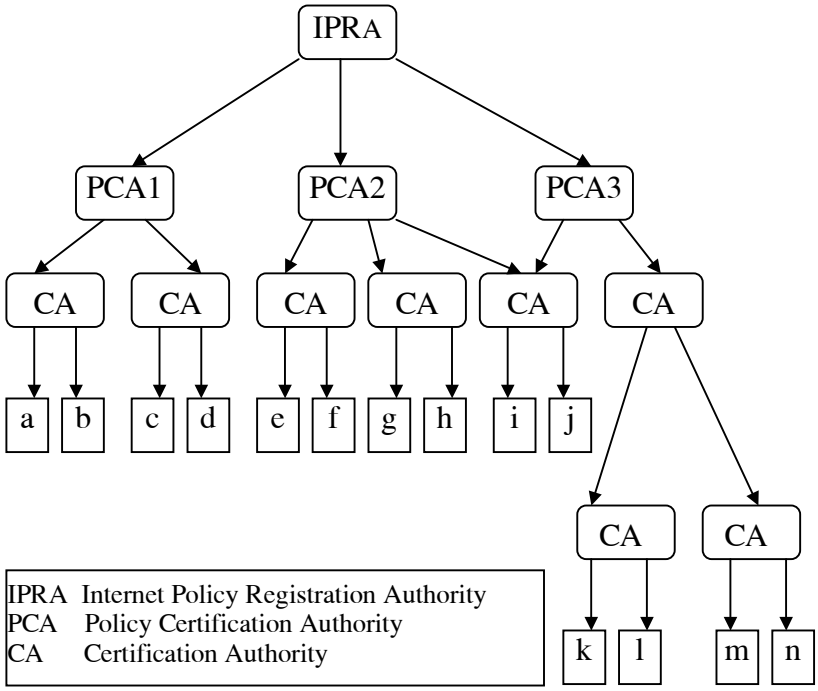
Cấu trúc này có một số ưu thế quan trọng:

- *Chỉ có một đường dẫn chứng thực cho bất kỳ thực thể cuối nào. Vì vậy, các đường dẫn chứng thực rất dễ tìm. Ví dụ, một thực thể cuối bất kỳ, chẳng hạn là **a**, có thể lưu giữ một số chứng chỉ đi từ gốc **Z** đến thực thể cuối và các chứng chỉ này được sắp xếp lần lượt trên đường dẫn, như một cấu trúc dữ liệu, một thực thể cuối khác có thể cần tới nó.*
- *Nếu một tổ chức mà các cơ sở hạ tầng của nó được cấu trúc phân cấp tự nhiên, ví dụ trong cấu trúc điều khiển phân cấp của Bộ quốc phòng, thì các mối quan hệ tin cậy trong đường dẫn chứng thực có thể lần theo và quay ngược trở lại một cách dễ dàng.*

Cấu trúc này cũng có một hạn chế. Sự bắt buộc phải tin cậy vào cơ quan chứng thực mức cao nhất nhiều hơn trong cấu trúc phân cấp tổng quát, khi tất cả các đường dẫn chứng thực đều xuất hiện CA này. Trừ khi cơ sở hạ tầng hỗ trợ một tổ chức được cấu trúc phân cấp tự nhiên giống như của Bộ quốc phòng, sự tin cậy có thể là một mối quan tâm đáng kể (thậm chí còn kém hơn trong cấu trúc phân cấp tổng quát). Mọi người nên tin cậy hoàn toàn vào cơ quan chứng thực mức cao nhất cho tất cả các mục đích.

5.2.4 Cơ sở hạ tầng PEM

Vào năm 1993, cộng đồng Internet hoàn thành việc phát triển một bộ tiêu chuẩn Internet dành cho một PKI, đó chính là cơ sở hạ tầng PEM. Trong PEM, người ta đã thử nghiệm sử dụng mô hình phân cấp top-down làm cơ sở cho một PKI mở và có phạm vi lớn. Việc phát triển cơ sở hạ tầng này nảy sinh nhiều vấn đề và nhiều giải pháp đã được đưa ra để giải quyết một số vấn quan trọng.



Hình 5.4 Cơ sở hạ tầng PEM

Tuy nhiên, việc thử nghiệm nhằm phát triển cơ sở hạ tầng PEM trong môi trường thực đã không thành công trên phạm vi lớn. Hình 5.4 minh hoạ cơ sở hạ tầng PEM.

Mô hình PEM có 3 kiểu CA như sau:

(a) Cơ quan đăng ký chính sách Internet (IPRA): Đây là cơ quan chứng thực mức cao nhất. Cơ quan này được MIT điều hành dưới sự bảo trợ của Hiệp hội Internet (Internet Society), đây là một tổ chức quốc tế phi lợi nhuận. Nó phân phối khoá công khai gốc một cách rộng rãi và chứng thực các cơ quan chứng thực chính sách.

(b) Cơ quan chứng thực chính sách (PCA): Các PCA chỉ là các cơ quan được IPRA chứng thực. Các cơ quan này nằm ở mức thứ hai trong hệ thống phân cấp. Một PCA phải đăng ký với IPRA và công bố chính sách của nó về việc chứng thực những người sử dụng hoặc các CA mức dưới của mình. Các PCA khác nhau có thể đáp ứng các nhu cầu khác nhau của người sử dụng. Ví dụ như một PCA có tổ chức (organizational PCA) có

thể hỗ trợ các nhu cầu an toàn bên trong của các tổ chức thương mại nào đó và một PCA bảo đảm cao (high- assurance PCA) có thể đưa ra một chính sách chặt chẽ hơn, chính sách này được tạo ra để đáp ứng các yêu cầu giao dịch tài chính có giá trị cao và có khả năng xảy ra rủi ro lớn. Do tất cả các đường dẫn của PEM đều chứa một PCA nên người sử dụng chứng chỉ có thể kết hợp một chính sách với mọi đường dẫn chứng thực.

(c) Cơ quan chứng thực mức thấp hơn (CA): Các cơ quan chứng thực này đại diện cho các tổ chức riêng biệt, các đơn vị được tổ chức riêng (ví dụ như các bộ, các nhóm hoặc các cá nhân), hoặc các vùng địa lý riêng.

Ở đây có một biến thể của cấu trúc phân cấp top-down. Một CA (ở mức thứ 3 của hệ thống phân cấp) có thể được một hoặc nhiều PCA chứng thực (ví dụ như ***CA5*** trong hình 5.4) có thể được cả ***PCA2*** và ***PCA3*** chứng thực). Điều này giúp cho việc xây dựng nhiều đường dẫn chứng thực với các chính sách khác nhau cho một thực thể cuối.

Đặc tả của PEM nhận dạng 3 kiểu chính sách, các chính sách này có thể kết hợp với các CA mức thấp hơn, có trong tuyên bố chính sách của một PCA:

(a) CA có tổ chức (Organizational CA): phát hành chứng chỉ cho các cá nhân ra nhập một tổ chức, ví dụ như một công ty, cơ quan của chính phủ hoặc cơ quan giáo dục.

(b) CA thường trú (Residential CA): phát hành các chứng chỉ cho các cá nhân theo địa chỉ địa lý, có thể hình dung như sau: các thực thể dân sự của chính phủ sẽ đảm nhận trách nhiệm chứng thực theo nhiệm kỳ.

(c) CA cá nhân (PERSONA CA): là một trường hợp cụ thể, trong đó việc chứng thực không yêu cầu liên kết tên (có trong chứng chỉ) với một người hoặc thực thể riêng biệt. Một chứng chỉ như vậy được thiết kế cho người sử dụng khi anh ta muốn dấu số hiệu nhận dạng của mình trong khi sử dụng các dịch vụ bảo vệ dữ liệu PEM.

Dự án PEM cũng đưa ra một quy tắc. Quy tắc này được gọi là quy tắc lệ thuộc tên. Mục đích của quy tắc này là hạn chế sự tin cậy của một người đối với các ***CA*** mức thấp. Quy tắc này quy định rằng một ***CA*** mức thấp chỉ có thể phát hành các chứng chỉ cho các thực thể có tên lệ thuộc vào tên của ***CA*** (trong cây định tên của X.500).

Ví dụ, một organizational CA là công ty thép Sharon, với tên X.500 là {*Country =US , Organization= Sharon's Steelcorp, Inc*}, ***CA*** này chỉ có thể chứng thực các thực thể có trong cây định tên của tổ chức này, ví dụ như các thực thể có tên X.500 bắt đầu bằng { *Country =US , Organization= Sharon's Steelcorp, Inc*., ...}. Các hệ thống sử dụng chứng chỉ có thể kiểm tra theo quy tắc tên lệ thuộc một cách máy móc. Ví dụ, nếu ***CA*** này (công ty thép Sharon) phát hành một chứng chỉ {*Country = Canada, Organization = Danielle's Machine Makers, Common Name = Danielle*}, thì theo logic, các hệ thống sử dụng chứng

chỉ sẽ tự động phát hiện sự không hợp lệ và loại bỏ chứng chỉ. Trong thực tế, quy tắc này hạn chế đáng kể thiệt hại xuất phát từ sai lầm của CA hoặc do các CA cố tình làm sai chức năng hoặc chủ tâm làm hại.

Quy tắc tên lệ thuộc không áp dụng cho các CA mức cao nhất hoặc cho các PCA, các CA này được tin cậy để phát hành các chứng chỉ cho một thực thể bất kỳ, phù hợp với các chính sách của chúng về tên và đối tượng.

Tóm lại, PEM thiết kế bổ xung hai đặc tính quan trọng cho cấu trúc phân cấp top-down cơ bản, như sau:

(a) Khả năng kết hợp một trong nhiều chính sách có hiệu lực với một đường dẫn chứng thực;

(b) Có khả năng ràng buộc một CA chỉ phát hành các chứng chỉ theo không gian tên X.500 của nó, vì vậy có thể hạn chế các thiệt hại do CA mắc sai lầm, bị thoả hiệp (làm lộ khoá) hoặc thiếu tinh thần trách nhiệm.

5.2.5 Các cây phân cấp

Có một vấn đề chính trong các cấu trúc phân cấp là một thành viên nào đó trong hệ thống phân cấp có thể không chấp nhận một cơ quan có thể được tin cậy cho tất cả các mục đích định trước. Ví dụ, chúng ta xem xét các cấu trúc phân cấp trong chính phủ của một nước, hệ thống phân cấp có thể hợp lý hoàn toàn. Tuy nhiên, mọi cố gắng nhằm mở rộng hệ thống phân cấp thành mức quốc tế luôn luôn thất bại. Trong khi chính phủ của các nước thiết lập các mối quan hệ song phương với chính phủ của các nước khác, song viễn cảnh tất cả các chính phủ của các nước chấp thuận tin cậy vào một cơ quan quốc tế trong việc bảo vệ các thông tin quốc tế và quốc gia nhạy cảm là không thực tế, vì các lý do về chủ quyền quốc gia.

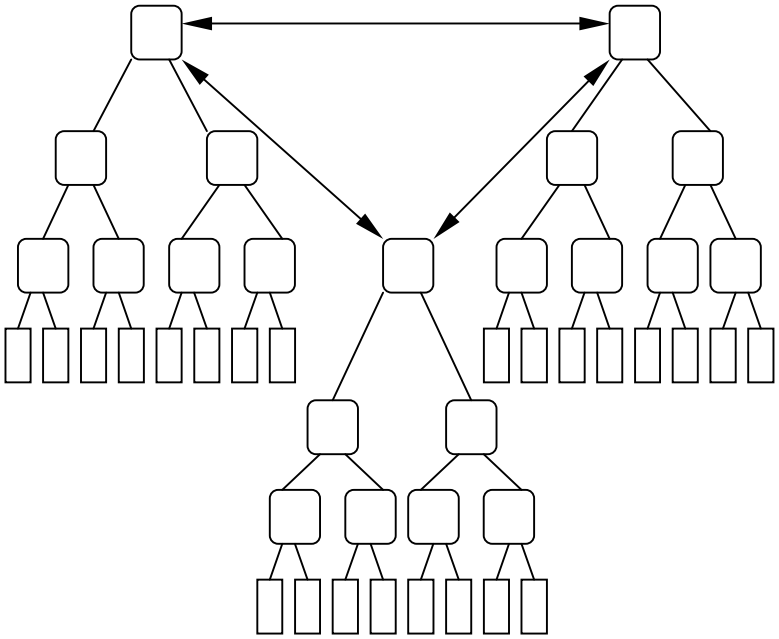
Khi áp dụng vấn đề này vào trong môi trường thương mại, các nhà kinh doanh có thể thiết lập các mối quan hệ gần gũi với các nhà kinh doanh khác, nhưng rất khó có thể tìm được một cơ quan mà tất cả các nhà kinh doanh đều tin cậy, đặc biệt đối với các thông tin nhạy cảm của họ.

Điều này dẫn đến một ý tưởng liên kết các cấu trúc phân cấp với nhau bằng cách: các CA mức đỉnh chứng thực lẫn nhau, ý tưởng này được minh họa trong hình 5.5.

Mô hình này rất quan trọng bởi vì, trong thực tế, các PKI được ví như là các đảo biệt lập, chắc chắn chúng cần liên kết với nhau trong phạm vi lớn hơn. Ví dụ, Bộ quốc phòng Mỹ đang đề xuất giải pháp cho việc thiết lập liên hoạt động giữa cơ sở hạ tầng (hệ thống phân cấp top-down) của bộ quốc phòng Mỹ với các tổ chức quốc phòng của các nước đồng minh. Giải pháp này cũng có thể được sử dụng để liên kết các cơ sở hạ tầng của các tổ chức cá nhân có quan hệ kinh doanh với nhau.

Liên kết một số lượng nhỏ các cấu trúc phân cấp top-down với nhau rõ ràng là một giải pháp không phức tạp và có thể xây dựng được. Tuy nhiên, nếu cấu trúc được sử dụng để hỗ

trợ liên hoạt động giữa các hệ thống phân cấp đơn lẻ (với số lượng các hệ thống không bị giới hạn), thì mạng lưới liên kết giữa các hệ thống phân cấp trở nên phức tạp, tuỳ tiện và trở thành trọng tâm mới của các mối quan tâm về cấu trúc. Đã đến lúc chúng ta cần xem xét một số thiết kế được cấu trúc lỏng lẻo.



Hình 5.5 Các cây phân cấp

5.2.6 Mô hình chứng thực của PGP

PGP không sử dụng các chứng chỉ X.509. Nó định nghĩa chứng chỉ riêng, có một cơ chế để lấy khoá công khai của PGP, tính toán chữ ký của PGP trên khoá công khai này bằng cách sử dụng khoá riêng của PGP khác và gắn chữ ký này vào khoá công khai ban đầu. Ở đây không có khái niệm cơ quan chứng thực, vì vậy một người sử dụng PGP bất kỳ có thể chứng thực khoá công khai của người sử dụng PGP khác. Tuy nhiên, một chứng chỉ như vậy sẽ chỉ được sử dụng thông qua phần mềm PGP của một thành viên tin cậy nếu thành viên tin cậy công nhận rõ ràng người ký là người giới thiệu được tin cậy.

Những người sử dụng PGP có thể xây dựng các đường dẫn chứng thực tuỳ ý, có thể đi qua toàn bộ cộng đồng những người sử dụng PGP. Nếu tôi là một người sử dụng PGP, tôi quyết định có một bản sao khoá công khai của Vera và tin tưởng Vera giới thiệu cho mình những người sử dụng khác bằng cách chứng thực các khoá công khai của họ, sau đó, dựa vào các chứng chỉ từ Vera, tôi có thể xây dựng một cộng đồng những người sử dụng PGP, có thể truyền thông với những người sử dụng này. Ngược lại, tôi cũng có thể chứng thực các khoá công khai của những người mà tôi quen biết trong cộng đồng của mình, cho phép những người có bản sao khoá công khai của tôi (và người tin cậy tôi) có được các bản sao

khoá công khai của những người mà tôi quen biết. Nếu các chứng thực như vậy có thể được ghép thành chuỗi hoặc xếp lồng vào nhau, chúng ta thu được một hệ thống phi thể thức, được sử dụng để xây dựng các cộng đồng người sử dụng PGP lớn, người này có thể truyền thông với người khác, không cần đưa ra bất kỳ cấu trúc chính thức nào giống như hệ thống phân cấp các CA. Mô hình chứng thực PGP được biết đến là "web of trust".

Việc quản lý chứng chỉ PGP được tiến hành thủ công. Nếu tôi là người sử dụng PGP, tôi lưu giữ một tập hợp các khoá công khai của những người sử dụng khác trong một file, file này được lưu giữ cục bộ và được gọi tên là một "key ring". Việc lưu giữ các khoá như vậy cho biết:

- *Trong bất cứ trường hợp nào, tôi cũng quan tâm đến tính hợp lệ của khoá;*
- *Mức độ tin cậy của tôi dành cho khoá này với mục đích chứng thực các khoá công khai của những người sử dụng khác.*

Khi tôi quyết định khoá là hợp lệ (ví dụ, vì người sở hữu khoá đưa khoá cho riêng tôi), lưu nó vào "key ring" của mình, tôi tự quyết định có nên tin cậy vào khoá được sử dụng cho mục đích chứng thực các khoá khác hay không. Trong thực tế, tôi có thể đánh giá sự tin cậy của mình đối với khoá được sử dụng cho mục đích chứng thực, ở bất kỳ mức nào trong 4 mức sau:

- Không biết (Don’t know). Nếu tôi báo khoá theo cách này, lập tức PGP sẽ hỏi tôi mỗi khi PGP cần sử dụng khoá này để kiểm tra việc chứng thực trên khoá khác, hoặc tôi có tin cậy khoá được sử dụng cho mục đích này hay không.

- Không (No): PGP sẽ không sử dụng chứng chỉ phụ thuộc vào khoá được sử dụng cho mục đích kiểm tra này.

- Thông thường (Usually): Tôi báo sự tin cậy của mình là “marginal” (bên lề). Như đã ngầm định, PGP biên dịch điều đó như sau: một mình chứng chỉ bên lề (marginal certificate) dành cho một khoá công khai không đủ để xem xét tính hợp lệ của một khoá công khai được chứng thực. Tuy nhiên, nếu phần mềm PGP của tôi có thể tìm ra hai chứng chỉ bên lề khác nhau dành cho một khoá công khai, phần mềm PGP của tôi sẽ xem khoá công được chứng thực là hợp lệ. (ở đây nảy sinh một vấn đề, chúng ta sẽ tiếp tục xem xét trong mục "Chứng chỉ được ký chồng chéo nhiều lần").

- Đồng ý (Yes): PGP sẽ tự động chấp nhận và sử dụng một chứng chỉ được kiểm tra bằng khoá công khai này.

So sánh với các cấu trúc CA không mềm dẻo (đã trình bày trong các mục trước), PGP web of trust cho phép bất kỳ thực thể nào cũng có thể hoạt động như là một CA và có thể phát hành các chứng chỉ cho các thực thể khác. Mô hình này làm việc tốt trong các cộng đồng tương tác lỏng lẻo, ví dụ như các cá nhân chỉ muốn bảo vệ các truyền thông thư tín điện tử cá nhân trên Internet của họ. Tuy nhiên, một vấn đề đặt ra là yêu cầu các cá nhân phải đưa ra các quyết định quan trọng về sự tin cậy, dẫn đến các rủi ro lớn nếu quyết định

sai lầm, chúng ta không thể đoán trước được hậu quả của những sai lầm này. Hơn nữa, các mô hình lỏng lẻo này rất khó buộc trách nhiệm giải trình, hoặc khó có thể có một hệ thống giải quyết các tranh chấp hiệu quả.

5.2.7 Mô hình tin cậy ràng buộc tăng dần

Qua xem xét các các mô hình trên, chúng ta có thể biết được hiệu lực của các thực thể khác nhau trong đường dẫn chứng thực, khi chúng ta lần theo một đường dẫn chứng thực đi từ người sử dụng chứng chỉ tới người nắm giữ cặp khoá, một thực thể trong đường dẫn chứng thực ít được tin cậy hơn so với thực thể trước đó.

Ví dụ:

- *Người sử dụng chứng chỉ tin cậy hoàn toàn vào bản thân mình và tin cậy các thực thể khác (các CA và những người nắm giữ cặp khoá) ít hơn. Ví dụ, người sử dụng chứng chỉ có thể giữ nhiều khoá công khai gốc và có thể đưa ra nhiều quyết định như: khoá công khai gốc nào sẽ được tin cậy cho mục đích này hoặc mục đích kia. (Khi chúng ta nói khoá gốc được tin cậy, có nghĩa là tất cả các đường dẫn chứng thực đều bắt đầu từ khoá gốc được tin cậy này). Điều này được áp dụng cho tất cả các mô hình.*

- *Trong mô hình web of trust , một CA có thể quyết định một thực thể (đã được chứng thực) được tin cậy như một thực thể cuối hoặc có thể hoạt động như một CA (yêu cầu về sự tin cậy cao hơn).*

- *Trong mô hình PEM, CA đầu tiên trong đường dẫn (CA mức đỉnh) được tin cậy trong tất cả các mục đích của PEM. Thành viên còn lại trong đường dẫn chứng thực chỉ được tin cậy trong một chính sách riêng biệt (như đã được chỉ ra thông qua tên của PCA).*

- *Trong mô hình PEM, từ CA thứ 3 trở đi trong đường dẫn chứng thực (đây là CA mức dưới của PCA), quy tắc tên lệ thuộc có hiệu lực. CA bất kỳ tiếp theo chỉ có thể được tin cậy để kiểm tra, với không gian tên bị giới hạn và giảm dần đi đối với các CA tiếp theo trong đường dẫn chứng thực.*

Để trung thành với các giới hạn tin cậy trên, hệ thống sử dụng chứng chỉ có thể chứng thực các giới hạn này một cách tự động, như là một phần của quá trình phê chuẩn đường dẫn chứng thực.

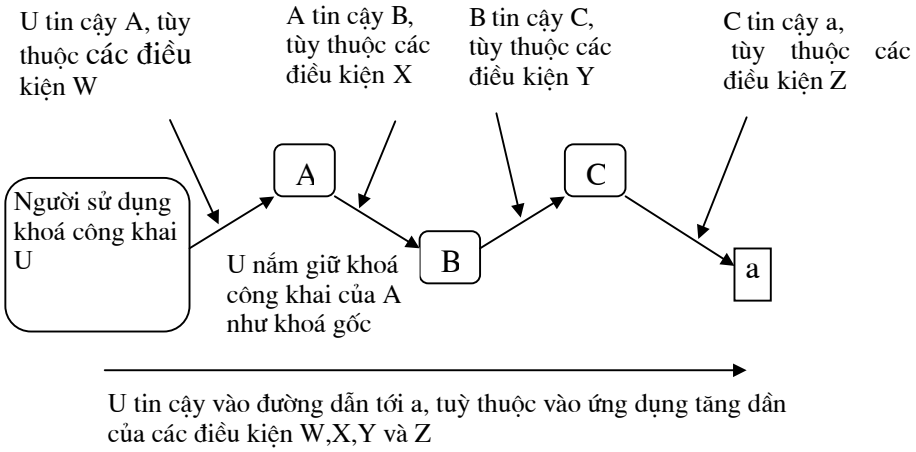
Nếu khái quát hoá những gì xảy ra ở trên, chúng ta có thể phát triển một mô hình được gọi là mô hình tin cây ràng buộc tăng dần. Mô hình này được hỗ trợ thông qua các mở rộng chuẩn phiên bản 3 của X.509 (minh hoạ trong hình 5.6).

Mô hình này cho phép một CA bất kỳ có thể xác định một tập hợp các điều kiện và các giới hạn đối với chủ thể của chứng thực. Ví dụ, các điều kiện hoặc các giới hạn có thể là các chính sách được hỗ trợ hoặc các ràng buộc đối với không gian tên. Trong giai đoạn đầu tiên, người sử dụng khoá công khai gắn các điều kiện tin cậy của mình đối với root CA (có nghĩa là ***U*** tin cậy ***A***), cũng làm tương tự như vậy đối với các giai đoạn còn lại, dù trên thực tế nó không phải là một trường hợp của "chứng thực".

Ở đây có một nguyên tắc quan trọng là các CA phải định rõ các điều kiện giới hạn, nhất là các điều kiện thiết thực, các đường dẫn chứng thực không được quá dài hoặc quá phức tạp

(nếu không sự tin cậy sẽ nhanh chóng mất đi). Điều này còn phù hợp cho cả những người sử dụng chứng chỉ và các CA. Nói chung, người sử dụng chứng chỉ ít khi gặp phải những đường dẫn chứng thực dài, hay phải gánh chịu các rủi ro do chứng thực sai lầm hoặc không thích hợp. Các CA hiếm khi gặp các đường dẫn chứng thực đáng ngờ hoặc các rủi ro do lạm dụng trách nhiệm pháp lý hoặc các vấn đề khác.

Ví dụ, chúng ta xem xét hiệu lực của một điều kiện, điều kiện này gồm có một ràng buộc đặt tên như trong quy tắc tên lệ thuộc của PEM. Công ty thép Sharon có thể phát hành các chứng chỉ cho bất cứ ai, nhưng chỉ các chứng chỉ dành cho các thực thể có tên trong không gian tên của công ty thép Sharon được hệ thống những người sử dụng chứng chỉ chấp nhận. Điều này giúp cho người sử dụng chứng chỉ hạn chế các thiệt hại do chứng thực sai lầm hoặc chủ tâm làm hại. Ví dụ, nếu công ty thép Sharon phát hành một chứng chỉ sai lầm hoặc chủ tâm làm hại cho một nhân viên của công ty thiết kế máy Danielle, chứng chỉ này sẽ bị loại bỏ tự động trong quá trình phê chuẩn đường dẫn chứng thực.



Hình 5.6 Mô hình tin cậy ràng buộc tăng dần

Mô hình tin cậy ràng buộc tăng dần là một mô hình không ép buộc, nó có thể là kết quả của việc sử dụng X.509 (phiên bản 1 hoặc phiên bản 2) mà không có giới hạn đặc biệt nào (ví dụ như các giới hạn PEM) và có thể là kết quả của thiết kế PGP. Sẽ xảy ra rủi ro nếu không hạn chế độ dài của các đường dẫn chứng thực hợp lệ, hay kết nối những người sử dụng trên thế giới bằng các đường dẫn chứng thực có độ dài không bị hạn chế và sự tin cậy không rõ ràng.

Hệ thống phân cấp CA của PEM áp dụng các nguyên tắc mô hình tin cậy ràng buộc tăng dần. Tuy nhiên, cấu trúc này còn có một số hạn chế như sau:

(a) Hệ thống phân cấp top-down thuần tuý (mọi đường dẫn chứng thực đều bắt đầu với CA mức đỉnh), hạn chế rất nhiều đối với các ứng dụng mở, phạm vi rộng. Nên cho phép kiểm tra các chuỗi chứng chỉ bắt đầu với một khoá công khai gốc từ domain của người sử dụng, đúng hơn là uỷ thác một khoá công khai tập trung tại đỉnh của một

hệ thống phân cấp. Vì thông thường, domain của người sử dụng là domain được tin cậy nhất, các hoạt động khởi tạo và cập nhật cặp khoá có thể quản lý hiệu quả hơn so với tại một thực thể cuối và một hệ thống quản lý cục bộ.

(b) Các ràng buộc trong quy tắc tên lệ thuộc của PEM này có thể gây rắc rối cho một tổ chức sử dụng hệ thống định tên X.500. Ví du, giả thiết công ty thép Sharon có một văn phòng chính tại Mỹ và một văn phòng chi nhánh tại Anh. Các tên thư mục X.500 dành cho các văn phòng này có thể là {Country=US, Organization= Sharon's Steelcorp, Inc.} và {Country=UK, Organization= Sharon's Steelcorp, Ltd.}. Công ty thép Sharon mong muốn có một CA trung tâm, CA này có thể bao trùm lên toàn bộ các văn phòng của nó trên toàn thế giới, nhưng rõ ràng là điều này không thể xảy ra bởi vì các không gian tên bị tách rời hoàn toàn.

(c) Khi sử dụng khái niệm PCA, đòi hỏi phải có các thông tin về các PCA cá nhân để hình thành logic kiểm tra đường dẫn chứng thực. Trong trường hợp thư tín điện tử Intenet, đây không phải là một vấn đề chính, người sử dụng có thể biết tên của PCA và có thể đưa ra một quyết định như: nên tin cậy những gì trong một đường dẫn chứng thực. Tuy nhiên, trong nhiều ứng dụng thương mại, ví dụ như thương mại điện tử hoặc EDI (trao đổi dữ liệu điện tử), sự can thiệp của người điều hành nhằm đưa ra các quyết định chính sách là không thực tế. Quá trình này cần được thực hiện tự động. Trong thực tế, tất cả các quá trình xử lý đường dẫn chứng thực cần có các phần mềm và phần cứng tin cậy.

Phiên bản 3 của X.509 có một số đặc tính hỗ trợ cho mô hình tin cậy ràng buộc tăng dần, có thể tránh được các hạn chế không mong muốn trong thiết kế PEM.

5.2.8 Chứng chỉ được ký chồng chéo nhiều lần

Một chứng chỉ X.509 được một CA ký; Do vậy, nó phụ thuộc hoàn toàn vào sự siêng năng và sự tin cậy của CA. Việc làm lộ khoá riêng của CA có thể gây ra những hậu quả nghiệm trọng. Tình trạng này có thể được giải quyết bằng cách đưa ra một chứng chỉ và chứng chỉ này được nhiều CA độc lập ký.

PGP có khả năng làm cho một khoá công khai được nhiều người chứng thực. Điều này tạo ra các chứng chỉ bên lề (marginal certificate), hai chứng chỉ này (tùy chọn, có thể nhiều hơn) được sử dụng để phê chuẩn một khoá. Hệ thống này có vấn đề, vì ở đây không có cách nào để đảm bảo rằng những người chứng thực là độc lập. Nếu đặt sự tin cậy vào hai người chứng thực, hai người này lại thông đồng với nhau, ví dụ hai thành viên của một tổ chức tội phạm, sẽ chỉ mang lại cảm giác không an toàn (trừ khi bạn là một thành viên của tổ chức này). Trong môi trường PGP, người sử dụng khoá công khai có cơ hội xem xét sự tin cậy của tất cả những người chứng thực trước khi sử dụng khoá. Tuy nhiên, nó không được mở rộng cho các môi trường tự động và mở, đáp ứng nhu cầu của thương mại điện tử.

X.509 không xét đến các chứng chỉ được ký chồng chéo nhiều lần, chủ yếu là do sự phức tạp. Giả sử các CA khác nhau sẵn sàng xác nhận các thuộc tính khác nhau của chủ thể, nhưng không phải tất cả đều sẵn sàng xác nhận toàn bộ các thuộc tính? Chưa chắc mọi CA đều công nhận các chính sách chứng chỉ? Các CA khác nhau muốn xác định các ràng buộc nào? Khi một CA huỷ bỏ một chứng chỉ, tất cả các CA có phải huỷ bỏ đồng thời hay không? Do tin rằng chứng chỉ được ký chồng chéo nhiều lần rất phức tạp cho nên không một nhà cung cấp nào muốn thiết lập chúng và không một tổ chức sử dụng nào có khả năng quản lý chúng. Đây là một hướng nghiên cứu trong tương lai, thuộc lĩnh vực cơ sở hạ tầng khoá công khai.

5.3 Các chính sách của chứng chỉ X.509

Khi CA phát hành một chứng chỉ, công bố với người sử dụng rằng một khoá công khai riêng biệt dành cho một thực thể riêng biệt (đối tượng của chứng chỉ). Nhưng mức độ tin cậy của người sử dụng đối với công bố này như thế nào? Hoạt động xác thực nhận dạng của một người và kiểm tra giấy uỷ nhiệm của một công ty rất quan trọng, những hoạt động này có thể được thực hiện với các mức chất lượng khác nhau và nếu chất lượng cao thì phải tính đến giá cả. Trong một số ứng dụng, chất lượng cao dẫn đầu danh sách các yêu cầu, còn trong một số ứng dụng khác chi phí thấp hơn chiếm ưu thế. Vì vậy, các chứng chỉ được phát hành tuỳ thuộc vào các chính sách và các thủ tục khác nhau và có thể phù hợp với các mục đích khác nhau.

Một CA công bố về các hoạt động và các thủ tục và đưa nó vào một tài liệu có tên là CPS.

X.509 có một số đặc tính tuỳ chọn, gọi là chính sách chứng chỉ, dựa vào một tham chiếu thông tin có trong chứng chỉ, người sử dụng chứng chỉ có thể sử dụng nó để quyết định "nên sử dụng chứng chỉ cho mục đích này hay mục đích khác?". Các PKI có thể được thiết kế để hỗ trợ các chính sách chứng chỉ khác nhau, nhằm thoả mãn yêu cầu của các ứng dụng khác nhau hay các mô hình đảm bảo hoặc tin cậy. Mỗi chứng chỉ cá nhân được kết hợp với một chính sách chứng chỉ riêng hoặc có thể được phát hành phù hợp với các chính sách khác nhau.

5.3.1 Khái niệm chính sách chứng chỉ

Chính sách chứng chỉ được định nghĩa như sau:

Một tập hợp các quy tắc được đặt tên, các quy tắc này chỉ ra khả năng ứng dụng của một chứng chỉ trong một cộng đồng riêng biệt và/hoặc lớp các ứng dụng có các yêu cầu an toàn chung.

Ví dụ, một chính sách chứng chỉ riêng biệt có thể chỉ ra khả năng ứng dụng của một loại chứng chỉ trong việc xác thực các giao dịch trao đổi dữ liệu điện tử, các giao dịch này được sử dụng khi mua bán hàng hoá có báo giá.

Các chính sách chứng chỉ phải được người phát hành và người sử dụng chứng chỉ công nhận.

Một chính sách chứng chỉ được đăng ký và được gán một tên đối tượng duy nhất (được trình bày chi tiết trong mục "Đăng ký đối tượng"). Trong trường hợp này, "đối tượng" được đăng ký sẽ được công bố. Trong một giao thức truyền thông, chỉ có tên đối tượng được truyền đi, nó sử dụng một tham chiếu tới CPS.

Ví dụ, công ty thép Sharon có thể định nghĩa hai chính sách, sử dụng trong PKI của công ty:

(a) Chính sách sử dụng chung của Sharon (Sharon's general - use policy): Chính sách này dự định được sử dụng trong bảo vệ dữ liệu hàng ngày, thông qua các nhân viên của công ty; Ví dụ, trong xác thực và mã hoá thư điện tử thông thường và trong các kết nối tới máy chủ Web của công ty. Các cặp khoá được chứng thực có thể được sinh ra, lưu giữ và quản lý thông qua các hệ thống chi phí thấp và có sử dụng phần mềm. Một chứng chỉ được phát hành tự động cho bất kỳ người nào được nhận diện trong thư mục của công ty, anh ta tạo ra một dạng yêu cầu chứng chỉ, yêu cầu này được ký và sau đó được gửi tới người quản trị mạng. Công ty thép Sharon gán cho chính sách này một tên đối tượng {joint-iso-itu-t(2) country(16) us(840) organization (1) sharon(15678) policies(4) general-use(1)}.

(b) Chính sách tài chính của Sharon (Sharon's financial policy): Chính sách này dự định được sử dụng trong bảo vệ các giao dịch tài chính có giá trị trên 1.000$. Các cặp khoá được chứng thực phải được tạo ra và được lưu giữ trong các thẻ bài phần cứng mật mã, chỉ có nhân viên quản lý và các cá nhân được chỉ định (trong một danh sách được phê chuẩn đặc biệt) mới được cấp thẻ bài và một chứng chỉ. Để được cấp một thẻ bài như vậy, cá nhân phải xuất hiện tại văn phòng an toàn của công ty và trình phù hiệu nhận dạng của mình. Công ty thép Sharon gán cho chính sách này một tên đối tượng {joint-iso-itu-t(2) country(16) us(840) organization (1) sharon(15678) policies(4) financial(1)}.

5.3.2 Mở rộng Chính sách chứng chỉ

Trong phiên bản 3 của chứng chỉ X.509, trường mở rộng Certificate Policies được định nghĩa để chuyển các tham chiếu chính sách chứng chỉ. X.509 áp dụng một mô hình, trong đó các hệ thống sử dụng chứng chỉ có thể được lập trình trước với các tham chiếu chính sách chứng chỉ, người sử dụng sẵn sàng chấp nhận chúng trong một ứng dụng xác định, cho phép các chứng chỉ được xử lý, được chấp nhận tự động và hiệu quả, chỉ ra chính sách chứng chỉ nào được sử dụng. Trong mô hình này, người sử dụng có thể quyết định chấp nhận chính sách hiện thời (hoặc người quản trị trong tổ chức của người sử dụng quyết định) trước khi lập trình. Dựa vào mô hình này, chuẩn X.509 đưa ra một hệ thống sử dụng chứng chỉ phải xử lý trường mở rộng Certificate Policies như thế nào.

Trường mở rộng này có hai biến, một trong hai biến được lật cờ "không thiết yếu" (non-critical), biến còn lại được lật cờ "thiết yếu" (critical). Chúng ta cần tìm hiểu sự khác nhau giữa hai trường hợp vì nó rất quan trọng. Trường lật cờ "không thiết yếu" liệt kê các chính sách chứng chỉ mà CA công bố áp dụng. Tuy nhiên, CA quy định rằng việc sử dụng chứng chỉ không chỉ bị giới hạn bởi các chính sách này mà còn có các chính sách khác. Tiếp tục với ví dụ về Công ty thép Sharon, các chứng chỉ được phát hành cho nhân viên bình thường của công ty, trong trường này, tên đối tượng dành cho chính sách sử dụng chung của Sharon (như đã trình bày ở trên). Các chứng chỉ được phát hành cho nhân viên quản lý của công ty, chứng thực các khoá có trong thẻ bài phần cứng của họ, có thể chứa các tên đối tượng về các chính sách sử dụng chung và chính sách tài chính của Sharon.

Trường lật cờ "không thiết yếu" được tạo ra và được sử dụng thông qua các ứng dụng như sau: mỗi ứng dụng được định trước cấu hình để biết yêu cầu chính sách như thế nào. Ví dụ, các ứng dụng thư điện tử và các máy chủ Web của công ty thép Sharon sẽ lập sẵn yêu cầu chính sách sử dụng chung của Sharon. Các ứng dụng tài chính của công ty có thể lập sẵn yêu cầu chính sách tài chính của Sharon, cho các chứng chỉ được sử dụng khi phê chuẩn các giao dịch có giá trị trên 1.000$, hoặc chính sách sử dụng chung của Sharon cho các giao dịch có giá trị thấp hơn.

Khi xử lý một đường dẫn chứng thực, một chính sách (được chấp nhận trong ứng dụng sử dụng chứng chỉ) phải xuất hiện trong tất cả các chứng chỉ có trên đường dẫn (trong các chứng chỉ của CA và của thực thể cuối). Ví dụ, công ty thép Sharon có thể có hai kiểu sản phẩm của CA, một sản phẩm chi phí thấp, dựa vào phần mềm, bộ phận quản trị mạng kiểm soát sản phẩm này theo một chế độ trực tuyến; còn một sản phẩm nữa, sản phẩm này chất lượng cao hơn, chi phí cao hơn, có một đơn vị ký dựa vào phần cứng do bộ phận an toàn của công ty kiểm soát. Kiểu sản phẩm trước có thể sử dụng khi công ty phát hành các chứng chỉ cho nhân viên, dành cho chính sách sử dụng chung của Sharon. Kiểu sản phẩm sau có thể được sử dụng khi công ty phát hành các chứng chỉ cho chính sách sử dụng chung và chính sách tài chính của Sharon.

Nếu trường mở rộng Certificate policies được lật cờ "thiết yếu", nó có cùng mục đích như đã trình bày ở trên, nhưng có thêm một vai trò. Nó chỉ ra rằng việc sử dụng chứng chỉ bị giới hạn bởi một trong các chính sách chỉ ra; Nói cách khác, CA quy định rằng, việc sử dụng chứng chỉ không phải tuân theo bất kỳ chính sách nào ngoài các chính sách đã được nhận dạng. Vì vậy, trường này được sử dụng để giúp CA chống lại việc lạm dụng trách nhiệm pháp lý, khi một thành viên sử dụng chứng chỉ cho mục đích không được dự định trước.

Ví dụ, một công ty thẻ tín dụng có thể phát hành các chứng chỉ cho những người giữ thẻ, họ sử dụng các chứng chỉ để bảo vệ các giao dịch thẻ tín dụng. Công ty thẻ tín dụng xác định được các rủi ro liên quan đến thẻ tín dụng và dễ dàng ước tính được sự lạm dụng khi một chứng chỉ bị lỗi nhưng vẫn được phát hành ngẫu nhiên, chẳng hạn như phát hành cho một người được xác thực không chính xác. Tuy nhiên, nếu một người sử dụng chứng chỉ thẻ

tín dụng khi mã hoá các bí mật độc quyền trị giá hàng triệu đôla, nhưng các bí mật này sẽ rơi vào tay đối tượng xấu nếu việc phát hành chứng chỉ thẻ tín dụng bị lỗi. Ở đây có một số vấn đề, chẳng hạn, công ty thẻ tín dụng có phải chịu trách nhiệm trước các thiệt hại do sử dụng chứng chỉ vào một mục đích không dự tính trước hay không?

Khi trường mở rộng Certificate Policies được lật cờ "không thiết yếu", trường này được sử dụng để chuyển thông tin bổ xung về chính sách trong trường qualifier, cùng với tên của mỗi chính sách chứng chỉ. Chuẩn không quy định trường qualifier phải được sử dụng cho mục đích nào. Thậm chí trong thực tế, không quy định kiểu cú pháp dữ liệu cho trường này. Bất cứ ai cũng có thể định nghĩa một kiểu qualifier và có thể đăng ký theo cách được trình bày trong mục "Đăng ký đối tượng". Bất cứ khi nào một chính sách chứng chỉ được định nghĩa, nó cần công bố các kiểu qualifier có thể được sử dụng.

Trong thực tế, các qualifier của chính sách sẽ trở nên hữu ích khi đạt được các thoả thuận (bên ngoài chính sách) về các mục đích sử dụng và các cú pháp dùng để biểu diễn chúng.

Ví dụ, một số mục đích quan trọng được dự tính cho các qualifier như sau:

(a) Chỉ ra một liên kết tin cậy, kết nối ngược trở lại một vị trí có thể lấy lại một bản sao của CPS. (qualifier sẽ chuyển một Web URL);

(b) Để chuyển (theo đúng nguyên văn) các thông tin nghĩa vụ pháp lý (ví dụ các giới hạn trách nhiệm pháp lý) và thông báo cho người sử dụng chứng chỉ biết bất cứ khi nào chứng chỉ được sử dụng.

5.3.3 Trường mở rộng Ánh xạ chính sách

X.509 định nghĩa trường mở rộng Policy Mapping, dùng khi một chứng chỉ được sử dụng để liên kết hai domain riêng lẻ, nghĩa là có một chứng chỉ chéo giữa các cơ sở hạ tầng do các tổ chức khác nhau điều hành. Trường này cho phép CA chỉ ra các chính sách chứng chỉ nào đó trong domain của CA được quan tâm ngang bằng với các chính sách khác trong domain của subject CA.

Ví dụ, giả sử công ty thép Sharon thiết lập quan hệ kinh doanh với công ty thiết kế máy Danielle và hai công ty này chứng thực chéo các cơ sở hạ tầng khoá công khai của nhau, để bảo vệ thư tín điện tử. Chính sách có sẵn của Danielle (dùng trong bảo vệ thư tín điện tử) là chính sách sử dụng chung của Danielle. Người ta nhận ra rằng, việc sinh các chứng chỉ chéo giữa hai domain cần được tiến hành song song, nhưng tất cả các ứng dụng thư tín điện tử của công ty Sharon được định cấu hình theo yêu cầu chính sách sử dụng chung của Sharon. Giải pháp (có thể thực hiện được) là định lại cấu hình cho tất cả các ứng dụng thư tín điện tử (chọn một trong hai chính sách) theo yêu cầu chính sách sử dụng chung của Danielle hoặc Sharon. Giải pháp khác là sử dụng trường Policy Mapping (giải pháp này phù hợp với người quản trị). Trong chứng chỉ chéo cho CA của công ty Danielle nhưng lại được một CA của công ty Sharon phát hành, trường này có thể đưa ra một công bố như sau: những người sử dụng chứng chỉ của công ty Sharon có thể quan tâm hai chính sách (chính sách sử dụng

chung của Danielle và Sharon) như nhau trong các mục đích đặc thù. Trường Policy Mapping thường được lật cờ không thiết yếu.

Thực tế sẽ chứng minh tính hữu ích của trường này. Toàn bộ chủ thể liên kết các cơ sở hạ tầng (được các tổ chức khác nhau điều hành) cần được nghiên cứu thêm và thử nghiệm trước khi chúng ta có thể tin tưởng vào việc thiết lập các giải pháp kỹ thuật riêng biệt.

5.3.4 Mở rộng Các ràng buộc chính sách

Policy Constraints gồm có hai trường chỉ báo tuỳ chọn, được dùng với mục đích riêng, như sau:

(a) Chỉ báo yêu cầu chính sách rõ ràng (Require Explicit Policy indicator): Một CA có thể sử dụng nó để thông báo tên chính sách (được chấp nhận) phải có mặt trong tất cả các chứng chỉ trên đường dẫn chứng thực và tên này phải rõ ràng. Tuỳ chọn này hữu ích trong một số trường hợp như sau: trong Home domain của người sử dụng chứng chỉ, ứng dụng của anh ta tin cậy các CA địa phương, mức độ tin cậy này đủ để nó không yêu cầu bất kỳ chính sách chứng chỉ nào phải có mặt trong các chứng chỉ. Ví dụ, trong công ty thép Sharon, các giao dịch nội bộ trong công ty không cần kiểm tra chính sách; Ứng dụng có thể tin cậy mọi chứng chỉ được CA phát hành. Trong trường hợp này, ứng dụng yêu cầu logic xử lý chứng chỉ của nó chấp nhận mọi chính sách. Điều này có thể đơn giản hoá đáng kể việc quản lý chứng chỉ. Tuy nhiên, nếu trên đường dẫn chứng thực xuất hiện một chứng chỉ của CA bên ngoài công ty, quy tắc có thể thay đổi, công ty thép Sharon có thể yêu cầu các CA bên ngoài cần có tên các chính sách được chấp nhận và chúng phải rõ ràng. Điều này có thể có hiệu lực đối với các chứng chỉ của CA bên ngoài, bằng cách thiết lập chỉ báo thông qua trường Require Explicit Policy.

(b) Chỉ báo ngăn cấm ánh xạ chính sách (Inhibit Policy Mapping indicator): Một CA có thể sử dụng nó để quy định, không được phép ánh xạ chính sách trên phần còn lại của đường dẫn chứng thực. Mặt khác, chỉ báo này hầu như được thiết lập trong chứng chỉ dành cho CA của một tổ chức bên ngoài. Sự phòng ngừa này rất cần thiết bởi vì sự ánh xạ này rất khó quản lý và có thể là đối tượng cho các sử dụng không thích hợp.

5.3.5 Các nội dung của một chính sách chứng chỉ

Ở đây không có định nghĩa chuẩn về việc yêu cầu một chính sách chứng chỉ phải bao gồm những chủ đề gì. Việc thiết lập các chủ đề (mà một CA thấy cần phải đưa vào và thoả mãn những người sử dụng chứng chỉ, như khả năng ứng dụng của các chứng chỉ đặc thù) rất đơn giản. Các chủ đề điển hình như sau:

(a) Các giới hạn về khả năng ứng dụng và cộng đồng: CA có thể chỉ phát hành các chứng chỉ cho các thành viên trong một cộng đồng riêng biệt theo một chính sách định sẵn. Ví dụ, những người làm công của một tổ chức hoặc các thuê bao dịch vụ của

một CA. Ngoài ra, các chứng chỉ (tuân theo một chính sách đặc thù) được dự định dùng cho một mục đích xác định.

(b) Chính sách xác thực và nhận dạng: Đây là các hoạt động mà CA cần tuân theo khi nhận dạng và xác thực các chủ thể của chứng chỉ.

(c) Chính sách quản lý khoá : CA cần thực hiện các biện pháp để bảo vệ các khoá mật mã của CA và khoá của các thuê bao của CA. Người ta cũng mong muốn các thuê bao tự bảo vệ các khoá mật mã của mình.

(d) Chính sách hoạt động : Đây là các hoạt động mà CA cần tuân theo khi tiến hành các dịch vụ của mình, ví dụ, thường xuyên phát hành các danh sách các chứng chỉ bị thu hồi (CRL) và các thủ tục kiểm toán.

(e) Chính sách an toàn cục bộ: Một CA, cơ quan đăng ký địa phương (LRA), và/ hoặc thực thể cuối cần thực hiện các biện pháp để đảm bảo an toàn cho môi trường của chúng. Trong đó, các biện pháp bảo vệ liên quan tới an toàn vật lý, an toàn cá nhân, bảo hành sản phẩm và an toàn truy nhập mạng.

(f) Các điều khoản pháp lý: Đây là một công bố về các giới hạn trách nhiệm pháp lý (CA xác nhận tuyên bố này), chẳng hạn, sử dụng các chứng chỉ theo một chính sách riêng biệt, cộng với các bác bỏ hợp pháp hoặc các điều khoản khác.

(g) Quản lý chính sách (Policy administration): Tên, các thông tin chi tiết liên quan đến cơ quan định nghĩa chính sách và các thông tin về các định nghĩa chính sách được duy trì và phát hành như thế nào.

5.4 Các ràng buộc tên X.509

Khái niệm "ràng buộc tên" được trình bày trong mục 5.2.7 (Mô hình tin cậy ràng buộc tăng dần). Các mở rộng chuẩn của X.509 có cơ chế ràng buộc tên hiệu quả, cơ chế này không phải chịu các hạn chế của quy tắc tên lệ thuộc trong PEM.

Các mô hình ràng buộc tên của X.509 cho phép mọi CA xác định chính xác các tên được công nhận trong các chứng chỉ trên đường dẫn chứng thực, khi CA chứng thực các CA khác. Ví dụ, khi CA của công ty thiết kế máy Danielle chứng thực chéo CA trung tâm của công ty thép Sharon, CA của công ty Danielle có thể xác định: chỉ có các tên chủ thể được chấp nhận xuất hiện trong các chứng chỉ trên đường dẫn chứng thực là các tên X.500 của một trong hai cây con:

{Country=US, Organization = Sharon's Steelcorp,Inc., ...} ; hoặc

{Country=UK, Organization = Sharon's Steelcorp,Ltd., ...}

Điều này không có nghĩa là công ty Sharon chỉ có thể phát hành các chứng chỉ với các tên này. CA của công ty có thể phát hành các chứng chỉ cho các chi nhánh khác của công ty ở nước ngoài, hoặc thậm chí có thể phát hành các chứng chỉ cho các công ty khác nhau tuỳ

thuộc vào mục đích kinh doanh. Tuy nhiên, công ty Danielle muốn hạn chế việc chứng thực của mình trong hai cây con (đã được nhận dạng) do hai cây này chỉ phản ánh những người mà công ty Danielle hợp tác kinh doanh. Nhờ vậy công ty Danielle có thể hạn chế các rủi ro bằng cách không cho phép các đường dẫn chứng thực tới các bộ phận khác của công ty Sharon mà nó không biết và không cần biết.

Trong thực tế, hiệu quả của mô hình cao hơn. Nó có thể tuỳ chỉnh các đặc tả không gian tên chính xác hơn nhiều so với việc chỉ sử dụng các cây con đầy đủ X.500.

Một ràng buộc tên sẽ được xác định theo các giới hạn của hai danh sách:

+ Danh sách các cây con được chấp nhận;

+ Danh sách các cây con bị ngăn cấm.

Một cây con được chấp nhận sẽ xác định phạm vi không gian tên, trong đó các tên được chấp nhận nằm trong phạm vi này (ví dụ trên sử dụng hai cây con được chấp nhận).

Một cây con bị chặn xác định phạm vi không gian tên, trong đó các tên không được chấp nhận nằm trong phạm vi này. Nếu cần, các quy tắc của cây con bị ngăn chặn có quyền cao hơn các quy tắc của cây con được chấp nhận. Ví dụ, công ty Danielle có thể cho phép các đường dẫn chứng thực tới tất cả các bộ phận của công ty Sharon tại Mỹ, trừ Industrial Machines, đây chỉ là một bộ phận của công ty Sharon và bộ phận này cạnh tranh với công ty Danielle. Công ty Danielle có thể chuẩn bị đường dẫn chứng thực gồm một cây con được chấp nhận *{Country=US, Organization = Sharon's Steelcorp,Inc., ...}*, cộng với một cây con bị ngăn chặn *{Country=US, Organization = Sharon's Steelcorp,Inc, Organization Unit = Industrial Machines Div.,...}*.

Có thể cắt bớt cây lớn nếu cần. Ta chỉ có thể xác định được: các mức nào đó của một cây con định tên sẽ áp dụng cho các cây con được chấp nhận hay cây con bị cấm.

Các ràng buộc tên cũng có thể được sử dụng với các dạng tên. Các dạng tên này khác với các tên theo X.500 và chúng có một cấu trúc phân cấp xác định. Các dạng tên khác có cùng cấu trúc như vậy gồm các địa chỉ thư tín điện tử trên Internet và các tên của Internet domain. IETF PKIX định rõ các quy tắc khi sử dụng các kiểu tên (có trong các ràng buộc tên của X.509). Ví dụ, nếu công ty Danielle sử dụng PKI để hỗ trợ thư tín điện tử an toàn với công ty Sharon, công ty Danielle quan tâm đến ràng buộc tên của một cây con được chấp nhận, sẽ sử dụng dạng tên địa chỉ thư tín điện tử trong các chứng chỉ của công ty Danielle dành cho công ty Sharon. Ràng buộc tên chỉ cho phép không gian tên *sharons.com*. Có nghĩa là, những người sử dụng của công ty Danielle có khả năng sử dụng các chứng chỉ của công ty Sharon, các chứng chỉ này liên kết các khoá công khai với các địa chỉ thư tín điện tử, dạng *someone@sharons.com*. Tuy nhiên, một chứng chỉ từ một CA của công ty Sharon chứng thực *president@whitehouse.gov* sẽ bị các ứng dụng thư tín điện tử của công ty Danielle tự động loại bỏ.

5.5 Tìm các đường dẫn chứng thực và phê chuẩn

Hai vấn đề quan trọng cần được quan tâm nhiều nhất trong thiết lập các hệ thống khoá công khai trên phạm vi lớn là làm thế nào để tìm được một đường dẫn chứng thực thích hợp và khi tìm được rồi thì phê chuẩn nó như thế nào. Các chức năng này phải được thiết lập trong tất cả các hệ thống sử dụng chứng chỉ (hoặc trong máy chủ hỗ trợ cho hệ thống này). Tốt nhất chúng ta nên tách riêng các thiết lập này, vì việc phát hiện đường dẫn chứng thực không phải là một chức năng an toàn thiết yếu, việc phê chuẩn đường dẫn chứng thực mới là chức năng an toàn thiết yếu.

5.5.1 Tìm đường dẫn chứng thực

Chẳng hạn, chúng ta gọi người sử dụng từ xa là người sử dụng đích. Chúng ta cũng giả thiết tồn tại một đường dẫn chứng thực nào đó.

Sự khó khăn của việc tìm đường dẫn chứng thực đi từ đơn giản đến phức tạp, tuỳ thuộc vào cấu trúc quan hệ của các CA và vào các thông tin bổ xung thích hợp để tìm đường dẫn.

Bây giờ ta bắt đầu với trường hợp phức tạp nhất, trong đó không có thêm các thông tin nào khác, ngoài tên của người sử dụng đích và tên của các CA gốc (root CA). Vấn đề này được minh hoạ trong hình 5.7.

Nếu tồn tại một đường dẫn và đường dẫn này có độ dài hợp lý, ta có thể tìm được đường dẫn này nếu các dịch vụ tìm thông tin có hiệu lực. Trước hết, ta cần lấy lại một chứng chỉ khoá công khai của người sử dụng đích (do một CA nào đó phát hành). Điều này không khó thực hiện vì với một chữ ký số, chứng chỉ dành cho khoá công khai của người sử dụng đích thường được phân phối cùng với chữ ký; với mã hoá, có thể dễ dàng thu được chứng chỉ của người sử dụng đích, từ các cuộc truyền thông trước với người sử dụng đích, ta có được một bản sao chứng chỉ (được cất giữ) hoặc tìm kiếm trong một thư mục riêng (từ thư mục này, các chứng chỉ được phân phối cho người sử dụng). Từ đó nảy sinh hai yêu cầu đối với dịch vụ lấy lại thông tin:

(a) Từ tên của một CA, dịch vụ lấy lại các chứng chỉ (có chứa khoá công khai của CA này) do các CA khác phát hành, và/hoặc:

(b) Từ tên của một CA, dịch vụ lấy lại các chứng chỉ mà CA này đã phát hành cho các CA khác.

Nếu dịch vụ (a) có hiệu lực, chúng ta có thể tìm được một đường dẫn chứng thực bằng cách lần ngược từng bước, từ chứng chỉ của người sử dụng đích tới một khoá gốc:

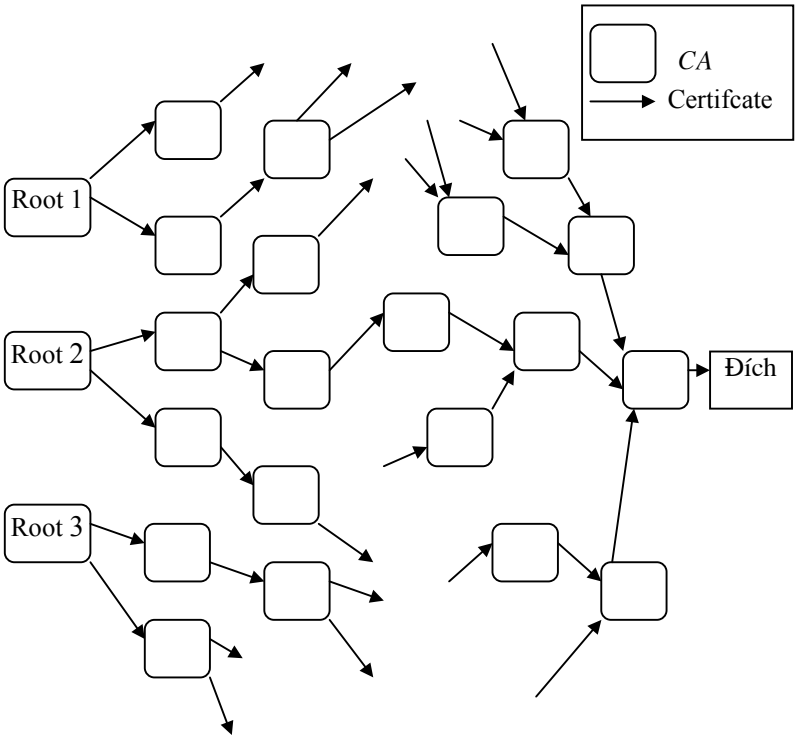
- *Bước 1: Từ một chứng chỉ do CA X phát hành, xác định các CA đã phát hành chứng chỉ cho khoá công khai của X;*
- *Bước 2: Nếu một trong các CA (đã được xác định ở bước 1) là cơ quan gốc thì có thể tìm được đường dẫn theo yêu cầu, còn không, tiếp tục bước 3;*
- *Bước 3: Tiếp tục tiến hành thủ tục của bước1 với mỗi CA được tìm thấy trong bước 1, xem CA này như là CA X.*

Cuối cùng, thủ tục này sẽ tìm được một đường dẫn chứng thực nếu nó tồn tại.

Nếu dịch vụ (b) có hiệu lực, có thể áp dụng một thủ tục tương tự (nhưng không được đảo ngược các bước), bắt đầu từ CA gốc, việc tìm kiếm kết thúc khi tìm được một đường dẫn tới CA đã phát hành chứng chỉ cho người sử dụng đích.

Nếu cả hai dịch vụ (a) và (b) có hiệu lực, việc tìm kiếm càng linh hoạt hơn. Ví dụ, có thể bắt đầu từ việc tìm kiếm CA của người sử dụng đích và các CA gốc trung gian. Từ hai dịch vụ này, có nhiều cách để tìm kiếm các đường dẫn chứng thực.

Có hợp lý không khi giả thiết cả hai dịch vụ (a) và (b) tồn tại? Giả sử ta có một dịch vụ thư mục ở khắp nơi, sử dụng kỹ thuật thư mục X.500 hoặc thư mục khác, khi đó cả hai dịch vụ (a) và (b) có thể tồn tại. X.500 có một thuộc tính dự trữ dành cho một CA, thuộc tính này được gọi là chính sách chứng chỉ chéo. Thông qua một CA xác định, thuộc tính này nắm giữ một số *forward certificate* (các chứng chỉ được các CA khác phát hành cho CA này) cộng với một số *reverse certificate* (các chứng chỉ được CA này phát hành cho các CA khác). Vì vậy, nếu giá trị của các thuộc tính này được duy trì hợp lệ thì thư mục X.500 cung cấp cả dịch vụ (a) và (b).



Hình 5.7 Vấn đề tìm đường dẫn chứng thực tổng quát

Ở đây còn có các cách khác để cung cấp các dịch vụ này, ví dụ như có thể thiết lập các cơ sở dữ liệu Web để chứa các chứng chỉ cần thiết. Nhóm IETF PKIX đề xuất các trường mở rộng trong các chứng chỉ X.509, cung cấp các con trỏ (Web URL) tới các chứng chỉ *forward certificate* và *reverse certificate*.

Chúng ta cũng nhận thấy rằng, các mô tả ở trên đưa ra trường hợp xấu nhất, khi tìm kiếm đường dẫn chứng thực mà các CA không có cấu trúc tổ chức. Bằng cách đưa ra cấu trúc, ví dụ cấu trúc phân cấp, việc tìm kiếm đường dẫn chứng thực trở nên đơn giản hơn. Ví dụ, trong cấu trúc phân cấp top-down đơn thuần, chỉ có một đường dẫn tới thực thể cuối và đường dẫn này được tìm thấy không mấy khó khăn. Trong thực tế, chúng ta có thể đoán trước các vấn đề nảy sinh trong khi tìm kiếm đường dẫn chứng thực.

5.5.2 Phê chuẩn đường dẫn chứng thực

Giả sử chúng ta tìm được một đường dẫn chứng thực thích hợp và sau đó cần phê chuẩn đường dẫn này. Các hoạt động bao gồm:

(a) Kiểm tra chữ ký số có trong mỗi chứng chỉ;

(b) Kiểm tra tên trong các chứng chỉ, xem các chứng chỉ này có phù hợp với một đường dẫn chứng thực hợp lệ hay không, có nghĩa là, chủ thể của mỗi chứng chỉ (trừ chứng chỉ cuối) là người phát hành chứng chỉ tiếp theo;

(c) Kiểm tra khoảng thời gian hợp lệ của tất cả các chứng chỉ một cách chính xác, các khoảng thời gian này có vượt quá thời điểm kiểm tra hay không (lưu ý, cần có một đồng hồ trong chính xác);

(d) Kiểm tra mỗi chứng chỉ xem chúng có bị thu hồi hay không. Đây có thể là một quá trình phức tạp, ví dụ, nhận lại, phê chuẩn và kiểm tra các CRL một cách chính xác, hoặc thực hiện một giao dịch kiểm tra tình trạng trực tuyến;

(e) Kiểm tra các chính sách chứng chỉ yêu cầu, các chính sách này được chỉ ra trong các chứng chỉ;

(f) Kiểm tra các ràng buộc cơ bản và các ràng buộc tên cần tuân theo.

Toàn bộ quá trình này được thực hiện an toàn. Nếu một đối tượng truy nhập trái phép có thể (bằng cách nào đó) phá hoại quá trình này hoặc phá hoại kết quả, mục đích của việc phá hoại này chẳng khác gì mục đích khi thay thế khoá công khai giả, đối tượng truy nhập trái phép có thể làm giả các chữ ký số và giải mã dữ liệu đã được mã hoá (dành cho người khác).

Đặc tả phiên bản 3 của X.509 tập trung chủ yếu vào yêu cầu an toàn này. Đặc tả trình bày chi tiết "một thuật toán thực thi quá trình phê chuẩn đường dẫn", nó cho phép quá trình được thực thi trong một ranh giới an toàn, có thể là phần cứng hoặc phần mềm.

5.6 Các giao thức quản lý chứng chỉ

Như đã trình bày, các chuẩn rất cần thiết khi các PKI phát triển khả năng của mình. Trong tương lai sẽ có nhiều nhà cung cấp các sản phẩm khoá công khai và người ta không thể nhận ra khả năng mở rộng của kỹ thuật khoá công khai nếu như các sản phẩm này không hoạt động cùng nhau. Ví dụ, một nhà cung cấp cần có khả năng liên lạc với CA của

các nhà cung cấp khác để có được chứng chỉ. Vì vậy, các giao thức quản lý chứng chỉ rất cần được chuẩn hoá.

Hiện tại, các nhà cung cấp sản phẩm PKI khác nhau dự định thiết lập các giao thức độc quyền để phục vụ cho các mục đích như yêu cầu phát hành chứng chỉ, yêu cầu thu hồi một chứng chỉ hoặc thiết lập chứng thực chéo giữa hai CA. Tuy nhiên, một số hoạt động chuẩn hoá cần được bắt đầu. Một dự án được thiết lập trên cộng đồng Internet và dự án này phát triển các chuẩn như vậy.

5.7 Ban hành luật

Việc triển khai và sử dụng có hiệu quả các PKI (đặc biệt trong lĩnh vực thương mại điện tử) phụ thuộc vào việc giải quyết tình trạng pháp lý không rõ ràng. Chẳng hạn, phụ thuộc vào việc giải quyết các vấn đề kỹ thuật. Nhiều luật sửa đổi bổ xung có thể giải quyết hiệu quả một số tình trạng pháp lý không rõ ràng. Thêm vào đó, các khởi xướng riêng có thể quy định cơ sở hạ tầng có tổ chức, dùng cho việc triển khai kỹ thuật khoá công khai.

Tuy nhiên, giải pháp phù hợp nhất cho việc giải quyết tình trạng pháp lý không rõ ràng và các yêu cầu của cơ sở hạ tầng là ban hành các luật thích hợp. Tối thiểu, các luật chữ ký số quy định rằng các truyền thông điện tử và các bản ghi được ký bằng chữ ký số là hợp pháp và có hiệu lực như các tài liệu được ký truyền thống. Các luật chữ ký số khác không chỉ đưa ra tính hợp lệ và giá trị dựa trên bằng chứng của tài liệu được ký số, mà còn thiết lập các chế độ quản lý PKI hợp pháp toàn diện, có thể giải quyết các vấn đề như trách nhiệm pháp lý, các kho lưu giữ và chất lượng của CA.

Tại Mỹ, Utah là bang đầu tiên ban hành luật chữ ký số, tiếp theo là bang Canifornia. Sau đó, nhiều bang của Mỹ đã ban hành luật chữ ký số hoặc đưa ra một số các đề xuất về luật chữ ký số. Một số nước đã ban hành luật, ví dụ như Đức, Đan mạch và Ý.

5.7.1 Công nghệ

Một số các đạo luật và các đề xuất liên quan tới "chữ ký" chỉ quan tâm đến mục tiêu của mật mã khoá công khai hoặc PKI. Các đề xướng như vậy quy định công nhận pháp lý và sự tuân thủ đối với truyền thông có các kiểu chữ ký điện tử đi kèm, trong đó có các chữ ký số. Đôi khi, các hoạt động và các đề xuất như vậy được mô tả như là *technology-neutral*.

Ngược lại, việc ban hành luật *technology-specific* (ví dụ như mật mã khoá công khai) cho phép liên kết chi tiết về mặt pháp lý, lập chính sách trong bối cảnh những khả năng đã biết, hoặc các điểm yếu của công nghệ cụ thể. Ví dụ, một hệ thống khoá công khai thực hiện chức năng đơn thuần, quy định một mức tin cậy cao đối với việc xác thực của các thành viên tham gia truyền thông, tính toàn vẹn của thông báo và có thể cả tính tin cậy.

Ban hành luật (đưa ra các PKI một cách chính xác và đầy đủ) cũng có thể cung cấp các giả định có bằng chứng để liên kết một thông báo (được ký bằng khoá riêng) với một tổ chức và có thể tạo ra cơ sở hạ tầng pháp lý cần thiết nhằm hỗ trợ chống chối bỏ. Nói cách

khác, ban hành luật *technology-neutral* cho phép những người điều chỉnh luật linh hoạt hơn, phù hợp với các giải pháp an toàn, bao gồm các công nghệ mới và các công nghệ này có thể được phát triển trong tương lai, thị trường sẽ chấp nhận các công nghệ thích hợp nhất.

5.7.2 Phạm vi và chi tiết

Những người làm chính sách tán thành các cách tiếp cận khác nhau đối với phạm vi và chi tiết trong luật chữ ký số. Ví dụ, một số nhà làm luật và các học giả cho rằng luật chữ ký số không nên quá chi tiết làm nó trở nên nặng nề. Ngược lại, nó nên quy định một cách ngắn gọn (tiếp cận tối thiểu) sự hợp lệ của các tài liệu điện tử và có thể uỷ quyền làm luật cho một thực thể quản trị thích hợp. Thêm vào đó, một số nước lựa chọn để đưa ra các luật mà chỉ giới hạn trong các nội dung thuộc lĩnh vực công khai.

Dưới đây là một ví dụ về tiếp cận tối thiểu do Canifornia quy định. Đây là một luật rất ngắn gọn, các nội dung của nó đơn giản như sau:

Sử dụng chữ ký số

(a) Trong một cuộc liên lạc bất kỳ với một thực thể công khai, trong đó yêu cầu hoặc sử dụng một chữ ký, mọi thành viên tham gia liên lạc có thể ký tên bằng một chữ ký số tuân theo các yêu cầu của mục này. Việc sử dụng chữ ký số sẽ có tác dụng và hiệu quả như khi sử dụng chữ ký viết tay, khi và chỉ khi chữ ký số có tất cả các tính chất sau:

1) Chữ ký số là duy nhất đối với người sử dụng nó.

2) Có khả năng kiểm tra được.

3) Chịu sự kiểm soát duy nhất của người sử dụng nó.

4) Được liên kết với dữ liệu theo cách: nếu dữ liệu bị thay đổi thì chữ ký số không còn hợp lệ nữa.

5) Tuân theo các quy định được Ngoại trưởng thông qua.

(b) Việc sử dụng và chấp nhận một chữ ký số thuộc quyền lựa chọn của các thành viên. Trong mục này, không có bất cứ điều gì yêu cầu một thực thể công khai sử dụng hoặc cho phép sử dụng một chữ ký số.

(c) Các chữ ký số được sử dụng theo đúng mục 71066 (trong Public Resources Code) được miễn mục này.

(d)"Chữ ký số" có nghĩa là một tên điện tử, được tạo ra thông qua máy tính, với mục đích người sử dụng nó có được hiệu quả như khi ký bằng tay.

Tiếp cận tối thiểu có thể làm cho công nghệ trở nên mềm dẻo hơn và đáp ứng các luật mới. Tuy nhiên, tiếp cận tối thiểu có thể bỏ qua nhiều yêu cầu quan trọng. Ví dụ, hạn chế hiệu quả của việc ban hành luật chữ ký số trong các hoạt động thuộc lĩnh vực công khai, hoặc các tác động qua lại giữa các thành viên bí mật và công khai, rõ ràng là hạn chế lợi ích, có thể bỏ qua các rào cản quan trọng và các vấn đề không được giải quyết. Kỹ thuật chữ ký số còn mới và phức tạp, do vậy các luật hiện hành nên quy định một khung làm việc hợp

pháp thích hợp nhằm thiết lập một PKI đáng tin cậy, việc thiết lập này cần được phối hợp và kiểm soát. Cần bổ xung thêm các vấn đề pháp lý thiết yếu (ví dụ như chia nhỏ trách nhiệm pháp lý), chứ không phải chỉ có tính hợp lệ của một chữ ký số.

Ngược lại với tiếp cận tối thiểu**,** tiếp cận toàn diện hình thành một luật, luật này bao trùm lên nhiều khía cạnh của vấn đề, chi tiết hơn và khả năng ứng dụng rộng hơn.

Tiếp cận toàn diện được luật chữ ký số của Utah tóm tắt, phác thảo như sau:
Phần 1. Đề mục, giải thích và các định nghĩa
Phần 2. Việc cấp phép và dự luật của các CA
Phần 3. Trách nhiệm của CA và thuê bao
Phần 4. Hiệu lực của một chữ ký số
Phần 5. Các dịch vụ và các kho chứa được tổ chức lại

5.7.3 Các văn bản và chữ ký

Yêu cầu tối thiểu đối với một đạo luật chữ ký số là công nhận tính hợp lệ và làm cho nó hiệu lực đối với (ít nhất) một kiểu thông báo điện tử nào đó. Các kiểu chữ ký điện tử và chữ ký số được sử dụng để phê chuẩn hợp pháp các bản ghi và các giao dịch. Mục 401, 403, 404 của Utah Act là các nguyên tắc điển hình:

Mục 401. Đáp ứng các yêu cầu chữ ký. Với một điều luật yêu cầu chữ ký, hoặc đưa ra hậu quả nào đó của việc thiếu chữ ký, chữ ký số có thể đáp ứng được yêu cầu này nếu:

a) chữ ký số được kiểm tra bằng cách sử dụng khoá công khai (khoá công khai này có trong một chứng chỉ hợp lệ do một CA có đăng ký phát hành);

b) chữ ký số này được người ký tạo ra cho thông báo;

c) người nhận không:

(i) làm thay đổi trách nhiệm của người tạo ra chữ ký số;

(ii) có khoá riêng để thay đổi chữ ký số.

Mục 403. Tài liệu (được ký số) được thảo thành văn bản. Một thông báo hợp lệ và có hiệu lực như khi nó được thảo thành văn bản (trên giấy tờ) nếu nó:

a) chứa toàn bộ chữ ký;

b) chữ ký số này được kiểm tra bằng khoá công khai trong chứng chỉ và chứng chỉ này:

(i) được một CA có đăng ký phát hành ;

(ii) nó hợp lệ tại thời điểm chữ ký số được tạo ra.

Mục 404. Các thông báo ban đầu được ký số. Một bản sao của thông báo được ký có hiệu lực và hợp lệ như thông báo ban đầu.

5.7.4 Chất lượng và các chuẩn của CA

Việc triển khai kỹ thuật chữ ký số có thành công hay không, phụ thuộc phần lớn vào các hỗ trợ. Vì vậy, luật nên thiết lập một cơ sở hạ tầng pháp lý cho các CA, bao gồm các quy tắc và các chuẩn về chất lượng, kho lưu giữ và trách nhiệm pháp lý.

Các đạo luật chữ ký số (ví dụ Đạo luật của Utah) cố gắng đưa ra chất lượng của CA bằng cách giới hạn việc cấp phép của các CA cho các thực thể thuộc chính phủ, những người được uỷ quyền đại diện trước toà, các cơ quan tài chính và những người được uỷ thác khác. Tuy nhiên, hầu hết các đạo luật và các đề xuất thừa nhận rằng, các giới hạn như vậy loại trừ không thích hợp phần lớn công nghệ thông tin. Vì vậy, họ không giới hạn việc cấp phép cho các thành viên như trên. Thêm vào đó, các nhà làm luật quan tâm đến việc luật nên yêu cầu cấp phép trong phạm vi quyền hạn, hoặc đơn giản chỉ cung cấp đặc quyền trong phạm vi quyền hạn của nước ngoài (các bang hoặc các nước khác) cấp phép cho các CA. Như một sự lựa chọn, nhiều nước quan tâm đến lợi ích của việc công nhận các CA quốc gia nhằm đảm bảo một giải pháp cụ thể phù hợp, từ đó có thể xác định chất lượng và thẩm quyền của các CA.

Các quy tắc và các chuẩn đặc trưng trình bày việc sử dụng các hệ thống tin cậy, công bố và đưa ra các tài liệu về chính sách và các hoạt động, sở hữu bản ghi, các biểu diễn và các đảm bảo mà một chứng chỉ có thể có, huỷ bỏ, treo và kết thúc các chứng chỉ.

5.7.5 Các chuẩn về thuê bao

Luật chữ ký số (thiết lập các cơ sở hạ tầng khoá công khai) có thể nêu các trách nhiệm và các quy tắc áp dụng cho các thuê bao, cũng như các CA. Ví dụ, trách nhiệm của các thuê bao khi sử dụng các hệ thống tin cậy là giữ bí mật các khoá riêng, treo hoặc huỷ bỏ nếu một trong các khoá riêng của họ bị lộ.

5.7.6 Chia nhỏ trách nhiệm pháp lý

Có lẽ vấn đề quan trọng nhất và hay được tranh luận nhiều nhất trong luật chữ ký số là việc người nào phải chịu trách nhiệm pháp lý và phải chịu mức độ như thế nào đối với các thiệt hại do tin cậy các chứng chỉ sai sót. Người phải chịu trách nhiệm pháp lý chính là các CA, các thuê bao và các thành viên tin cậy vào các chứng chỉ sai sót. Khi CA phát hành một chứng chỉ, CA là mục tiêu đầu tiên đối với các khiếu kiện. Gánh nặng này có thể được chia xẻ cho các thành viên khác (ở mức độ nào đó). Hai câu hỏi quan trọng được đặt ra cho vấn đề này là trước tiên, có nên chia nhỏ trách nhiệm pháp lý cho tất cả các thành viên hay không, thứ hai, nếu chia nhỏ thì tiến hành như thế nào?

Thừa nhận rằng, PKI có đủ khả năng xúc tiến thông qua các luật chia nhỏ trách nhiệm pháp lý, sau đó vấn đề chỉ còn là lược đồ chia nhỏ hiệu quả nhất có khả năng hỗ trợ triển khai PKI và phân chia công bằng các rủi ro như thế nào. Đạo luật của Utah đã đưa ra một mô hình ban đầu, trong đó một CA (được cấp phép) tuân theo tất cả các yêu cầu cần thiết của đạo luật để tránh các thiệt hại và các trách nhiệm pháp lý khác nằm ngoài các giới hạn tin cậy đã được công bố trong chứng chỉ.

Một CA được cấp phép:

(a) không phải chịu trách nhiệm đối với bất kỳ mất mát nào là hậu quả của việc tin cậy một chữ ký số (của một thuê bao) bị lỗi hoặc bị làm giả, nếu chữ ký số bị lỗi hoặc bị làm giả, CA tuân theo tất cả các yêu cầu cần thiết của phần này;

(b) không phải chịu trách các nhiệm pháp lý ngoài các trách nhiệm được xác định trong chứng chỉ, như giới hạn tin cậy được đề nghị cho:

(i) mất mát do tin cậy vào một biểu diễn sai trong chứng chỉ, chính vì vậy cần sử dụng CA để xác nhận; hoặc:

(ii) không tuân theo các điều luật về phát hành chứng chỉ;

(c) chỉ phải chịu trách nhiệm pháp lý đối với các thiệt hại trực tiếp, đền bù trong bất kỳ hoạt động nào nhằm khôi phục lại mất mát do tin cậy chứng chỉ, các thiệt hại không bao gồm:

(i) các thiệt hại nhằm trừng phạt hoặc cảnh cáo; hoặc:

(ii) các thiệt hại do mất lợi nhuận, tiền tiết kiệm hoặc cơ hội; hoặc:

(iii) thiệt hại do nỗi đau tinh thần và thể xác.

5.8 Hai mô hình PKI

Để minh hoạ cho PKI, chúng ta xem xét hai đề xuất PKI của những năm 1990. Trước hết là SET, được các tổ chức Visa và MasterCard phát triển nhằm hỗ trợ các thanh toán sử dụng thẻ ngân hàng trên Internet. Tiếp theo, chúng ta xem xét PKI của Bộ quốc phòng Mỹ, PKI này được thiết kế nhằm hỗ trợ thư tín điện tử an toàn và các ứng dụng khác của chính phủ.

5.8.1 Cơ sở hạ tầng SET

Các tổ chức Visa và MasterCard cùng nhau phát triển SET, một giao thức toàn diện và đặc tả về cơ sở hạ tầng, nhằm hỗ trợ các thanh toán sử dụng thẻ ngân hàng như là một phần của mua bán điện tử trên Internet.

Các thành phần trong môi trường SET gồm:

(a) Bộ phận phát hành (Issuer): là một cơ quan tài chính, cơ quan này phát hành các thẻ ngân hàng (thẻ tín dụng hoặc thẻ nợ), có một brand đặc trưng (ví dụ, các brand như Visa và MasterCard).

(b) Người nắm giữ thẻ (Cardholder): là người nắm giữ thẻ ngân hàng hợp pháp, anh ta đã đăng ký với bộ phận phát hành tương ứng để tiến hành thương mại điện tử.

(c) Thương gia (Merchant): là người bán hàng, hoặc tổ chức có hàng hoá, dịch vụ hoặc thông tin bán cho người nắm giữ thẻ.

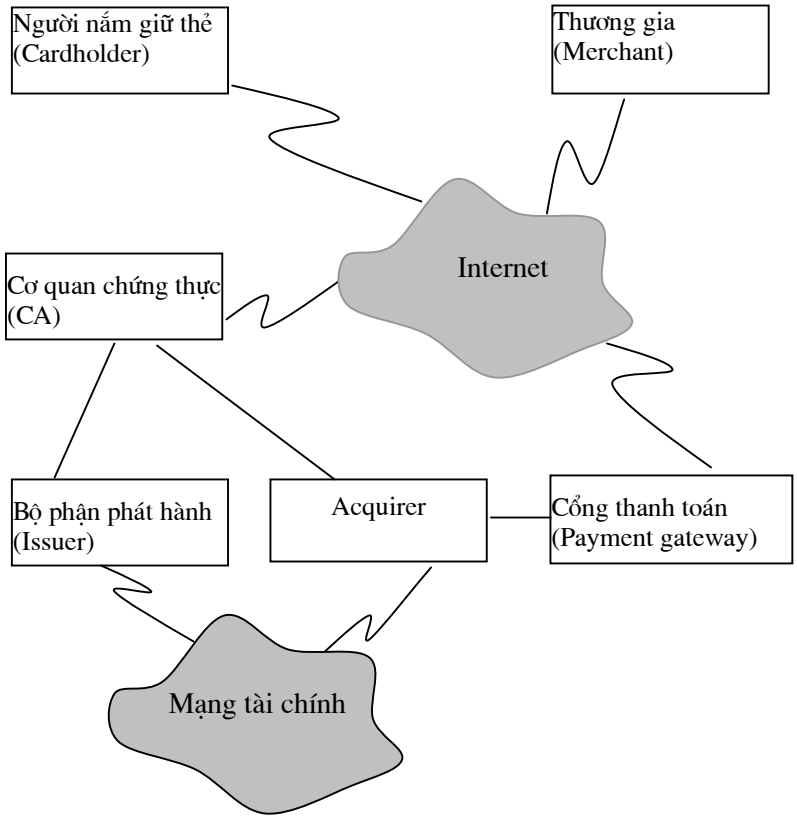
(d) Acquirer: là một cơ quan tài chính hỗ trợ các thương gia qua dịch vụ xử lý giao dịch thẻ ngân hàng.

(e) Cổng thanh toán (Payment gateway): là hệ thống cung cấp các dịch vụ thương mại điện tử trực tuyến cho các thương gia. Hệ thống được điều hành bởi một Acquirer hoặc một thành viên khác (hỗ trợ các Acquirer); Trong PKI được trình bày ở mục sau, cổng thanh toán cần có giao diện với Acquirer để hỗ trợ xác thực và giành được các giao dịch.

(f) Cơ quan chứng thực (Certification authorites): là một thành phần của cơ sở hạ tầng, chứng thực khoá công khai của người nắm giữ thẻ, thương gia, và/hoặc Acquirer, hoặc các cổng.

Khi thực hiện một giao dịch thanh toán điện tử, các thành phần ở trên tác động lẫn nhau như sau:

Sau khi người nắm giữ thẻ đồng ý tiến hành mua bán với thương gia, anh ta gửi cho thương gia một chỉ dẫn thanh toán. Thương gia liên lạc với Acquirer thông qua một cổng thanh toán, chuyển một phần hoặc toàn bộ chỉ dẫn thanh toán, nhằm xác thực và giành được giao dịch. Tất cả các hoạt động này được tiến hành trực tuyến. Acquirer giành được giao dịch. Việc xác thực có thể yêu cầu một giao dịch hỏi đáp ngược trở lại với bộ phận phát hành. Khi đó, giao dịch này được thực hiện qua các mạng tài chính hiện có (chứ không phải qua Internet). Mối quan hệ của các thành phần trong môi trường SET được minh hoạ trong hình 5.8.



Hình 5.8. Các thành phần trong môi trường SET

Trong môi trường này, kỹ thuật khoá công khai hỗ trợ nhiều chức năng, bao gồm:

 Mã hoá các chỉ dẫn thanh toán đảm bảo rằng số hiệu thẻ ngân hàng của người sử dụng không bao giờ bị lộ khi chuyển trên Internet và trên các hệ thống thương mại.

 Việc xác thực người nắm giữ thẻ cho thương gia (hay cơ sở thương mại) và Acquirer nhằm bảo vệ, không cho phép các cá nhân sử dụng trái phép thẻ bị đánh cắp khi họ tiến hành các giao dịch điện tử;

 Việc xác thực các thương gia cho người nắm giữ thẻ và Acquirer nhằm bảo vệ, không cho phép các cá nhân thiết lập các Internet site, nơi mà họ tự cho mình là các thương gia hợp pháp và tiến hành các giao dịch gian lận;

 Việc xác thực các Acquirer cho người nắm giữ thẻ và thương gia nhằm bảo vệ, không cho phép bất kỳ người nào tự nhận mình là một Acquirer có khả năng giải mã các thông tin nhạy cảm có trong chỉ dẫn thanh toán;

 Việc đảm bảo tính toàn vẹn của thông tin giao dịch nhằm ngăn chặn giả mạo trên Internet.

Hình 5.9 minh hoạ cơ sở hạ tầng khoá công khai SET. Nó được cấu trúc như một hệ thống phân cấp top-down, bao gồm các kiểu CA như sau:

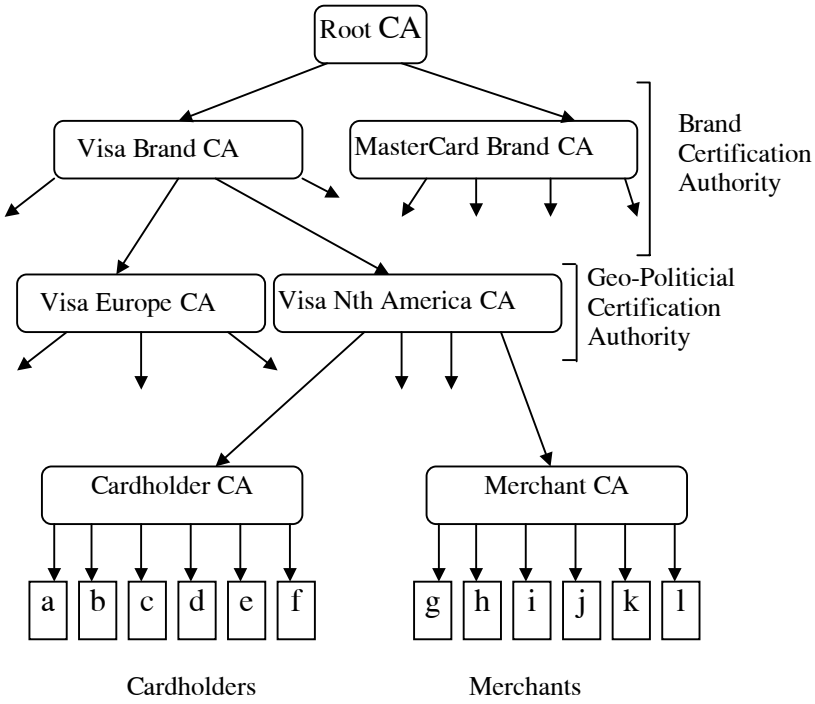
(a) Root CA (CA gốc): Tất cả các đường dẫn chứng thực bắt đầu với khoá công khai của CA gốc. CA này được giữ tách riêng và an toàn, rất hiếm khi được truy nhập vào, nó phát hành các chứng chỉ cho các brand CA. Khoá gốc ban đầu được tạo cho hệ thống SET và trong tương lai nó cũng được thay thế. CA gốc được một tổ chức điều hành và tổ chức này được toàn bộ ngành kinh doanh thỏa thuận tin cậy.

(b) Brand CA: Các CA này được điều hành bởi chính các brand khác nhau, ví dụ như Visa và MasterCard. Mỗi brand có quyền tự trị rất lớn để có thể quản lý được các chứng chỉ mức thấp hơn.

(c) Geo-political CA: Mức CA này (tuỳ chọn) cho phép một brand phân chia trách nhiệm quản lý các chứng chỉ mức thấp hơn đi qua các khu vực địa lý và chính trị khác nhau. Các khu vực khác nhau có thể có các chính sách khác nhau, do việc điều hành hệ thống tài chính có sự khác nhau.

(d) Cardholder CA: Các CA này tạo ra và phân phối các chứng chỉ của người nắm giữ thẻ cho những người khác. Các yêu cầu chứng chỉ có thể được đệ trình thông qua thư tín điện tử hoặc Web. Tuỳ thuộc vào các quy tắc của brand, CA có thể được điều hành bởi một bộ phận phát hành hoặc một thành viên khác. Nói chung, trong trường hợp sau, CA cần liên lạc với bộ phận phát hành để kiểm tra các thông tin chi tiết về người giữ thẻ trước khi phát hành một chứng chỉ.

(e) Merchant CA: Các CA phát hành các chứng chỉ cho các thương gia, dựa vào sự chấp thuận của một Acquirer. Tuỳ thuộc vào các quy tắc của brand, CA có thể được điều hành bởi một Acquirer hoặc một thành viên khác.



Hình 5.9 Cơ sở hạ tầng khoá công khai SET

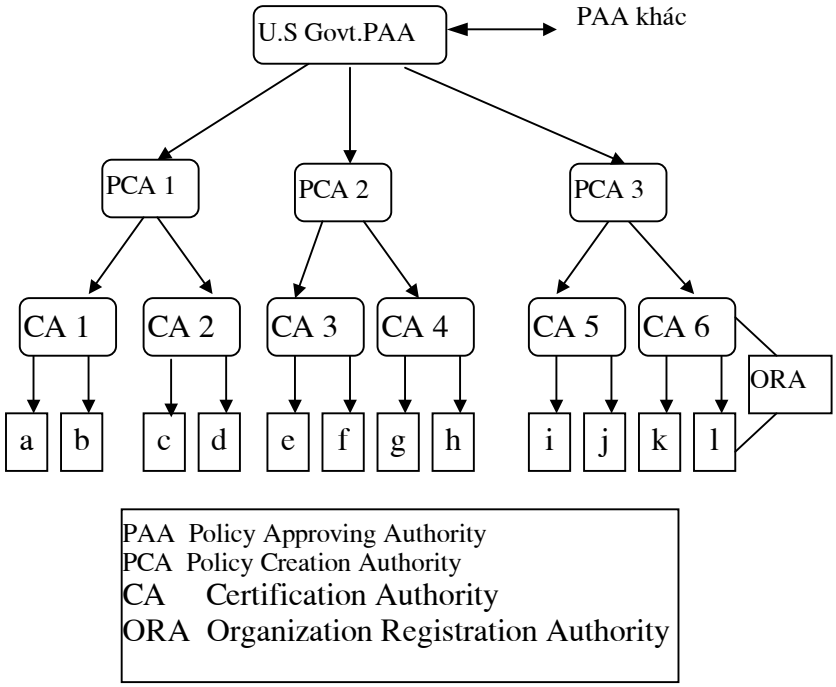
Hệ thống phân cấp top-down có thể phù hợp với kiểu ứng dụng này, vì toàn bộ cơ sở hạ tầng dành cho một mục đích ứng dụng đơn lẻ và do môi trường kinh doanh tài chính không có các vấn đề nghiêm trọng trong việc thiết lập các mối quan hệ tin cậy cần thiết. Cơ sở hạ tầng được dự kiến cẩn thận, không hỗ trợ các ứng dụng khác ngoài thanh toán sử dụng thẻ ngân hàng và không kết hợp hoạt động với các cơ sở hạ tầng khác. Lý do chính là để đảm bảo các tổ chức điều hành không phải chịu bất kỳ rủi ro nào do sử dụng các chứng chỉ vào các mục đích không dự tính trước.

5.8.2 Cơ sở hạ tầng DoD MISSI

Tổ chức NSA của Mỹ đi đầu trong việc phát triển một cơ sở hạ tầng dựa vào một chương trình, chương trình này được gọi là MISSI.

Một ứng dụng cho cơ sở hạ tầng này là DMS, hỗ trợ gửi tin trong quân sự, gửi đi các thông tin nhạy cảm nhưng chưa được xếp vào loại mật và các thông tin được phân loại ở mức thấp hơn. Tuy nhiên, cấu trúc MISSI không bị hạn chế.

Cơ sở hạ tầng MISSI có mối liên quan chặt chẽ với thiết kế Internet PEM, được minh hoạ trong hình 5.10.



Hình 5.10 Cơ sở hạ tầng khoá công khai MISSI

Các thành phần ban đầu trong cơ sở hạ tầng này (một ví dụ khác của hệ thống phân cấp top-down) như sau:

(a) Cơ quan phê chuẩn chính sách (PAA): Đây là CA gốc, mọi đường dẫn đều bắt đầu từ nó. PAA chứng thực các PCA tại mức kề dưới và cũng cho phép chứng thực chéo các PAA khác trong các domain riêng lẻ hoàn toàn, ví dụ PAA của một cơ sở hạ tầng tương tự tại một nước đồng minh.

(b) Cơ quan tạo ra chính sách (PCA): Mỗi PCA là gốc quản trị dành cho domain chính sách an toàn riêng lẻ. Ví dụ, có thể có các PCA khác nhau dành cho domain nhạy cảm nhưng chưa được xếp loại; dành cho domain SECRET của Bộ quốc phòng; dành cho các ứng dụng dân sự của chính phủ liên bang và dành cho các ứng dụng thương mại.

(c) Cơ quan chứng thực (CA): CA là một cơ quan quản trị đặc trưng cho một tổ chức quản trị, hoặc một đơn vị chủ chốt của một tổ chức trong một domain chính sách. CA đăng ký các thực thể cuối và phát hành các chứng chỉ của chúng.

(d) Cơ quan đăng ký của tổ chức (ORA): ORA là dạng của một cơ quan đăng ký địa phương (LRA) của MISSI. ORA không phát hành các chứng chỉ. Nó giúp CA đăng ký những người sử dụng cuối bằng cách thu thập các thông tin về họ và gửi các thông tin đó cho CA.

Cơ sở hạ tầng MISSI là trường hợp có cấu trúc phân cấp top-down hoạt động tốt.

5.9 Tóm tắt

Nhiều dịch vụ cơ sở hạ tầng mang tính công nghệ và pháp lý được sử dụng để khai thác có hiệu quả các kỹ thuật khoá công khai hỗ trợ cho thương mại điện tử. Các dịch vụ này tập trung xung quanh các CA và các phương tiện quản lý chứng chỉ liên quan. Nhiều vấn đề nảy sinh khi các dịch vụ này bắt buộc các tổ chức và các cộng đồng làm việc với nhau.

Bất cứ người nào sử dụng khoá công khai của một thành viên từ xa cần tìm và phê chuẩn một đường dẫn chứng thực, đi qua nhiều CA, từ khoá công khai này tới một CA gốc, khoá công khai của CA này được lưu giữ trong một khuôn dạng tin cậy. Việc tìm và phê chuẩn các đường dẫn chứng thực dễ hay khó phụ thuộc vào các quy ước cấu trúc, thông qua chúng có thể quản lý các CA chứng thực các CA khác. Các quy ước này phụ thuộc phần lớn vào các mô hình quan hệ tin cậy.

Mô hình phân cấp tổng quát như sau: các CA được cấu trúc theo hình cây, mỗi nút chứng thực các nút trên và dưới nó. Một đường dẫn chứng thực có thể được xây dựng giữa các cặp thực thể cuối, không quan tâm đến nút nào được chọn là một root CA. Các liên kết chứng thực bổ xung giữa các nút có thể được thêm vào nhằm cải thiện hiệu năng. Cấu trúc phân cấp top-down có điểm khác biệt là tất cả các đường dẫn chứng thực đều bắt đầu từ một root CA và tất cả những người sử dụng phải tin cậy CA này. Nếu mối quan hệ tin cậy được chấp nhận, có thể thiết lập được một cấu trúc có hiệu quả. Mô hình Internet PEM sử dụng hệ thống phân cấp top-down với các đặc tính bổ xung để liên kết các chính sách với các đường dẫn chứng thực và tuân theo các không gian tên của chủ thể. PGP sử dụng web of trust, trong đó, cộng đồng có thể chứng thực khoá công khai của những người sử dụng khác. Phiên bản 3 của X.509 hỗ trợ một mô hình hiệu quả hơn, được gọi là mô hình tin cậy ràng buộc tăng dần, trong đó mọi CA có thể chứng thực các CA khác, nhưng mọi chứng chỉ có thể tuân theo các chính sách chứng chỉ, các không gian tên và các các khía cạnh khác của chứng thực. Mục đích của nó là làm cho các đường dẫn chứng thực ngắn và có thể kiểm soát được.

Các chính sách chứng chỉ được sử dụng để chỉ ra cho người sử dụng biết chứng chỉ có phù hợp với mục đích ứng dụng đặc thù hay không. Phiên bản 3 của X.509 có các trường dành cho việc xác định các chính sách áp dụng và ánh xạ từ chính sách này tới chính sách khác khi một đường dẫn chứng thực đi qua ranh giới của một domain quản trị. Trường policy qualitier có thể chứa các thông tin bổ xung, ví dụ một con trỏ trỏ tới CPS.

Các ràng buộc tên cho phép một CA bất kỳ xác định chính xác các tên được phép trong các chứng chỉ tiếp theo trên đường dẫn chứng thực khi nó chứng thực CA khác. Điều này có thể giúp cho người sử dụng hạn chế các thiệt hại xuất phát một CA sai lầm hoặc cố tình làm hại.

Khi thiết lập các hệ thống khoá công khai trên phạm vi rộng lớn, hai vấn đề quan trọng và cần được quan tâm nhiều nhất là làm thế nào để tìm được một đường dẫn chứng thực

thích hợp và khi đã tìm được rồi thì chứng thực nó như thế nào. Tìm đường dẫn có thể được thực hiện tự động bằng các các dịch vụ lấy lại thông tin cần thiết, ví dụ như dịch vụ thư mục.Việc phê chuẩn đường dẫn cần tuân theo một thuật toán xác định và cần được thiết lập an toàn.

Việc triển khai rộng rãi các PKI trong lĩnh vực thương mại điện tử phụ thuộc phần lớn vào việc giải quyết tình trạng pháp lý không rõ ràng và các vấn đề về kỹ thuật. Tại Mỹ, nhiều luật liên quan đến chữ ký số đã được ban hành. Luật chữ ký số công nhận tính hợp pháp của các thông báo được ký số trong các trường hợp xác định. Chúng cũng có thể thiết lập cơ sở hạ tầng quản trị và các giới hạn trách nhiệm pháp lý áp dụng cho các CA.

Hai ví dụ về thiết kế PKI là SET của Visa/MasterCard (dùng để hỗ trợ các thanh toán sử dụng thẻ ngân hàng) và PKI của Bộ quốc phòng Mỹ (dùng để hỗ trợ thư tín điện tử an toàn và các ứng dụng khác của chính phủ).

CHỮ KÝ ĐIỆN TỬ

TRONG HOẠT ĐỘNG THƯƠNG MẠI ĐIỆN TỬ

GIỚI THIỆU

Thương mại điện tử đã và đang phát triển nhanh chóng trên thế giới và Việt Nam. Sự phát triển của thương mại điện tử đã mang lại những hiệu quả to lớn trong các hoạt động kinh doanh. Sự ra đời của thương mại điện tử đã làm thay đổi nhiều những nhận thức quen thuộc trong các hoạt động thương mại truyền thống. Nhiều vấn đề về hạ tầng kỹ thuật, cũng như hạ tầng pháp lý cần phải giải quyết khi thương mại điện tử đi vào cuộc sống.

Trong các giao dịch thương mại truyền thống, người ta sử dụng chữ ký viết tay trên các văn bản giấy tờ để xác nhận nội dung của văn bản và nhận dạng người ký. Nhưng trong các giao dịch thương mại điện tử, các văn bản giấy tờ đã được chuyển đổi thành các văn bản điện tử, việc ký trên các văn bản điện tử trở thành một vấn đề cần quan tâm nghiên cứu. Để đảm bảo có thể tiến hành các hoạt động thương mại điện tử thì việc giải quyết các vấn đề liên quan đến chữ ký điện tử là điều thực sự cần thiết và cấp bách.

Trong môi trường điện tử, để các chữ ký điện tử có hiệu lực ngang bằng với các chữ ký viết tay, chúng ta cần tập trung giải quyết hai vấn đề quan trọng là cơ sở công nghệ và cơ sở pháp lý cho chúng.

Chữ ký điện tử có rất nhiều loại, tương ứng với mỗi kiểu chữ ký điện tử cụ thể, chúng ta có cơ sở công nghệ riêng áp dụng cho từng kiểu chữ ký điện tử này. Do hiện nay, người ta chủ yếu sử dụng chữ ký số trong các giao dịch thương mại điện tử, để tài liệu tập trung hơn, chúng tôi không trình bày dàn trải vào tất cả các công nghệ áp dụng cho các chữ ký điện tử, mà chỉ tập trung vào cơ sở công nghệ áp dụng cho chữ ký số. Còn về cơ sở pháp lý cho tất cả các kiểu chữ ký điện tử, người ta đã đưa ra một công cụ chung và thực sự hiệu quả để giải quyết các vấn đề về hiệu lực pháp lý cho chúng, đó chính là Luật mẫu về Chữ ký điện tử. Nó chính là cơ sở pháp lý cho chữ ký điện tử nói chung và chữ ký số nói riêng.

Phần I trình bày những cơ sở công nghệ thiết yếu để xây dựng chữ ký số như mật mã khoá công khai, xác thực thông báo và các hàm băm. Đồng thời, trình bày các yêu cầu đối với một chữ ký số, chuẩn chữ ký số DSS và thuật toán ký số DSA cũng được xem xét trong phần này.

*Phần II trình bày cơ sở pháp lý cho chữ ký số trên cơ sở Luật mẫu về chữ ký điện tử của UNCITRAL (*Uỷ ban về Luật Thương mại Quốc tế của Liên Hợp Quốc*), bản hướng dẫn ban hành luật. Luật mẫu về chữ ký điện tử của UNCITRAL hiện nay đang được xem như một căn cứ quan trọng để xây dựng các văn bản pháp lý cho chữ ký điện tử của nhiều quốc gia được soạn ra bởi Liên hợp quốc nhằm thúc đẩy thương mại điện tử phát triển toàn cầu. Bởi tính không biên giới của hoạt động thương mại điện tử nên vấn đề pháp lý là một vấn đề hết sức phức tạp và nhạy cảm. Nó làm sao phải thoả mãn cả vấn đề quốc gia, vấn đề tôn giáo, chính trị, xã hội, v.v. Nhận thức được tính phức tạp của nó, Liên hợp quốc đã xây dựng Luật mẫu về Chữ ký điện tử với tính mở cao, làm căn cứ để các quốc gia xây dựng nên các luật về chữ ký điện tử cho mình.*

PHẦN A

CƠ SỞ CÔNG NGHỆ CHO CHỮ KÝ SỐ

1.1 MẬT MÃ KHOÁ CÔNG KHAI

Cơ sở mật mã được áp dụng cho các chữ ký số là mật mã khoá công khai. Để đảm bảo bí mật thông tin, người ta có thể sử dụng 2 loại mã hoá là mã hoá khoá công khai (mã hoá phi đối xứng) và mã hoá khoá riêng (mã hoá đối xứng).

Mã hoá đối xứng

Trước hết, chúng ta tìm hiểu sơ qua về mã hoá đối xứng, tìm ra ưu và nhược điểm của nó so với mã hoá khoá công khai. Trong mã hoá đối xứng, bản rõ (dạng văn bản ban đầu có thể hiểu được) được chuyển thành bản mã (dạng văn bản vô nghĩa khó hiểu). Quá trình mã hoá và giải mã sử dụng cùng một thuật toán và khoá.

Độ an toàn của mã hoá đối xứng phụ thuộc vào một vài yếu tố như thuật toán mã hoá phải đủ mạnh (sao cho việc giải mã thông báo mà chỉ dựa vào bản mã là không khả thi), sự bí mật của khoá (không phải là sự bí mật của thuật toán).

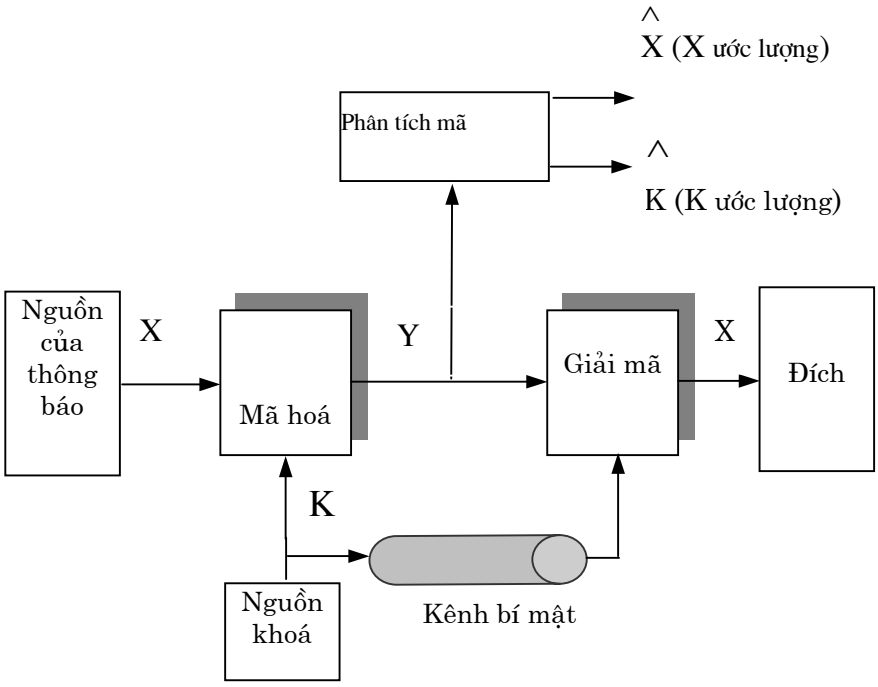
Xem lược đồ mã hoá đối xứng trong hình 1.1. Nguồn A tạo ra một thông báo ở dạng rõ, X= $\{X_1, X_2, ..., X_M\}$. Khoá được sử dụng khi mã hoá có dạng K=$\{K_1, K_2,..., K_1\}$. Nếu khoá do nguồn sinh ra, khoá phải được chuyển cho đích theo một kênh an toàn nào đó. Có thể sử dụng một thành viên thứ ba *a* để sinh khoá và phân phối khoá an toàn cho cả nguồn và đích.

Với đầu vào là thông báo X và khoá mã K, đầu ra của thuật toán mã hoá là một bản mã Y = $\{Y_1, Y_2,..., Y_N\}$. Chúng ta có thể viết như sau:

$Y = E_K(X)$

Khi nhận được bản mã, người nhận có thể giải mã bản mã bằng cách cùng một khoá và thuật toán (dùng khi mã hoá) như sau:

$X = D_K(Y)$



Hình 1.2 Mô hình mã hóa đối xứng

Việc mã hoá và giải mã thông báo sử dụng mã hoá đối xứng rất nhanh và hiệu quả. Tuy nhiên, khoá phải được lưu giữ cẩn thận. Nếu khoá bị lộ, tất cả các thông báo trước đó đều bị lộ và cả người gửi lẫn người nhận phải sử dụng khoá mới cho các cuộc truyền thông tiếp theo.

Quá trình phân phối khoá mới cho các thành viên rất khó khăn. Một vấn đề nảy sinh đối với mã hoá đối xứng là chúng không thích hợp trong các môi trường lớn, chẳng hạn trên Internet. Do mỗi cặp thành viên truyền thông trên Internet phải có một khoá bí mật khi họ muốn trao đổi thông tin với nhau một cách an toàn, dẫn đến số lượng khoá sẽ rất lớn, giống như hệ thống các đường dây điện thoại riêng không có các trạm chuyển mạch. Với N thành viên tham gia truyền thông, chúng ta cần có C^2_N khoá bí mật, chẳng hạn với 12 người muốn truyền thông với nhau, chúng ta cần 66 khoá bí mật.

Mã hoá khoá công khai

Mã hoá khoá công khai có một số thuận lợi so với mã hoá đối xứng. Thứ nhất, số lượng khoá không lớn. Nếu có N người muốn trao đổi thông tin với người khác một cách an toàn, thì chỉ cần duy nhất N cặp khoá, ít hơn rất nhiều so với mã hoá đối xứng. Thứ hai, việc phân phối khoá không phải là một vấn

đề. Khoá công khai của mỗi người có thể được gửi đi theo kênh an toàn nếu cần thiết và không yêu cầu bất kỳ sự kiểm soát đặc biệt nào khi phân phối. Thứ ba, mã hoá khoá công khai có khả năng thực thi chữ ký số. Có nghĩa là, một tài liệu điện tử có thể được ký và gửi cho người nhận bất kỳ, cùng với chống chối bỏ. Thực tế, khó có thể tồn tại một người nào khác ngoài người ký - sinh ra chữ ký điện tử; thêm vào đó, người ký không thể chối bỏ việc ký tài liệu sau khi đã ký.

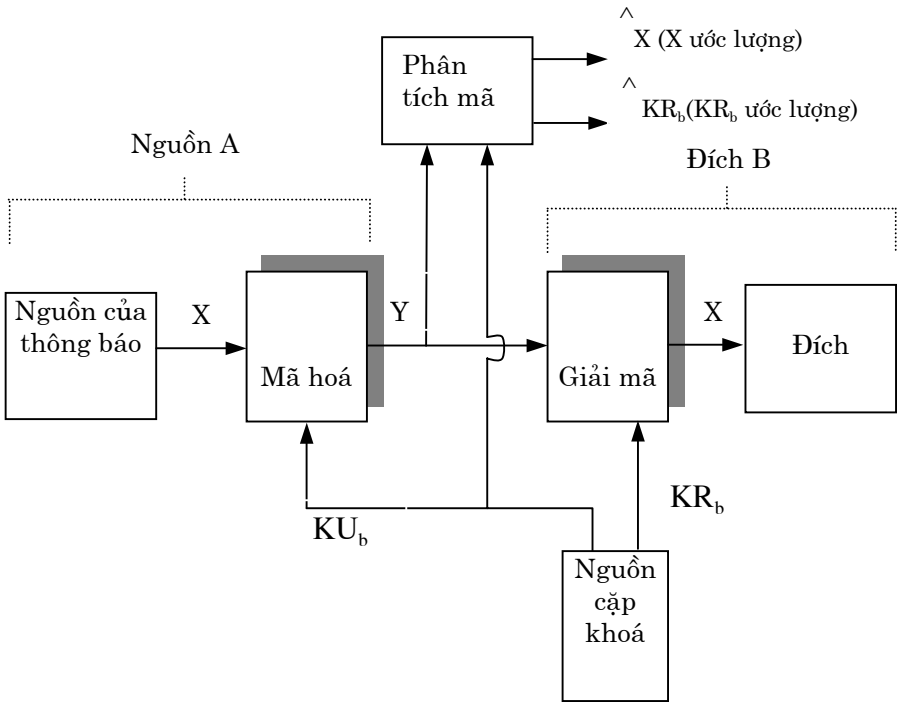
Mã hoá khoá công khai có một số khó khăn. Một trong các khó khăn đó là quá trình mã hoá và giải mã khá chậm so với mã hoá khoá đối xứng. Khoảng thời gian chênh lệch này sẽ tăng lên một cách nhanh chóng nếu bạn và các khách hàng của bạn tiến hành thương mại trên Internet. Người ta không có ý định thay thế mã hoá đối xứng bằng mã hoá khoá công khai. Chúng bổ sung lẫn nhau.

Các thuật toán khoá công khai sử dụng một khoá để mã hoá và một khoá khác để giải mã (tạo thành một cặp khoá). Chúng có tính chất quan trọng là không thể xác định được khoá giải mã nếu chỉ căn cứ vào các thông tin về thuật toán và khoá mã hoá.

Để phân biệt giữa mật mã khoá công khai và mã hoá đối xứng, người ta gọi khoá được sử dụng trong mã hoá đối xứng là khoá bí mật. Hai khoá dùng trong mã hoá khoá công khai là khoá công khai và khoá riêng.

Quá trình mã hoá khoá công khai bao gồm các bước cơ bản sau đây:

1. Mỗi thành viên sinh ra một cặp khóa, cặp khoá này được sử dụng để mã hoá và giải mã các thông báo.
2. Mỗi thành viên công bố khóa mã hoá của mình bằng cách đặt khoá này vào một địa chỉ được công bố công khai. Đây chính là khoá công khai. Khoá cùng cặp được giữ bí mật, đó chính là khoá riêng.
3. Nếu A muốn gửi cho B một thông báo, A mã hoá thông báo với khoá công khai của B.
4. Khi B nhận được thông báo, B giải mã thông báo bằng khoá riêng của B. Không một người nhận nào khác có thể giải mã thông báo, bởi vì chỉ có B mới biết khoá riêng của mình.



Hình 1.2 Lược đồ mã hoá khoá công khai: Bí mật

Với cách giải quyết này, tất cả các thành viên tham gia truyền thông đều có thể có được các khoá công khai. Khoá riêng của mỗi thành viên được giữ bí mật. Quá trình liên lạc chỉ an toàn chừng nào khoá riêng còn được giữ bí mật. Mỗi thành viên có thể thay đổi các khoá riêng của mình bất cứ lúc nào, đồng thời công bố các khoá công khai cùng cặp để thay thế khoá công khai cũ.

Chúng ta xem xét các yếu tố cần thiết trong lược đồ mã hoá khoá công khai trong hình 1.2.

Nguồn A đưa ra một thông báo rõ và bản rõ của thông báo là $X = [X_1, X_2,...,X_M]$. A dự định gửi thông báo cho đích B. B sinh ra một cặp khoá là khoá công khai KU_b, khoá riêng KR_b. Chỉ có B biết KR_b, còn KU_b được công bố công khai, do vậy A có thể có được khoá công khai này.

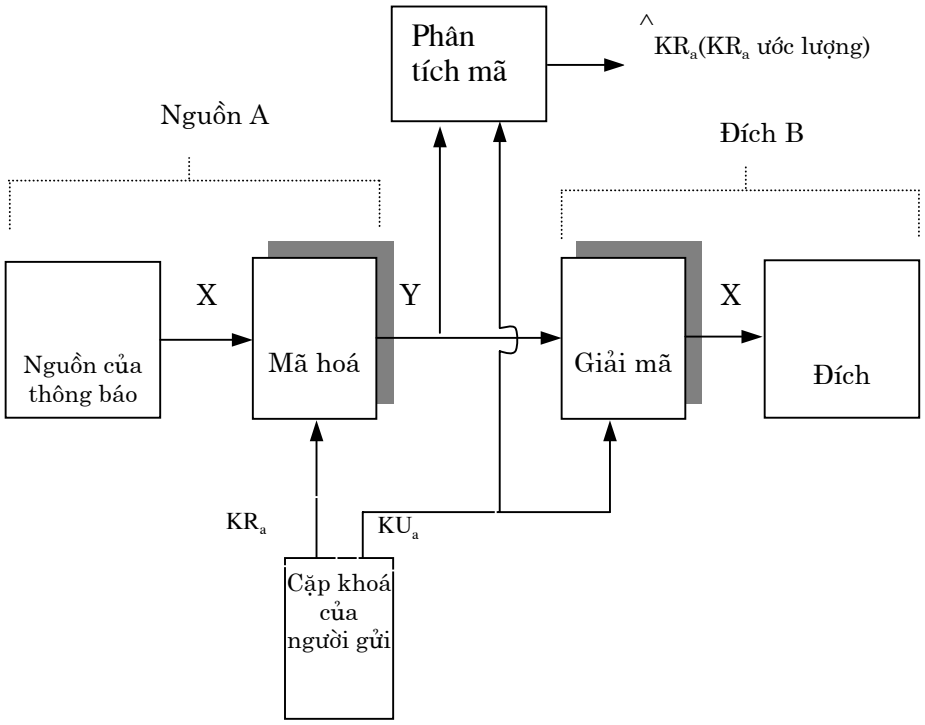
Với đầu vào là thông báo X và khoá mã hoá KU_b, A tạo ra một bản mã $Y = [Y_1, Y_2, ..., Y_N]$ với $Y = E_{KUb}(X)$.

Người nhận hợp lệ (người sở hữu khoá riêng) thu được X, qua phép biến đổi ngược $X = D_{KRb}(Y)$.

Chúng ta đã biết, một trong hai khoá trong cặp khoá có thể được sử dụng để mã hoá, khoá còn lại được sử dụng để giải mã. Điều này cho phép thực hiện

một lược đồ mã hơi khác một chút. Lược đồ được minh hoạ trong hình 1.2 cung cấp tính bí mật. Hình 1.3 minh hoạ việc sử dụng mã hoá khoá công khai cho xác thực:

$$Y = E_{KRa}(X)$$
$$X = D_{KUa}(Y)$$



Hình 1.3 Lược đồ mã hoá khoá công khai: Xác thực

Trong trường hợp này, A chuẩn bị một thông báo để gửi cho B và mã hoá thông báo với khoá riêng của A trước khi truyền đi. B có thể giải mã thông báo bằng khoá công khai của A. Thông báo được mã hoá bằng khoá riêng của A nên có thể xác định chỉ có A là người tạo ra thông báo. Do vậy, toàn bộ thông báo mã hoá được sử dụng như một chữ ký số. Hơn nữa, không thể sửa đổi thông báo nếu không có khoá riêng của A, chính vì vậy thông báo được xác thực cả nguồn gốc lẫn tính toàn vẹn dữ liệu.

Trong lược đồ trước, toàn bộ thông báo được mã hoá, nó đòi hỏi khả năng lưu giữ lớn. Mỗi tài liệu phải được lưu giữ ở dạng rõ. Bản sao được lưu giữ ở dạng mã, do vậy chúng ta có thể kiểm tra được nguồn gốc và các nội dung trong trường hợp tranh chấp. Một cách hiệu quả hơn để có được các kết quả như trên là mã hoá một khối nhỏ các bit. Khối này được gọi là dấu xác thực. Nó phải có tính chất là mọi thay đổi trên tài liệu dẫn đến sự thay

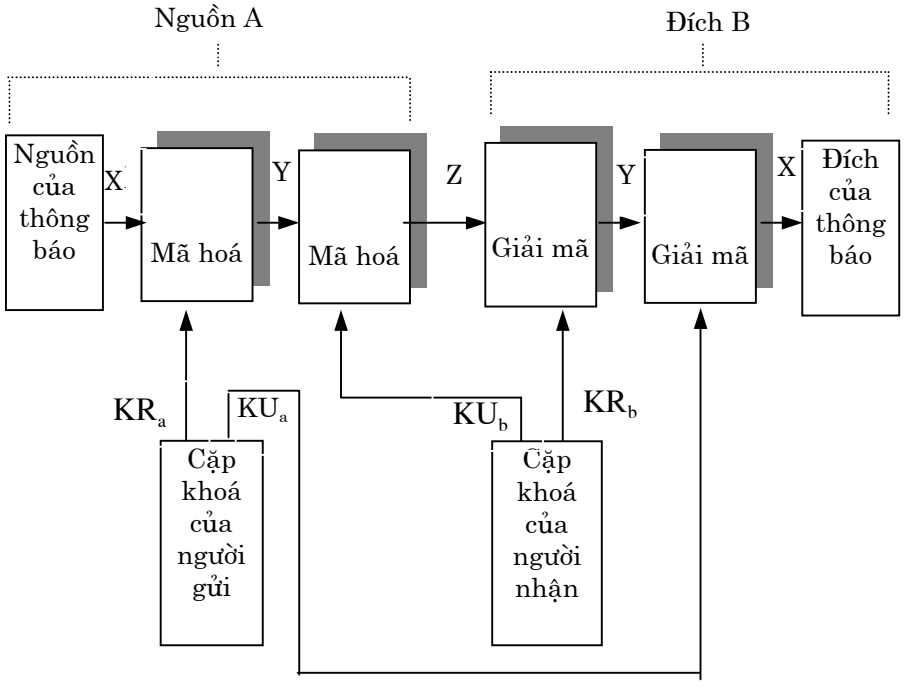
đổi của dấu xác thực. Nếu dấu xác thực được mã hoá bằng khoá riêng của người gửi, nó được sử dụng như một chữ ký. Chữ ký được sử dụng để kiểm tra nguồn gốc và nội dung thông báo.

Việc sử dụng lược đồ mã hoá khoá công khai có thể đảm bảo tính xác thực và bí mật được trình bày trong hình 1.4:

$$Z = E_{KUb}[E_{KRa}(X)]$$

$$X = D_{KUa}[D_{KRb}(Z)]$$

Trước hết, chúng ta mã hoá một thông báo bằng khoá riêng của người gửi, đưa ra một chữ ký số. Tiếp theo, mã hoá một lần nữa bằng khoá công khai của người nhận. Chỉ có người nhận hợp pháp mới giải mã được bản mã cuối cùng này vì anh ta có khoá riêng cùng cặp. Như vậy sẽ đảm bảo được tính bí mật. Khó khăn của biện pháp này là thuật toán khoá công khai, nó thực sự phức tạp, phải tiến hành 4 lần (chứ không phải là 2 lần) cho mỗi cuộc truyền thông .



Hình 1.4. Lược đồ mã hoá khoá công khai: Bí mật và xác thực

Như đã được trình bày ở trên, một đặc điểm của mã hoá khoá công khai là khoá công khai được công bố công khai và khoá riêng cùng cặp được người chủ sở hữu lưu giữ bí mật. Do vậy, vấn đề đặt ra là khoá công khai được phân phối như thế nào, tuy biết rằng nó được công bố công khai, bất cứ

người sử dụng cũng có thể lấy được khoá công khai khi muốn sử dụng nó, nhưng cần phải sử dụng một cơ chế nào đó để xác thực rằng, khoá công khai đó chính là của người gửi thông báo hoặc người nhận thông báo chủ định; và khoá công khai này cùng cặp với khoá riêng của họ.

Vấn đề phân phối khoá công khai được giải quyết thông qua nhiều kỹ thuật phân phối khoá công khai như khai báo công khai, thư mục công khai, trung tâm quản lý khoá công khai và chứng chỉ khoá công khai.

Hiện nay người ta chủ yếu sử dụng hệ thống chứng chỉ khoá công khai để phân phối khoá công khai. Sau đây, chúng ta sẽ đi xem xét chi tiết kỹ thuật phân phối khoá công khai này.

Mỗi chứng chỉ có chứa một khoá công khai và các thông tin khác. Nó được một cơ quan quản lý chứng chỉ tạo ra và phát hành cho các thành viên. Mỗi thành viên chuyển thông tin khoá công khai của mình cho thành viên khác thông qua chứng chỉ. Các thành viên khác có thể kiểm tra chứng chỉ do cơ quan quản lý tạo ra.

Yêu cầu đối với các thành viên và cơ quan quản lý như sau:

1. Một thành viên có thể đọc chứng chỉ để xác định tên và khoá công khai của người sở hữu chứng chỉ.
2. Mọi thành viên có thể kiểm tra: nguồn gốc của chứng chỉ và nó có bị giả mạo không.
3. Chỉ có cơ quan quản lý chứng chỉ mới có thể tạo ra và cập nhật các chứng chỉ.

Và một yêu cầu được bổ sung thêm là:

4. Mọi thành viên có thể kiểm tra sự lưu hành của chứng chỉ.

Hình 1.5 minh hoạ một lược đồ phân phối chứng chỉ. Trong đó, mỗi thành viên yêu cầu cơ quan quản lý chứng chỉ cung cấp một khoá công khai và một chứng chỉ. Đối với thành viên A, cơ quan quản lý cung cấp cho A một chứng chỉ như sau:

$C_A = E_{KRauth}[T, ID_A, KU_a]$

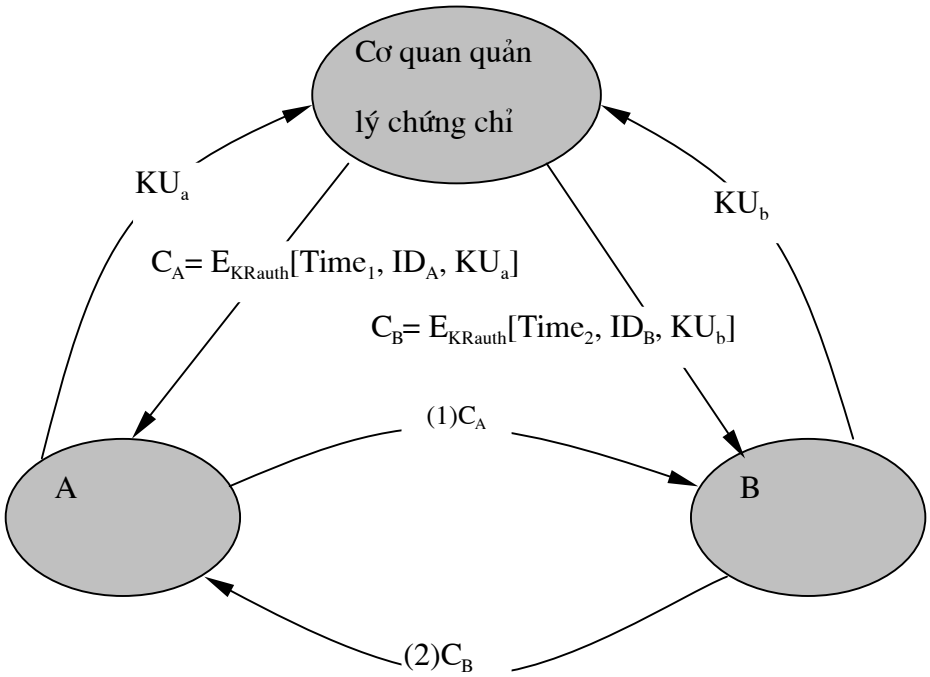
KR_{auth} là khoá riêng được cơ quan quản lý sử dụng. Sau đó, A có thể chuyển chứng chỉ này cho thành viên khác, thành viên này đọc và kiểm tra chứng chỉ như sau:

$D_{KUauth}[C_A] = D_{KUauth}[E_{KRauth}[T, ID_A, KU_a] = (T, ID_A, KU_a)$

Người nhận sử dụng khoá công khai của cơ quan quản lý (KU_{auth}) để giải mã chứng chỉ. Do chỉ có thể đọc chứng chỉ bằng cách sử dụng khoá công khai của cơ quan quản lý nên việc kiểm tra này chứng tỏ rằng: chứng chỉ có nguồn gốc từ cơ quan quản lý chứng chỉ.

ID_A và KU_a cung cấp cho người nhận tên và khoá công khai của người nắm giữ chứng chỉ.

Nhãn thời gian T phê chuẩn sự lưu hành của chứng chỉ. Nó được sử dụng để đối phó khi khoá riêng của A bị lộ. A sinh ra một cặp khoá mới và yêu cầu cơ quan quản lý chứng chỉ cấp một chứng chỉ mới. Trong lúc đó, đối phương vẫn sử dụng chứng chỉ cũ với B. Sau đó, nếu B mã hoá các thông báo bằng khoá công khai cũ, đối phương có thể đọc toàn bộ các thông báo này.



Hình 1.5. Trao đổi các chứng chỉ khoá công khai

1.2 Xác thực thông báo và các hàm băm

Xác thực thông báo là một thủ tục nhằm kiểm tra các thông báo nhận được, xem chúng có đến từ một nguồn hợp lệ và có bị sửa đổi hay không. Xác thực thông báo cũng có thể kiểm tra trình tự và tính đúng lúc. Chữ ký số là một kỹ thuật xác thực, nó cũng bao gồm nhiều biện pháp để chống lại việc chối bỏ đã gửi hay nhận thông báo của hai bên gửi và nhận.

Tiếp theo, chúng ta xem xét các hàm có thể được sử dụng để tạo ra dấu xác thực (một giá trị dùng để xác thực một thông báo). Chúng có thể được nhóm thành 3 loại là mã hoá thông báo, mã xác thực thông báo (MAC) và hàm băm.

Loại mã hoá thông báo

Bản mã của toàn bộ thông báo được sử dụng làm dấu xác thực của chính nó. Hình 1.6 minh hoạ các sử dụng cơ bản của mã hoá thông báo. Tiếp theo chúng ta phân tích sự khác nhau của hai lược đồ mã hoá đối xứng và mã hoá khoá công khai.

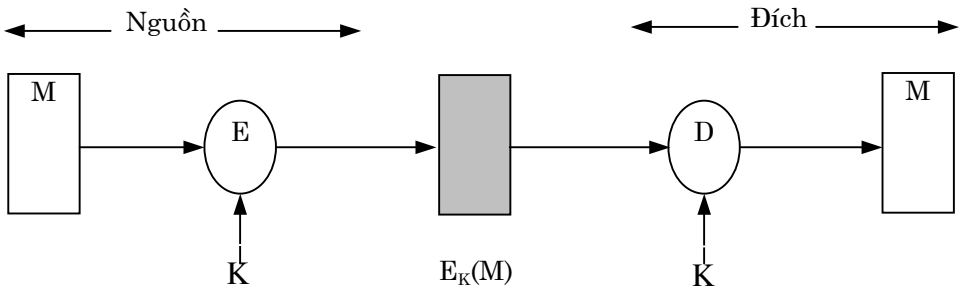
Trong mã hoá đối xứng, thông báo đi từ nguồn A đến đích B được mã hoá, bằng cách sử dụng một khoá bí mật K giữa A và B.

Tính bí mật được đảm bảo khi không một thành viên nào khác biết được khoá này và họ không thể khôi phục lại bản rõ của thông báo. Hơn nữa, B được đảm bảo rằng thông báo B nhận được do A sinh ra và nó không bị sửa đổi. Mọi sửa đổi trên bản mã đều bị B phát hiện.

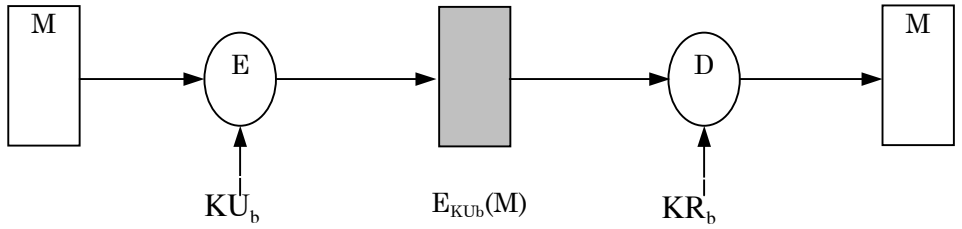
Mã hoá đối xứng cũng cung cấp tính xác thực. Tuy nhiên, điều này cũng cần được xem xét cẩn thận. Chúng ta quan sát những gì xảy ra ở đích B. Biết trước hàm giải mã D và khoá bí mật K, với một đầu vào X bất kỳ, chúng ta có đầu ra như sau $Y= D_K(X)$. Nếu X là bản mã của thông báo gốc M thì đầu ra Y chính là bản rõ của thông báo đó. Nếu không, Y sẽ là một chuỗi bit vô nghĩa. B cần có một số hình thức xác định tự động, Y có phải là bản rõ đích thực hay không, nếu đúng thì nó có nguồn gốc từ A.

Mã hoá khoá công khai cung cấp tính bí mật nhưng không cung cấp tính xác thực. Nguồn A sử dụng khoá công khai (KU_b) của đích B để mã hoá thông báo M. Do B có khoá riêng tương ứng (KR_b) nên chỉ B mới có thể giải mã thông báo. Lược đồ này không cung cấp tính xác thực, bởi vì bất kỳ người nào cũng có thể sử dụng khoá công khai của B để mã hoá thông báo, tự nhận mình là A.

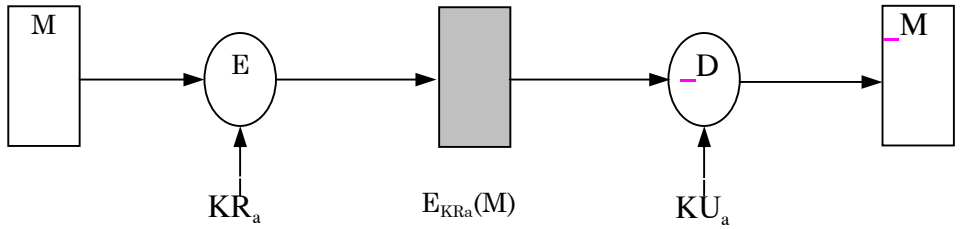
Để đảm bảo tính xác thực, A sử dụng khoá riêng của mình để mã thông báo và B sử dụng khoá công khai của A để giải mã (hình 1.6c). Cũng lập luận như trong trường hợp mã hoá đối xứng - thông báo phải có nguồn gốc từ A, do A là thành viên duy nhất sở hữu khoá KR_a. A sử dụng KR_a và các thông tin cần thiết để tạo ra bản mã. Bản mã được giải mã bằng khoá KU_a. Một lập luận nữa là cần phải có một cấu trúc bên trong nào đó cho bản rõ, qua đó người nhận có thể phân biệt bản rõ được định dạng trước với các bit ngẫu nhiên.



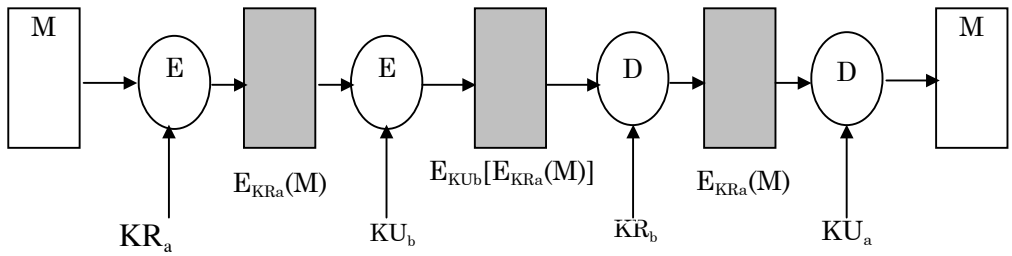
(a)Mã hoá đối xứng: bí mật và xác thực



(b)Mã hoá khoá công khai: bí mật



(c)Mã hoá khoá công khai: xác thực và chữ ký



(d) Mã hoá khoá công khai: bí mật, xác thực và chữ ký

Hình 1.6.Các dạng mã hoá thông báo cơ bản

Giả sử có một cấu trúc như vậy thì lược đồ trong hình 1.6c cung cấp tính xác thực và chữ ký số. A là thành viên duy nhất tạo ra bản mã vì A sở hữu khoá KR_a. Thậm chí cả người nhận B cũng không thể tạo ra bản mã. Vì vậy, nếu B có bản mã, B cần chứng minh thông báo có nguồn gốc từ A. Thực tế là A đã "ký" thông báo bằng khoá riêng.

Lưu ý rằng, lược đồ này không cung cấp tính bí mật vì bất cứ ai sở hữu khoá công khai của A cũng có thể giải được bản mã.

Để đảm bảo cả tính bí mật lẫn xác thực, trước tiên A mã thông báo M bằng khoá riêng của A (nhằm cung cấp chữ ký số), sau đó là khoá công khai của B (đảm bảo tính bí mật). Khó khăn của giải pháp này là thuật toán khoá công khai phức tạp, phải thực hiện 4 lần (chứ không phải là 2 lần) cho mỗi cuộc truyền thông.

Loại dùng MAC

Một kỹ thuật xác thực (mang tính lựa chọn) như sau: sử dụng một khoá bí mật để tạo ra một khối dữ liệu nhỏ có kích thước cố định (được gọi là MAC, đây là các chữ cái đầu của Message Authentication Code, hay mã xác thực thông báo). MAC được gắn với thông báo.

Kỹ thuật này tiến hành như sau: hai thành viên, chẳng hạn là A và B, có chung một khoá bí mật K. Khi A muốn gửi một thông báo cho B, A tính toán MAC như sau: $MAC = C_K(M)$. Thông báo cùng với MAC được gửi cho B. B tiến hành tính toán tương tự trên thông báo nhận được bằng cách sử dụng khoá bí mật giữa A và B để tạo ra một MAC mới. So sánh MAC đi kèm với thông báo và MAC do B tính ra (hình 1.7a). Tổng quát hoá, nếu chỉ có người nhận và người gửi biết khoá bí mật, đồng thời MAC nhận được trùng khớp với MAC mới tính toán, thì:

1. *Người nhận được đảm bảo thông báo không bị sửa đổi. Nếu đối tượng tấn công sửa đổi thông báo nhưng không sửa đổi MAC, thì giá trị MAC mới (do người nhận tính toán) sẽ không trùng khớp với MAC đi kèm với thông báo. Do giả thiết đối tượng tấn công không biết khoá bí mật nên không thể sửa đổi MAC sao cho phù hợp với mọi sửa đổi trên thông báo.*

Người nhận được đảm bảo rằng thông báo có nguồn gốc từ người gửi hợp pháp. Do không ai khác (ngoài người gửi và người nhận chủ định) biết khoá bí mật, nên không ai có thể chuẩn bị thông báo với một MAC hợp lệ.

Một biến thể của MAC là hàm băm một chiều. Hàm băm có đầu vào là thông báo M có kích thước thay đổi, đầu ra là một mã băm H(M) có kích thước cố định. Đôi khi người ta còn gọi đầu ra của hàm băm là tóm lược thông báo. Mã băm là một hàm của tất cả các bit có trong thông báo, đồng thời nó cung cấp khả năng phát hiện lỗi: nếu A thay đổi một bit bất kỳ hoặc nhiều bit trong thông báo dẫn đến kết quả là mã băm cũng thay đổi theo.

Mục đích của hàm băm là tạo ra một "dấu vân tay" cho một tệp, một thông báo, hoặc khối dữ liệu. Để đáp ứng được việc xác thực thông báo, một hàm băm H phải bao gồm các tính chất sau đây:

7. H được áp dụng cho một khối dữ liệu có kích cỡ bất kỳ.
8. Đầu ra của H có độ dài cố định.
9. Dễ dàng tính toán được H(x) với mọi x cho trước.
10. Với mọi mã h cho trước, không thể tìm được x sao cho H(x)=h. Đôi khi, tính chất này còn được gọi là tính chất một chiều.
11. Với mọi khối x cho trước, không thể tìm được $y \neq x$ sao cho H(y)=H(x). Đôi khi, tính chất này được gọi là va chạm yếu (khả năng trùng ít).
12. Không thể tìm được bất cứ cặp (x,y) nào sao cho H(x)=H(y). Tính chất này được gọi là va chạm mạnh.

Hình 1.8 minh hoạ các sử dụng cơ bản của mã băm để đảm bảo xác thực thông báo, như sau:

a. *Thông báo cùng với mã băm được mã hoá với một khoá bí mật, sử dụng mã hoá đối xứng. Với cùng lập luận như sau: do A và B cùng sử dụng một khoá bí mật, nên thông báo phải có nguồn gốc từ A và không bị sửa đổi. Mã băm cung cấp cấu trúc hoặc phép kiểm tra dư thừa nhằm đảm bảo xác thực. Do mã hoá được áp dụng cho toàn bộ thông báo và mã băm nên đảm bảo được tính bí mật.*

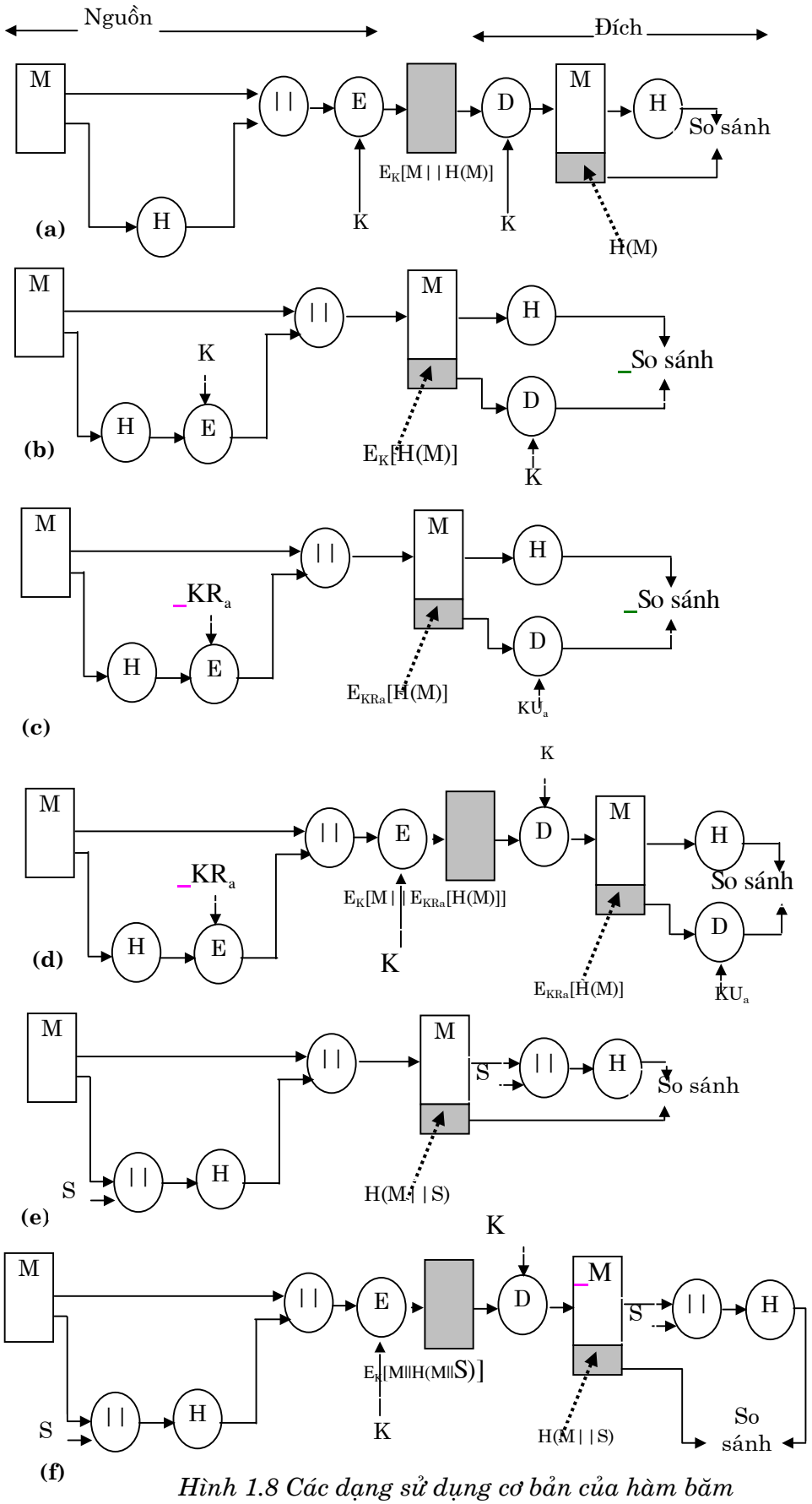
b. *Chỉ mã hoá mã băm với khoá bí mật, sử dụng mã hoá đối xứng. Lưu ý rằng, trong thực tế, việc kết hợp các kết quả băm và mã hoá chính là MAC (hình 1.7a). Có nghĩa là, $E_K[H(M)]$ là một hàm của thông báo M (thông báo này có độ dài thay đổi) và một khoá bí mật K, nó tạo ra một đầu ra có kích thước cố định. Đối phương không biết khoá bí mật nên không thể biết đầu ra này.*

c. *Chỉ mã hoá mã băm với khoá riêng của người gửi, sử dụng mã hoá khoá công khai. Giống như (b), nó đảm bảo tính xác thực. Nó cũng cung cấp chữ ký số, bởi vì chỉ có người gửi mới có thể đưa ra mã băm mã hoá. Trong thực tế, đây chính là bản chất của kỹ thuật chữ ký số.*

d. *Để đảm bảo tính bí mật và cung cấp chữ ký số, thông báo cùng với mã băm (mã băm này đã được mã hoá bằng khoá công khai) có thể được mã hoá, bằng cách sử dụng một khoá bí mật.*

e. *Sử dụng một hàm băm (nhưng không mã hoá) khi xác thực thông báo. Quá trình như sau: hai thành viên tham gia truyền thông sử dụng chung một giá trị bí mật S. A tính toán giá trị băm từ M và S, sau đó gắn giá trị băm này vào M. Do B sở hữu S, B có thể tính toán lại giá trị băm để kiểm tra. Do giá trị bí mật S không được gửi đi, đối phương không thể sửa đổi thông báo và tạo ra một thông báo giả.*

f. *Để bổ sung thêm tính bí mật vào (e), chúng ta có thể mã hoá toàn bộ thông báo cùng với mã băm.*



Hình 1.8 Các dạng sử dụng cơ bản của hàm băm

1.3 Chữ ký số

Các yêu cầu

Giả thiết A gửi một thông báo đã được xác thực cho B, bằng một trong các lược đồ được minh hoạ trong hình 1.7. Có thể xảy ra một số dạng tranh chấp giữa hai thành viên như sau:

1. B có thể làm giả một thông báo khác và tuyên bố rằng thông báo này có nguồn gốc từ A. B có thể tạo ra một thông báo và gắn mã xác thực một cách đơn giản bằng khoá chung của họ.
2. A có thể chối bỏ đã gửi thông báo. Vì B có thể làm giả thông báo và vì vậy không có cách nào để chứng minh A đã gửi thông báo.

Các tranh chấp xảy ra do giữa người gửi và người nhận không có sự tin cậy tuyệt đối. Giải pháp hiệu quả nhất cho vấn đề này là chữ ký số. Chữ ký số tương tự như chữ ký bằng tay. Nó phải có một số tính chất như sau:

1. Có khả năng kiểm tra người ký và thời gian ký.
2. Có khả năng xác thực các nội dung tại thời điểm ký.
3. Các thành viên thứ ba có thể kiểm tra chữ ký để giải quyết các tranh chấp.

Vì vậy, chức năng ký số bao hàm cả chức năng xác thực. Dựa vào các tính chất cơ bản này, chúng ta có thể đưa ra các yêu cầu sau đây đối với một chữ ký số:

1. Chữ ký phải là một mẫu bit phụ thuộc vào thông báo được ký.
2. Chữ ký phải sử dụng một thông tin duy nhất nào đó từ người gửi, nhằm ngăn chặn tình trạng làm giả và chối bỏ.
3. Tạo ra chữ ký số dễ dàng.
4. Dễ dàng nhận ra và kiểm tra chữ ký số.
5. Khó có thể làm giả chữ ký số bằng cách tạo ra một thông báo mới cho một chữ ký số hiện có, hoặc tạo ra một chữ ký số giả cho một thông báo cho trước.
6. Trong thực tế, cần phải lưu giữ một bản sao của chữ ký số.

Có rất nhiều hướng tiếp cận được đề xuất cho chữ ký số. Các hướng tiếp cận này chia thành 2 loại: chữ ký số trực tiếp và chữ ký số của thành viên thứ ba.

Chữ ký số trực tiếp

Chữ ký số trực tiếp chỉ có sự tham gia của các thành viên truyền thông (người gửi và người nhận). Giả thiết người gửi và người nhận biết khoá công

khai của nhau. Chữ ký số được tạo ra bằng cách mã hoá toàn bộ thông báo với khoá riêng của người gửi (hình 1.6c), hoặc mã hoá mã băm của thông báo với khoá riêng của người gửi (hình 1.8c).

Ngoài ra, để đảm bảo tính bí mật, có thể mã hoá toàn bộ thông báo và chữ ký với khoá công khai của người nhận (nếu dùng mã hoá khoá công khai), hoặc khoá bí mật giữa người gửi và người nhận (nếu dùng mã hoá đối xứng); ví dụ trong hình 1.6d và 1.8d. Để đảm bảo tính bí mật và xác thực, người gửi có thể tiến hành ký thông báo trước, sau đó mã hoá toàn bộ thông báo và chữ ký; hoặc ngược lại, mã hoá thông báo trước, sau đó mới tiến hành ký lên thông báo đã được mã hoá. Trong trường hợp xảy ra tranh chấp, cần có sự can thiệp của thành viên thứ 3 nào đó, thành viên này phải được xem thông báo và chữ ký. Trong cả hai trường hợp, ký trước- mã sau, hoặc mã trước- ký sau, thành viên thứ 3 này đều phải biết khoá riêng (hoặc khoá bí mật) của người gửi.

Tất cả các lược đồ trực tiếp đều có chung một điểm yếu là tính hợp lệ của lược đồ phụ thuộc vào sự an toàn của khoá riêng của người gửi. Sau đó, nếu người gửi muốn chối bỏ việc anh ta đã gửi một thông báo, anh ta có thể tuyên bố: khoá riêng bị mất hoặc bị đánh cắp, một người nào đó đã làm giả chữ ký của anh ta. Để ngăn chặn tình trạng này, cần phải thực hiện các biện pháp kiểm soát quản lý (liên quan đến sự an toàn của các khoá riêng), nhưng hiểm hoạ vẫn còn tồn tại. Ví dụ, yêu cầu tất cả các thông báo được ký phải có nhãn thời gian (ngày và giờ), yêu cầu báo cáo cho cơ quan trung tâm về tình trạng các khoá bị lộ.

Một đe doạ khác là khoá riêng nào đó có thể bị đánh cắp từ X tại thời điểm T. Sau đó, đối phương có thể gửi thông báo đã được ký với chữ ký của X và gán một nhãn thời gian trước hoặc đúng thời điểm T.

Chữ ký số của thành viên thứ ba-thành viên trọng tài

Có thể giải quyết các vấn đề liên quan đến chữ ký số trực tiếp nhờ một thành viên thứ ba. Có một số lược đồ chữ ký của thành viên thứ ba như sau:

Khi X muốn gửi các thông báo cho Y, X ký tất cả các thông báo, sau đó chuyển chúng cho thành viên thứ ba A trước khi gửi cho Y. A kiểm tra nguồn gốc, nội dung của thông báo và chữ ký của nó. Sau đó, thông báo được gán nhãn thời gian và gửi cho Y với chỉ báo là thông báo đã được thành viên thứ ba kiểm tra. Sự xuất hiện của A có thể giải quyết vấn đề (X chối bỏ thông báo) trong các lược đồ chữ ký số trực tiếp.

Thành viên thứ ba đóng một vai trò nhạy cảm và quyết định trong kiểu lược đồ này. Bảng 1.1 trình bày một số ví dụ về chữ ký số của thành viên thứ ba, được minh hoạ thông qua hình 1..

Kỹ thuật đầu tiên sử dụng mã hoá đối xứng. Giả định rằng, X và A có chung một khoá bí mật K_{xa}, A và Y có chung một khoá bí mật K_{ay}. X tạo ra một thông báo M và tính toán giá trị hàm băm H(M) của thông báo này. Sau đó, X gửi thông báo cùng với một chữ ký cho A. Chữ ký (gồm tên của X và giá trị băm) được mã hoá bằng khoá K_{xa}. A giải mã chữ ký và kiểm tra giá trị băm để xác nhận tính hợp lệ của thông báo. Sau đó A gửi cho Y một thông báo đã được mã hoá bằng K_{ay}.Thông báo bao gồm ID_X, thông báo gốc của X, chữ ký và một nhãn thời gian. Y có thể giải mã để khôi phục lại thông báo và chữ ký. Nhãn thời gian báo cho Y biết, thông báo đến đúng lúc và không phải là thông báo bị chuyển tiếp nhiều lần. Y có thể lưu giữ M và chữ ký. Trong trường hợp xảy ra tranh chấp, Y xác nhận đã nhận được thông báo M từ X, Y gửi cho A một thông báo như sau:

E_{Kay} [ID_X || M || E_{Kxa} [ID_X || H(M)]]

Bảng 1.1 Các kỹ thuật chữ ký số của thành viên thứ ba

Mã hoá đối xứng, thành viên thứ ba xem thông báo
$X \rightarrow A$: M || E_{Kxa}[ID_X|| H(M)] $A \rightarrow Y$: E_{Kay}[ID_X || M || E_{Kxa}[ID_X|| H(M)] || T]
Mã hoá đối xứng, thành viên thứ ba không xem thông báo

$X \rightarrow A: ID_X \| E_{Kxy}[M] \| E_{Kxa}[ID_X \| H(E_{Kxy}[M])]$ $A \rightarrow Y: E_{Kay}[ID_X \| E_{Kxy}[M] \| E_{Kxa}[ID_X \| H(E_{Kxy}[M])] \| T]$
Mã hoá khoá công khai, thành viên thứ ba không xem thông báo
$X \rightarrow A: ID_X \| E_{KRx}[ID_X \| E_{KUy}(E_{KRx}[M])]$ $A \rightarrow Y: E_{KRa}[ID_X \| E_{KUy}[E_{KRx}[M]] \| T]$

Thành viên thứ ba sử dụng K_{ay} để khôi phục lại ID_X, M và chữ ký, sau đó sử dụng K_{xa} để giải mã chữ ký và kiểm tra mã băm. Trong lược đồ này, Y không thể kiểm tra trực tiếp chữ ký của X. Chính vì vậy, chỉ có chữ ký mới giải quyết được tranh chấp. Y quan tâm đến tính đích thực của thông báo (của X) vì nó được gửi đến từ A. Trong trường hợp này, cả hai phía đều phải tin cậy vào A:

- X phải tin cậy A không làm lộ K_{xa} và không tạo ra các chữ ký (theo dạng $E_{Kxa}[ID_X \| H(M)]$) giả.
- Y phải tin cậy A chỉ gửi $E_{Kay}[ID_X \| M \| E_{Kxa}[ID_X \| H(M)] \| T]$ khi nào giá trị băm đúng và chữ ký do X tạo ra.
- Cả hai phải tin cậy A giải quyết tranh chấp công bằng.

Nếu A đáp ứng được sự tin cậy này thì X được đảm bảo rằng không một ai có thể làm giả chữ ký của anh ta, đồng thời Y được đảm bảo X không thể chối bỏ chữ ký của anh ta. Trong trường hợp này, đối tượng nghe trộm vẫn có thể đọc được các thông báo X gửi cho Y. Trường hợp thứ hai có thể đảm bảo cả tính bí mật. Giả định rằng, X và Y cùng sử dụng khoá bí mật K_{xy}. X gửi cho A tên của X, một bản sao của thông báo đã được mã hoá bằng khoá K_{xy} và một chữ ký. Chữ ký (gồm tên của X và giá trị băm của thông báo đã được mã hoá) được mã hoá bằng khoá K_{xa}. Do vậy, A giải mã chữ ký và kiểm tra giá trị băm để xác nhận tính hợp lệ của thông báo. Trong trường hợp này, A chỉ làm việc với bản sao của thông báo đã được mã hoá, chính vì vậy A không thể xem thông báo. Sau đó, A mã hoá mọi thứ (mà A nhận được từ X), cùng với một nhãn thời gian bằng khoá K_{ay}, rồi gửi chúng cho Y.

Mặc dù không xem được thông báo nhưng thành viên thứ ba vẫn có thể ngăn chặn được tình trạng gian lận của một trong hai phía, X hoặc Y. Một vấn đề tồn tại (như trong trường hợp đầu tiên) là thành viên thứ ba có thể liên kết với

người gửi chối bỏ một thông báo đã được ký, hoặc liên kết với người nhận làm giả chữ ký của người gửi.

Có thể giải quyết được tất cả các vấn đề này, bằng một lược đồ khoá công khai. Trong trường hợp này, X mã hoá thông báo M hai lần, lần thứ nhất bằng khoá riêng của X (KR_X), lần thứ hai bằng khoá công khai của Y (KU_Y). Đây chính là một bản sao bí mật của thông báo đã được ký. Thông báo này cùng với ID_X được mã bằng khoá KR_X, sau đó đều được gửi đến A.

Thông báo (được mã hoá hai lần liên tiếp) được giữ bí mật, thành viên thứ ba (cũng như mọi thành viên khác trừ Y) không thể xem nó. Tuy nhiên, A có thể giải mã thông báo (được mã hoá sau đó) để đảm bảo rằng thông báo có nguồn gốc từ X (bởi vì chỉ X có KR_X). A kiểm tra để đảm bảo rằng - cặp khoá (công khai/riêng) của X vẫn còn hợp lệ. Sau đó, A gửi cho Y một thông báo và thông báo này được mã hoá bằng khoá KR_a. Thông báo bao gồm ID_X, thông báo được mã hoá hai lần liên tiếp và một nhãn thời gian.

> Lược đồ này có một số thuận lợi so với hai lược đồ trước. Thứ nhất, các thành viên không phải chia sẻ thông tin trước khi liên lạc, vì thế có thể ngăn chặn tình trạng liên kết gian lận. Thứ hai, không thể gửi các thông báo có thời gian không hợp lệ. Cuối cùng, nội dung của thông báo (X gửi cho Y) được giữ bí mật, A cũng như mọi thành viên khác không thể xem nó.

Chuẩn chữ ký DSS

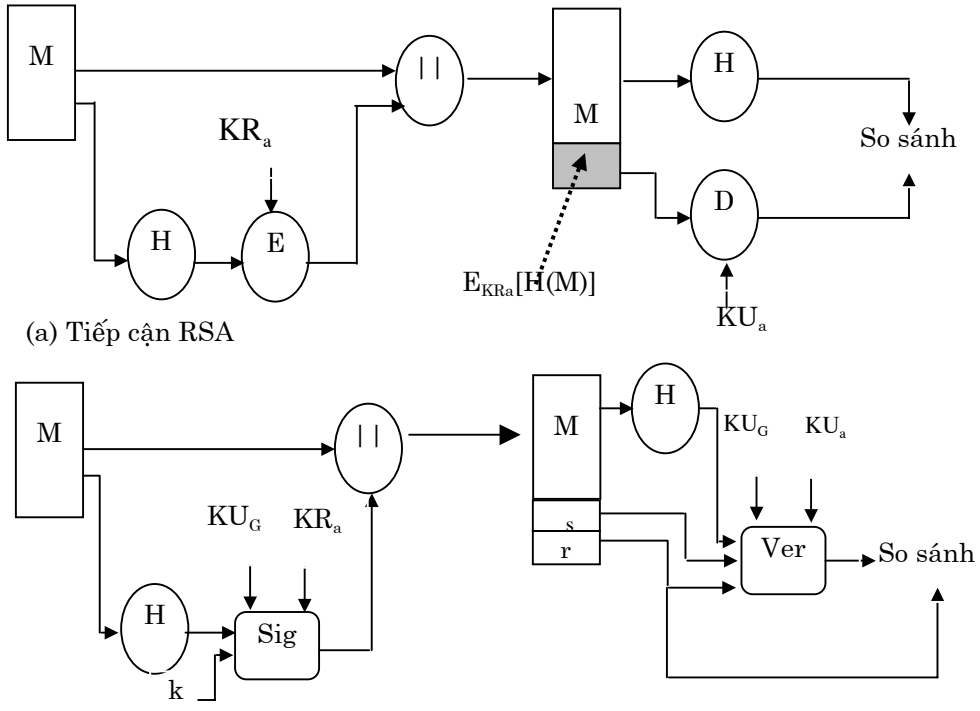
Chuẩn chữ ký số (DSS) được NIST (Viện tiêu chuẩn và công nghệ Quốc gia) công bố. DSS sử dụng thuật toán băm an toàn (SHA) và đưa ra thuật toán ký số (DSA). DSS được đề xuất lần đầu tiên vào năm 1991, lần tiếp theo vào năm 1993 và lần gần đây vào năm 1996.

DSS sử dụng một thuật toán cung cấp duy nhất chức năng chữ ký số. Không giống RSA, nó không được sử dụng cho để mã hoá, hoặc trao đổi khoá. Tuy nhiên, nó là một kỹ thuật khoá công khai.

Hình 1.9 trình bày sự khác nhau trong quá trình sinh chữ ký số của RSA và DSS. Trong RSA, thông báo chính là đầu vào của hàm băm. Đầu ra là một mã băm có độ dài cố định. Sau đó, mã băm được mã hoá bằng khoá riêng của người gửi để tạo ra chữ ký. Cuối cùng, thông báo cùng với chữ ký được gửi đi. Người nhận lấy thông báo và tính toán một mã băm, đồng thời giải mã chữ ký bằng khoá công khai của người gửi. Nếu mã băm vừa được tính toán trùng

khớp với phần chữ ký được giải mã, chữ ký được công nhận là hợp lệ. Do người gửi biết khoá riêng nên chỉ người gửi có thể đưa ra chữ ký hợp lệ.

DSS cũng sử dụng một hàm băm. Mã băm cùng với một số ngẫu nhiên *k* (k được sinh ra cho từng chữ ký riêng biệt) là các đầu vào của một hàm ký. Hàm ký cũng phụ thuộc vào khoá riêng của người gửi (KR_a) và một tập hợp các tham số (của một nhóm các chủ thể truyền thông) tạo thành một khoá công khai toàn cục (KU_G). Kết quả là chữ ký có hai thành phần, được gọi là *s* và *r*.



(a) Tiếp cận RSA

(b) Tiếp cận DSS

Hình 1.9. Hai tiếp cận chữ ký số

Tại nơi nhận, người nhận tính toán mã băm của thông báo gửi đến. Mã băm này cùng với chữ ký là các đầu vào của hàm kiểm tra. Hàm kiểm tra cũng phụ thuộc vào KU_G và khoá công khai KU_a của người gửi (KU_a và KR_a là hai khoá của cùng một cặp khoá). Đầu ra của hàm kiểm tra là một giá trị, nếu giá trị này trùng khớp với thành phần *r* của chữ ký, thì chữ ký được công nhận là hợp lệ. Do duy nhất người gửi biết khoá riêng nên chỉ người gửi có thể đưa ra chữ

ký hợp lệ. Chúng ta sẽ xem xét chi tiết thuật toán chữ ký số trong mục tiếp theo.

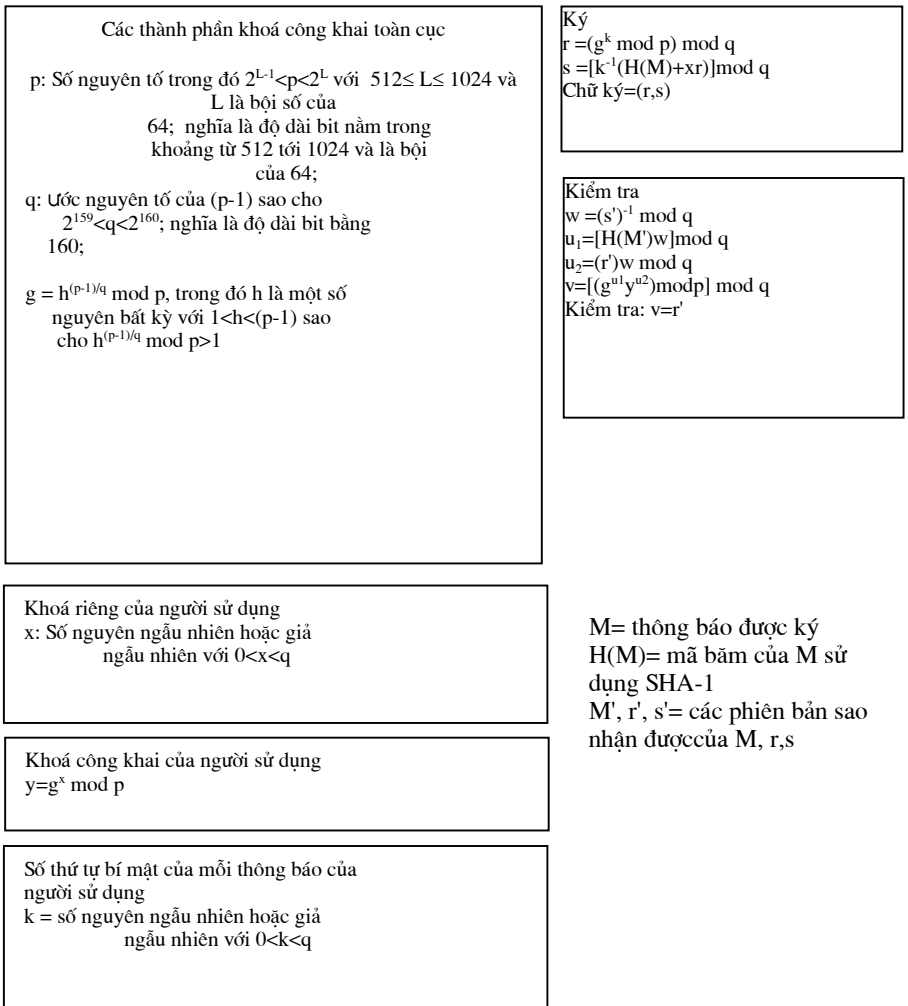
Thuật toán chữ ký số

DSA dựa vào độ phức tạp tính toán logarit rời rạc và các lược đồ do ElGamal và Schnorr đưa ra.

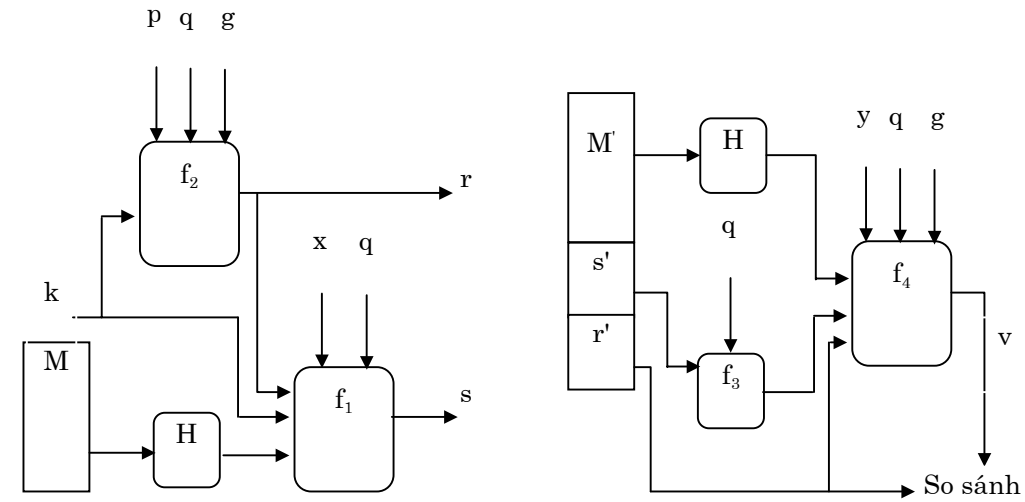
Hình 1.10 trình bày tóm tắt thuật toán. ở đây có 3 tham số công khai và có thể là sở hữu chung của một nhóm người sử dụng. Chọn một số nguyên tố *q* có độ dài 160 bit, tiếp theo chọn một số *p* có độ dài nằm trong khoảng từ 512 tới 1024 bit sao cho *q* chia hết cho *(p-1)*. Cuối cùng, chọn $g = h^{(p-1)/q} \ mod \ p$, với *h* là một số nguyên nằm trong khoảng từ 1 tới (*p-1*) trong đó g phải lớn hơn 1.

Với các số đã chọn, người sử dụng chọn một khoá riêng và sinh ra một khoá công khai. Khoá riêng *x* phải là một số nằm trong khoảng từ 1 tới (*q-1*) và nên được chọn ngẫu nhiên hoặc giả ngẫu nhiên. Khoá công khai được tính toán từ khoá riêng như sau: $y=g^x \ mod \ p$.

Dễ dàng tính toán được *y* từ *x* cho trước. Tuy nhiên, nếu biết trước khoá công khai *y*, việc tính toán *x* lại không khả thi.



Hình 1.10 Thuật toán ký số (DSA)



Hình 1.11. Qui trình ký và kiểm tra chữ ký của DSS

Để tạo ra một chữ ký, người sử dụng tính toán *r* và *s*, chúng là các hàm của các thành phần khoá công khai (*p*, *q*, *g*), khoá riêng của người sử dụng (*x*), mã băm của thông báo, H(M) và số nguyên *k* (*k* được sinh ra ngẫu nhiên hoặc giả ngẫu nhiên, là số duy nhất cho mỗi lần ký).

Tại nơi nhận, người nhận tạo ra *v*. *v* là một hàm của các thành phần khoá công khai, khoá công khai của người gửi và mã băm của thông báo nhận được. Nếu *v* trùng khớp với *r* thì chữ ký được xác nhận hợp lệ.

Hình 1.11 mô tả các hàm ký và kiểm tra. Trong đó, cấu trúc của thuật toán khá hấp dẫn. Lưu ý rằng, việc kiểm tra tại đích dựa vào việc tính toán giá trị *r*, nó hoàn toàn không phụ thuộc vào thông báo. *r* là một hàm của *k* và 3 thành phần khoá công khai toàn cục. *s* được tính như sau: $s = (k^{1}(H(M) + xr)) \bmod q$ trong đó k^{-1} là phần tử nghịch đảo của k đối với phép nhân. Cấu trúc của hàm này giúp người nhận khôi phục lại *r* từ thông báo nhận được, chữ ký, khoá công khai của người sử dụng và khoá công khai toàn cục. Việc khôi phục *k* từ *r* hoặc khôi phục *x* từ *s* là không khả thi.

Có một điểm cần lưu ý trong quá trình ký là việc tính toán số mũ $g^k \bmod p$. Do giá trị này không phụ thuộc vào thông báo được ký, nó có thể được tính toán trước. Thực vậy, người sử dụng có thể tính toán trước một số các giá trị của *r*, khi cần thiết có thể sử dụng các giá trị này để ký các tài liệu.

PHẦN B

CƠ SỞ PHÁP LÝ CHO CHỮ KÝ SỐ

Để đảm bảo cơ sở pháp lý cho các chữ ký điện tử nói chung, chữ ký số nói riêng, Liên Hợp Quốc đã biên soạn và phê chuẩn Luật mẫu về Chữ ký điện tử, đây là văn kiện pháp lý thực sự hiệu quả trong việc xúc tiến việc phát triển thương mại điện tử toàn cầu. Thông qua nó, nhiều Quốc gia có thể xây dựng luật chữ ký điện tử cho riêng mình. Đi kèm với Luật mẫu là bản hướng dẫn ban hành luật, giải thích chi tiết các điều khoản có trong Luật mẫu này, khi xem xét bản hướng dẫn ban hành luật, chúng ta có thể thấy được các hướng dẫn cụ thể về công nghệ cho các chữ ký số như đã được trình bày trong phần A, vai trò cũng như trách nhiệm pháp lý, nghĩa vụ của các thành viên tham gia.

Trong phần này, chúng tôi tập trung vào tìm hiểu những nội dung chủ yếu của đạo luật mẫu về chữ ký điện tử đã được Liên hợp quốc công bố. Nó sẽ cho ta hiểu rõ hơn khung pháp lý về chữ ký điện tử. Những điểm chính khi giải quyết vấn đề này là gì và cách giải quyết ra sao. Trong tài liệu này không có tham vọng đưa ra được một khung pháp lý cho chữ ký điện tử của Việt nam mà chủ yếu là những tham khảo về khung pháp lý mà thôi. Đây cũng là một việc làm cần thiết vì cho đến thời điểm hiện nay vấn đề này đang còn là thời sự ở nước ta.

Phần I

LUẬT MẪU VỀ CHỮ KÝ ĐIỆN TỬ CỦA UNCITRAL (2001)

Mục 1: Phạm vi ứng dụng

Luật này áp dụng cho các chữ ký điện tử được sử dụng trong phạm vi * hoạt động thương mại **. Tuân thủ mục đích bảo vệ các khách hàng.

* Uỷ ban đề nghị đoạn văn bản dưới đây dành cho các nước mong muốn mở rộng khả năng áp dụng đối với luật này:

" Luật này áp dụng khi các chữ ký điện tử được sử dụng, ngoại trừ các trường hợp ."

** Thuật ngữ "thương mại" nên được làm sáng tỏ để bao trùm lên các vấn đề xuất phát từ các mối quan hệ tự nhiên trong thương mại, cho dù có hợp đồng hay không. Các quan hệ tự nhiên trong thương mại bao gồm các giao dịch sau, nhưng không chỉ giới hạn trong đó: mọi giao dịch được thực hiện để cung cấp hoặc trao đổi hàng hoá hoặc dịch vụ; thoả thuận phân phối; đại diện hoặc đại lý thương mại; phương pháp đại lý; thuê tài sản; tư vấn; kỹ thuật; đăng ký; đầu tư; tài chính; ngân hàng; bảo hiểm; thoả thuận hoặc đặc quyền khai thác; liên doanh và các dạng hợp tác kinh doanh; vận chuyển hàng hoá hoặc hành khách thông qua các hình thức như hàng không, đường biển, đường sắt hoặc đường bộ.

Mục 2: Các định nghĩa

Phù hợp với các mục đích của luật này:

(a) Chữ ký điện tử

Là dữ liệu được lưu giữ ở dạng điện tử, được gắn vào một thông báo để nhận dạng người ký, chỉ ra rằng thông tin có trong thông báo đã được người ký phê chuẩn.

(b) Chứng chỉ

Là thông báo hoặc bản ghi, được sử dụng để xác nhận mối liên kết giữa người ký và dữ liệu tạo chữ ký.

(c) Thông báo dữ liệu

Là thông tin được tạo ra, gửi/nhận, lưu giữ bằng các hình thức điện tử, quang học, hoặc các hình thức khác như EDI (trao đổi dữ liệu điện tử), thư tín điện tử, điện tín, telex.

(d) Người ký

Là người nắm giữ dữ liệu tạo chữ ký, đại diện cho chính bản thân người ký hoặc đại diện cho người khác.

(e) Nhà cung cấp dịch vụ chứng thực

Là người phát hành các chứng chỉ và có thể cung cấp các dịch vụ khác liên quan đến các chữ ký điện tử.

(f) Thành viên tin cậy

Là người có thể hoạt động dựa vào chứng chỉ hoặc chữ ký điện tử.

Mục 3: Đối xử bình đẳng đối với các công nghệ chữ ký

Không có điều gì trong luật này, ngoại trừ mục 5, được áp dụng để loại trừ, giới hạn hoặc lấy đi phương pháp tạo ra một chữ ký điện tử mà thoả mãn các yêu cầu được đưa ra trong mục 6 (1), hoặc đáp ứng các yêu cầu của luật có thể áp dụng.

Mục 4: Làm sáng tỏ

1) Khi làm sáng tỏ luật này, mối quan tâm là nguồn gốc Quốc tế của nó, không có sự phân biệt trong việc xúc tiến ứng dụng của nó và tuân theo thiện ý.

2) Các câu hỏi liên quan đến những vấn đề mà luật này chi phối (không được giải quyết triệt để trong luật này) được giải quyết phù hợp với các nguyên tắc chung mà luật này dựa vào.

Mục 5: Thay đổi thông qua thoả thuận

Các điều khoản trong luật này có thể giảm đi hoặc hiệu lực của chúng có thể được thay đổi thông qua thoả thuận, trừ khi thoả thuận này không hợp lệ, hoặc không có hiệu lực theo luật có thể áp dụng.

Mục 6: Phù hợp với yêu cầu dành cho một chữ ký

1) Khi luật yêu cầu chữ ký của một người, yêu cầu này được thoả mãn, thông qua quan hệ với một thông báo dữ liệu nếu một chữ ký điện tử tin cậy được sử dụng tin cậy, phù hợp với mục đích - trong đó, thông báo dữ liệu được tạo ra và truyền đi, dưới ánh sáng của tất cả các trường hợp, bao gồm mọi thoả thuận liên quan.
2) Đoạn (1) áp dụng khi yêu cầu nằm trong giao ước hoặc luật đưa ra hậu quả của việc thiếu chữ ký.
3) Một chữ ký điện tử được xem là tin cậy cho mục đích thoả mãn yêu cầu được đưa ra trong đoạn (1) nếu:
   (a) dữ liệu tạo chữ ký (trong phạm vi nó được sử dụng) được liên kết với người ký, ngoài ra không có người nào khác;
   (b) tại thời điểm ký, không người nào khác ngoài người ký kiểm soát dữ liệu tạo chữ ký;
   (c) có thể phát hiện được mọi sửa đổi đối với chữ ký điện tử sau thời điểm ký; và
   (d) vì mục đích của yêu cầu pháp lý đối với một chữ ký là đảm bảo tính toàn vẹn của thông tin liên quan tới chữ ký, có thể phát hiện được mọi sửa đổi đối với thông tin này sau thời điểm ký.
4) Đoạn (3) không hạn chế khả năng của mọi người:
   (a) trong việc thiết lập sự tin cậy của một chữ ký điện tử theo các cách khác, với mục đích đáp ứng yêu cầu được đưa ra trong đoạn (1);
   (b) trong việc đưa ra bằng chứng về sự không tin cậy của một chữ ký điện tử.
5) Các điều khoản của mục này không áp dụng cho [...] sau đây.

Mục 7: Thoả mãn mục 6

1) *[Mọi người, cơ quan, hoặc công cộng hoặc cá nhân, được xác định trong phạm vi nước ban hành luật]* có thể quyết định những loại chữ ký điện tử nào thoả mãn các điều khoản trong mục 6.
2) Mọi quyết định được đưa ra trong đoạn (1) nên phù hợp với các chuẩn Quốc tế được công nhận.
3) Không có điều gì trong mục này ảnh hưởng đến việc sử dụng các quy tắc trong tư pháp Quốc tế.

Mục 8: Hướng dẫn người ký

1) Khi dữ liệu tạo chữ ký được sử dụng để tạo ra một chữ ký có hiệu lực pháp lý, người ký nên:

(a) Quan tâm một cách hợp lý nhằm tránh việc sử dụng trái phép dữ liệu tạo chữ ký.

(b) Không được chậm trễ, thông báo ngay cho đối tượng tin cậy vào người ký hoặc cung cấp dịch vụ hỗ trợ chữ ký điện tử khi:

(i) Người ký biết dữ liệu tạo chữ ký bị lộ; hoặc

(ii) Người ký được biết đã gây ra rủi ro đáng kể do dữ liệu tạo chữ ký bị lộ;

(c) Khi chứng chỉ được sử dụng để hỗ trợ chữ ký điện tử, người ký cần quan tâm hợp lý để đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn cần thiết do người ký đưa ra, liên quan tới chứng chỉ trong suốt thời gian tồn tại của nó, hoặc các biểu diễn nằm trong chứng chỉ.

2) Người ký cần phải chịu trách nhiệm pháp lý do không thực hiện các yêu cầu trong đoạn (1).

Mục 9: Hướng dẫn nhà cung cấp dịch vụ chứng thực

(1) Khi nhà cung cấp dịch vụ chứng thực cung cấp các dịch vụ nhằm hỗ trợ một chữ ký điện tử, muốn chữ ký này có hiệu lực hợp pháp như là một chữ ký, nhà cung cấp dịch vụ chứng thực nên:

(a) Hoạt động phù hợp với các biểu diễn về chính sách và hoạt động do chính nhà cung cấp đưa ra;

(b) Quan tâm hợp lý nhằm đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn cần thiết do nhà cung cấp đưa ra, liên quan tới chứng chỉ trong suốt thời gian tồn tại của nó, hoặc các biểu diễn nằm trong chứng chỉ.

(c) Cung cấp các phương tiện có khả năng truy nhập được, cho phép thành viên tin cậy có thể xác định từ chứng chỉ:

(i) Nhận dạng của nhà cung cấp dịch vụ chứng thực;

(ii) Người ký (được nhận dạng trong chứng chỉ) kiểm soát được dữ liệu tạo chữ ký tại thời điểm chứng chỉ được phát hành;

(iii) Dữ liệu tạo chữ ký hợp lệ tại thời điểm hoặc trước thời điểm chứng chỉ được phát hành;

(d) Cung cấp các phương tiện có khả năng truy nhập được, cho phép thành viên tin cậy xác định từ chứng chỉ, hoặc bằng cách khác:

(i) Phương pháp được sử dụng để nhận dạng người ký;

(ii) Mọi giới hạn về mục đích hoặc giá trị đối với dữ liệu tạo chữ ký hoặc chứng chỉ có thể được sử dụng;

(iii) Dữ liệu tạo chữ ký hợp lệ và không bị lộ;

(iv) Mọi giới hạn về phạm vi hoặc mức trách nhiệm pháp lý mà nhà cung cấp dịch vụ chứng thực đặt ra;

(v) Phương tiện mà người ký sử dụng để đưa ra thông báo theo đúng mục 8 (1) (b);

(vi) Dịch vụ thu hồi được đưa ra đúng lúc;

(e) Đưa ra các dịch vụ theo (d) (v), cung cấp cho người ký phương tiện thông báo theo đúng mục 8 (1) (b) và đưa ra các dịch vụ theo (d) (vi), đảm bảo tính sẵn sàng của dịch vụ thu hồi đúng lúc;

(f) Sử dụng các nguồn tài nguyên hệ thống, thủ tục và con người tin cậy khi thực hiện các dịch vụ.

(2) Nhà cung cấp dịch vụ chứng thực cần phải chịu trách nhiệm pháp lý do không thực hiện các yêu cầu trong đoạn (1).

Mục10: Sự tin cậy

Phù hợp với các mục đích của mục 9 (1) (f), khi xác định các nguồn tài nguyên hệ thống, thủ tục và con người mà nhà cung cấp dịch vụ chứng thực sử dụng có tin cậy hay không, nên quan tâm đến các yếu tố sau đây:

(a) Các nguồn tài chính và con người, bao gồm cả các tài sản;

(b) Chất lượng của các hệ thống phần mềm và phần cứng;

(c) Các thủ tục xử lý chứng chỉ và các ứng dụng dành cho chứng chỉ, duy trì các bản ghi;

(d) Tính sẵn sàng của các thông tin dành cho người ký (được nhận dạng trong chứng chỉ) và các thành viên tin cậy;

(e) Kiểm toán định kỳ hoặc mở rộng do một thực thể độc lập tiến hành;

(f) Sự công bố của một nước, thực thể được uỷ nhiệm hoặc nhà cung cấp dịch vụ chứng thực về việc tuân thủ hoặc sự tồn tại của những gì đã đề cập ở trên; hoặc

(g) Bất kỳ yếu tố liên quan khác.

Mục 11: Hướng dẫn thành viên tin cậy

Thành viên tin cậy phải gánh chịu hậu quả phân loại do không:

(a) Tiến hành các bước hợp lý để kiểm tra sự tin cậy của một chữ ký điện tử, hoặc:

(b) Khi chữ ký điện tử được hỗ trợ thông qua một chứng chỉ,

(i) Kiểm tra khoảng thời gian tồn tại hợp lệ, tình trạng treo hoặc huỷ bỏ của chứng chỉ; và

(ii) Tuân theo mọi giới hạn về chứng chỉ.

Mục 12: Công nhận chứng chỉ và chữ ký điện tử của các nước khác

1) Khi xác định một chứng chỉ hoặc một chữ ký điện tử có hiệu lực pháp lý hay không, không cần phải quan tâm tới:

(a) Vị trí địa lý - nơi chứng chỉ được phát hành; hoặc nơi chữ ký điện tử được tạo ra và sử dụng; hoặc

(b) Vị trí địa lý - nơi kinh doanh của người phát hành hoặc người ký.

2) Một chứng chỉ được phát hành bên ngoài [*Nước ban hành luật*] nên có cùng hiệu lực pháp lý như một chứng chỉ được phát hành trong [*Nước ban hành luật*] nếu nó đảm bảo mức tin cậy ngang bằng.

3) Một chữ ký điện tử được tạo ra hoặc sử dụng bên ngoài [*Nước ban hành luật*] nên có cùng hiệu lực pháp lý như một chữ ký điện tử được tạo ra và sử dụng trong [*Nước ban hành luật*] nếu nó đảm bảo mức tin cậy ngang bằng.

4) Khi xác định một chứng chỉ hoặc một chữ ký điện tử có đưa ra một mức tin cậy ngang bằng hay không, theo đoạn (2) và (3), vấn đề cần được quan tâm là các chuẩn Quốc tế được công nhận và các yếu tố liên quan khác.

5) Trong đoạn (2), (3) và (4), tuy các thành viên tự thoả thuận với nhau trong việc sử dụng một số kiểu chữ ký điện tử hoặc chứng chỉ nào đó,

thoả thuận này nên được công nhận, phù hợp với các mục đích công nhận qua biên giới, trừ khi thoả thuận này không hợp lệ hoặc không có hiệu lực đối với luật có thể áp dụng.

Phần II

HƯỚNG DẪN BAN HÀNH LUẬT MẪU VỀ CHỮ KÝ ĐIỆN TỬ CỦA UNCITRAL (2001)

Nội dung

Môc ®Ých cña H-íng dÉn

Chương I. Giới thiệu về Luật mẫu

I. MỤC ĐÍCH VÀ XUẤT XỨ CỦA LUẬT MẪU

A. Mục đích

B. Nền tảng cơ sở

C. Lịch sử

II. LUẬT MẪU LÀ CÔNG CỤ HOÀ HỢP CÁC LUẬT

III. CÁC ĐÁNH GIÁ CHUNG VỀ CHỮ KÝ ĐIỆN TỬ

A. Chức năng của các chữ ký

B. Các chữ ký số và các chữ ký điện tử khác

1. Các chữ ký điện tử dựa vào kỹ thuật hơn là mật mã khoá công khai

2. Các chữ ký số dựa vào mật mã khoá công khai

a. Các khái niệm kỹ thuật và thuật ngữ

(i) Mật mã

(ii) Các khoá công khai và khoá riêng

(iii) Hàm băm

(iv) Chữ ký số

(v) Kiểm tra chữ ký số

b. Cơ sở hạ tầng khoá công khai và nhà cung cấp dịch vụ chứng thực

(i) Cơ sở hạ tầng khoá công khai

(ii) Nhà cung cấp dịch vụ chứng thực

c. Tóm tắt quá trình xử lý chữ ký số

IV. CÁC ĐẶC ĐIỂM CHÍNH CỦA LUẬT MẪU

A. Tính pháp lý của Luật mẫu

B. Mối quan hệ với Luật mẫu về Thương mại điện tử của UNCITRAL

1. Luật mẫu trên là một văn kiện pháp lý
2. Luật mẫu trên phù hợp hoàn toàn với Luật mẫu về thương mại điện tử của UNCITRAL
3. Mối quan hệ với mục 7 Luật mẫu về thương mại điện tử của UNCITRAL

C. Các quy tắc khung được bổ sung thông qua các quy định kỹ thuật và hợp đồng

D. Làm tăng tính chắc chắn về hiệu lực pháp lý của các chữ ký điện tử

E. Các quy tắc cơ bản trong việc hướng dẫn các thành viên Tham gia

F. Khung công nghệ trung lập

G. Không phân biệt các chữ ký điện tử nước ngoài

V. SỰ TRỢ GIÚP TỪ PHÒNG THƯ KÝ CỦA UNCITRAL

A. Sự trợ giúp trong quá trình soạn thảo luật

B. Thông tin về việc làm sáng tỏ luật dựa vào Luật mẫu

Chương II. Giải thích chi tiết các mục trong Luật mẫu

Tiêu đề

Mục 1 Phạm vi ứng dụng

Mục 2 Các định nghĩa

Mục 3 Đối xử bình đẳng với các công nghệ chữ ký

Mục 4 Làm sáng tỏ

Mục 5 Thay đổi thông qua thoả thuận

Mục 6 Phù hợp với yêu cầu dành cho một chữ ký

Mục 7 Thoả mãn mục 6

Mục 8 Hướng dẫn người ký

Mục 9 Hướng dẫn nhà cung cấp dịch vụ chứng thực

Mục 10 Sự tin cậy

Mục 11 Hướng dẫn thành viên tin cậy

Mục 12 Công nhận chứng chỉ và chữ ký điện tử của nước ngoài

Mục đích của Hướng dẫn

1. Trong quá trình soạn thảo và phê chuẩn Luật mẫu về chữ ký điện tử, UNCITRAL mong muốn Luật mẫu này có thể trở thành một công cụ hiệu quả, trợ giúp các nước trong việc xây dựng luật cho riêng mình. Uỷ ban cũng nhận thấy khả năng Luật mẫu sẽ được sử dụng tại nhiều nước có sử dụng các kiểu kỹ thuật truyền thông được đưa ra trong Luật mẫu. Bản hướng dẫn đi kèm giải thích chi tiết các điều khoản có trong Luật mẫu.

2. Bản hướng dẫn này do Phòng thư ký soạn thảo theo đúng yêu cầu của UNCITRAL, được đưa ra trong phiên họp thứ 34, năm 2001.

Chương I:

GIỚI THIỆU VỀ LUẬT MẪU

I. Môc ®Ých vµ xuÊt xø cña LuËt mÉu

A. Mục đích

3. Do việc sử dụng ngày càng tăng các kỹ thuật xác thực điện tử, thay thế cho các chữ ký viết tay và các thủ tục xác thực truyền thống, nhu cầu đặt ra là cần có một khung pháp lý cụ thể nhằm giải quyết tình trạng không rõ ràng là kết quả của việc sử dụng các kỹ thuật này (chúng thường được gọi là "các chữ ký điện tử").

4. Việc xây dựng các nguyên lý cơ bản tuân theo mục 7 của Luật mẫu (được trình bày ở trên) liên quan đến việc thực thi chức năng của một chữ ký trong môi trường điện tử, Luật mẫu này được thiết kế nhằm trợ giúp cho các nước trong việc xây dựng một khung pháp lý hiện đại, hoà hợp và công bằng, nhằm giải quyết hiệu quả hơn các vấn đề về chữ ký điện tử. Luật mẫu đưa ra các chuẩn dựa vào sự tin cậy chữ ký điện tử có thể đánh giá về mặt kỹ thuật. Thêm vào đó, Luật mẫu cung cấp liên kết giữa sự tin cậy này với hiệu lực mong muốn dành cho một chữ ký điện tử xác định. Luật mẫu tạo điều kiện cho việc tìm hiểu các chữ ký điện tử và tin tưởng rằng các kỹ thuật chữ ký điện tử được tin cậy sử dụng trong các giao dịch hợp pháp. Hơn nữa, thông qua một tập các quy tắc cơ bản hướng dẫn các thành viên khác nhau trong việc sử dụng các chữ ký điện tử (ví dụ người ký, thành viên tin cậy và nhà cung cấp dịch vụ chứng thực), Luật mẫu có thể trợ giúp cho các hoạt động thương mại hoà hợp hơn.

5. Các mục tiêu của Luật mẫu (trong đó, tạo điều kiện hoặc cho phép sử dụng các chữ ký điện tử, đối xử ngang bằng với những người sử dụng tài liệu trên giấy tờ và những người sử dụng thông tin trên máy tính) là các yếu tố cần thiết, nhằm tạo điều kiện kinh tế và hiệu quả trong thương mại Quốc tế. Bằng cách kết hợp chặt chẽ các thủ tục đã được mô tả trong Luật mẫu trên (và các điều khoản trong Luật mẫu về Thương mại điện tử của UNCITRAL), cụ thể trong luật của mỗi Quốc gia liên quan tới các trường hợp - trong đó, thành viên lựa chọn sử dụng các phương tiện truyền thông điện tử, nước ban hành luật có thể tạo ra một môi trường truyền thông trung lập thích hợp. Hướng tiếp cận phương tiện truyền thông trung lập được sử dụng trong Luật mẫu về Thương mại điện tử của UNCITRAL, nhằm mục đích bao trùm lên tất cả các trường

hợp thực tế - trong đó, thông tin được tạo ra, lưu giữ hoặc truyền đi. Các từ "môi trường truyền thông trung lập" được sử dụng trong Luật mẫu về Thương mại điện tử của UNCITRAL phản ánh nguyên tắc không phân biệt thông tin được lưu giữ trên giấy tờ và thông tin được truyền đi hay lưu giữ điện tử. Luật mẫu trên cũng phản ánh nguyên tắc không phân biệt các kỹ thuật có thể được sử dụng để truyền hoặc lưu giữ thông tin điện tử.

B. Nền tảng cơ sở

6. Luật mẫu là một trong các văn kiện Quốc tế được UNCITRAL thông qua, nó tập trung chủ yếu vào sự cần thiết của thương mại điện tử; hoặc sự cần thiết của các phương tiện truyền thông hiện đại. Trong trường hợp đầu tiên, các văn kiện cụ thể hướng phục vụ cho thương mại điện tử bao gồm hướng dẫn về mặt pháp lý cho chuyển quỹ điện tử (1987), Luật mẫu về Chuyển Tín dụng Quốc tế của UNCITRAL (1992) và Luật mẫu về Thương mại điện tử của UNCITRAL (1996 và 1998). Trong trường hợp thứ hai, bao gồm tất cả các công ước Quốc tế và các văn kiện pháp lý khác được UNCITRAL thông qua từ năm 1978 liên quan tới truyền thông.

7. Trong lĩnh vực thương mại điện tử, văn kiện được biết đến nhiều nhất của UNCITRAL là "Luật mẫu về Thương mại điện tử của UNCITRAL". Nó được soạn thảo từ trước những năm 1990, xuất phát từ nhu cầu sử dụng ngày càng tăng các phương tiện truyền thông hiện đại, chẳng hạn như, sử dụng thư điện tử và trao đổi dữ liệu điện tử (EDI) khi tiến hành các giao dịch thương mại Quốc tế. Người ta cũng nhận thấy rằng, các công nghệ mới đã và đang phát triển nhanh chóng, chúng có thể phát triển xa hơn nữa, không chỉ dừng lại ở phạm vi hỗ trợ kỹ thuật, chẳng hạn như xa lộ thông tin và Internet có khả năng truy nhập rộng rãi hơn. Tuy nhiên, việc truyền các thông tin đủ hợp pháp theo dạng các thông báo (không phải trên giấy tờ) đã bị cản trở, hoặc không rõ ràng về mặt pháp lý. Với mục đích tạo điều kiện cho việc sử dụng các phương tiện truyền thông hiện đại, UNCITRAL đã soạn thảo Luật mẫu về thương mại điện tử. Mục đích của Luật mẫu này là tạo ra một môi trường pháp lý an toàn hơn, loại bỏ các rào cản cho thương mại điện tử.

8. Tại một số nước, luật hiện hành về quản lý truyền thông và lưu giữ thông tin không đầy đủ hoặc đã lỗi thời, do chúng không được dự định sử dụng cho thương mại điện tử. Trong một số trường hợp, những luật này còn lạm dụng, hoặc giới hạn sử dụng các phương tiện truyền thông hiện đại, ví dụ, bắt buộc

phải sử dụng các tài liệu "viết tay", "được ký" và "nguyên bản". Luật mẫu về Thương mại điện tử của UNCITRAL đã phê chuẩn một hướng tiếp cận có chức năng ngang bằng. "Hướng tiếp cận có chức năng ngang bằng" dựa vào việc phân tích mục đích và các chức năng trên giấy tờ truyền thống, xác định mục đích hoặc chức năng nào có thể được thực thi thông qua các kỹ thuật thương mại điện tử (xem hướng dẫn ban hành Luật mẫu về Thương mại điện tử của UNCITRAL, đoạn 15-18).

9. Tại thời điểm khi UNCITRAL soạn thảo Luật mẫu về Thương mại điện tử, một vài nước đã phê chuẩn các điều khoản xác định nhằm giải quyết một số khía cạnh nào đó của thương mại điện tử. Tuy nhiên, không có một luật nào giải quyết tất cả các vấn đề về thương mại điện tử. Điều này có thể gây ra tình trạng không rõ ràng về mặt pháp lý và tính hợp lệ của thông tin có trong các khuôn dạng khác, so với tài liệu trên giấy tờ truyền thống. Hơn nữa, các luật đầy đủ và hoàn chỉnh thực sự cần thiết cho tất cả các nước có sử dụng phổ biến EDI và thư tín điện tử; điều này cũng thực sự cần thiết cho các nước có sử dụng các kỹ thuật truyền thông như telex và telecopy. Mục 2(b) trong Luật mẫu về Thương mại điện tử của UNCITRAL định nghĩa EDI như sau "thông tin điện tử được truyền từ máy tính này sang máy tính khác và sử dụng một chuẩn được chấp nhận để hình thành cấu trúc thông tin".

10. Luật mẫu về Thương mại điện tử của UNCITRAL cũng góp phần giải quyết các khó khăn do luật của mỗi Quốc gia không đầy đủ, tạo ra các rào cản đối với thương mại Quốc tế và cản trở việc sử dụng các kỹ thuật truyền thông hiện đại. Trong phạm vi rộng giữa các nước, sự chênh lệch và thiếu rõ ràng trong luật quản lý sử dụng các kỹ thuật truyền thông này có thể hạn chế các nhà kinh doanh ra nhập thị trường Quốc tế.

11. Hơn nữa, ở phạm vi Quốc tế, Luật mẫu về Thương mại điện tử của UNCITRAL có thể hữu ích trong các trường hợp nào đó, chẳng hạn, được xem là công cụ làm sáng tỏ các công ước Quốc tế hiện hành và các văn kiện Quốc tế khác mà có thể tạo ra các rào cản về mặt pháp lý đối với việc sử dụng thương mại điện tử, ví dụ bắt buộc sử dụng các tài liệu hoặc điều khoản hợp đồng theo dạng viết tay. Với các nước tham gia văn kiện Quốc tế này, việc phê chuẩn Luật mẫu về Thương mại điện tử của UNCITRAL (được xem như là một quy tắc làm sáng tỏ) có thể khuyến khích việc sử dụng thương mại điện tử.

C. Lịch sử

12. Sau khi phê chuẩn Luật mẫu về Thương mại điện tử của UNCITRAL, tại phiên họp thứ 29 (1996), Uỷ ban quyết định đưa vấn đề chữ ký số và cơ quan chứng thực vào chương trình nghị sự của mình. Nhóm làm việc về thương mại điện tử (*Working Group on Electronic Commerce*) được yêu cầu xem xét tính khả thi của việc soạn thảo các quy tắc thống nhất về các chủ đề nêu trên, nhất trí rằng các quy tắc được soạn thảo phải giải quyết các vấn đề như cơ sở pháp lý hỗ trợ cho quá trình chứng thực, cụ thể là công nghệ chứng thực và xác thực số; khả năng áp dụng chứng thực; xác định rủi ro và trách nhiệm pháp lý của người sử dụng, nhà cung cấp và thành viên thứ 3 trong phạm vi sử dụng các kỹ thuật chứng thực; vấn đề nảy sinh khi chứng thực sử dụng cơ quan đăng ký.

13. Tại phiên họp thứ 30, Nhóm làm việc đã báo cáo với Uỷ ban về tầm quan trọng, nhu cầu và công việc cần làm để hoà hợp các luật liên quan đến lĩnh vực này. Nhóm làm việc cũng lưu ý rằng, bên cạnh chữ ký số và cơ quan chứng thực, những công việc tiếp theo trong lĩnh vực thương mại điện tử là giải quyết các vấn đề về lựa chọn mật mã khoá công khai; chức năng của thành viên thứ 3; hợp đồng điện tử (A/CN.9/437, đoạn 156-157). Uỷ ban tán thành cách giải quyết mà Nhóm làm việc đưa ra, giao nhiệm vụ cho Nhóm làm việc soạn thảo các quy tắc thống nhất về vấn đề pháp lý cho chữ ký số và cơ quan chứng thực.

14. Tuỳ thuộc vào phạm vi và dạng quy tắc thống nhất, Uỷ ban nhất trí không đưa ra quyết định nào trong giai đoạn xử lý ban đầu này. Nhóm làm việc có thể tập trung vào các vấn đề về chữ ký số, do vai trò nổi bật của mật mã khoá công khai trong hoạt động thương mại điện tử, các quy tắc thống nhất nên phù hợp với hướng tiếp cận phương tiện truyền thông trung lập được đưa ra trong Luật mẫu về Thương mại điện tử của UNCITRAL. Chính vì vậy, các quy tắc thống nhất không nên ngăn cản việc sử dụng các kỹ thuật xác thực khác. Hơn nữa, để phù hợp với mật mã khoá công khai, các quy tắc thống nhất nên dàn xếp các mức an toàn, công nhận hiệu lực pháp lý và mức trách nhiệm pháp lý tương ứng với các kiểu dịch vụ trong phạm vi chữ ký số. Với các cơ quan chứng thực, Nhóm làm việc có thể đề xuất thiết lập một tập tối thiểu các chuẩn mà cơ quan chứng thực phải đáp ứng, đặc biệt trong chứng thực chéo.

15. Nhóm làm việc bắt đầu soạn thảo các quy tắc thống nhất trong phiên họp thứ 32 của mình.

16. Trong suốt phiên họp thứ 31 và 32, Nhóm làm việc đã báo cáo với Uỷ ban những khó khăn của mình trong việc tìm hiểu các vấn đề pháp lý mới xuất phát từ việc sử dụng ngày càng tăng các chữ ký số và chữ ký điện tử khác. Nhóm làm việc cũng nhất trí rằng, có thể giải quyết các vấn đề này trong một khung pháp lý Quốc tế có thể chấp nhận được.

17. Uỷ ban xác nhận lại một lần nữa quyết định được đưa ra trong phiên họp thứ 30 về tính khả thi của việc soạn thảo các quy tắc thống nhất, đồng thời tin tưởng rằng Nhóm làm việc sẽ hoàn thành công việc tại phiên họp thứ 33. Ngoài ra, Uỷ ban ghi nhận Nhóm làm việc được công nhận là một diễn đàn Quốc tế đặc biệt quan trọng trong việc trao đổi các quan điểm về các vấn đề pháp lý trong thương mại điện tử và chuẩn bị giải pháp cho các vấn đề này.

18. Nhóm làm việc tiếp tục xem xét các quy tắc thống nhất tại phiên họp thứ 33 (1998) và 34 (1999). Báo cáo tại các phiên họp được lưu trong tài liệu A/CN.9/454 và 457.

19. Tại phiên họp thứ 32 (1999), Uỷ ban đã nghe Nhóm làm việc báo cáo về 2 phiên họp nêu trên (A/CN.9/454 và 457). Uỷ ban đánh giá cao nỗ lực của Nhóm làm việc trong việc soạn thảo các quy tắc thống nhất. Đồng thời cũng nhất trí rằng, quá trình tìm hiểu các vấn đề pháp lý liên quan tới chữ ký điện tử được tiến hành trong 2 phiên họp nêu trên. Uỷ ban cũng nhận thấy rằng, Nhóm làm việc sẽ vấp phải nhiều khó khăn để có được sự nhất trí về chính sách lập pháp mà các quy tắc thống nhất dựa vào.

20. Có quan điểm cho rằng, hướng tiếp cận mà Nhóm làm việc đang tiến hành không phản ánh đầy đủ tính mềm dẻo của việc sử dụng các chữ ký điện tử và các kỹ thuật xác thực khác trong kinh doanh. Các quy tắc thống nhất đã quan trọng hoá các kỹ thuật chữ ký số và ứng dụng có sự tham gia của thành viên thứ 3 (trong phạm vi của các chữ ký số). Do vậy, Nhóm làm việc chỉ nên tập trung vào các vấn đề pháp lý liên quan tới chứng thực chéo, hoặc dừng lại cho đến khi các hoạt động thị trường được thiết lập tốt hơn. Một quan điểm nữa cho rằng, theo các mục đích của thương mại Quốc tế, hầu hết các vấn đề pháp lý xuất phát từ việc sử dụng các chữ ký điện tử đã được giải quyết hoàn toàn trong Luật mẫu về Thương mại điện tử của UNCITRAL (xem đoạn 28 tiếp theo). Do việc sử dụng các chữ ký điện tử có thể nằm ngoài phạm vi luật thương mại, không nên để Nhóm làm việc tham gia vào bất kỳ hoạt động điều chỉnh nào như vậy.

21. Đa phần các quan điểm đều cho rằng, Nhóm làm việc nên tiếp tục nhiệm vụ của mình. Các quan điểm này giải thích rằng, do nhu cầu cần có các quy tắc thống nhất về chữ ký điện tử, tại nhiều nước, các cơ quan của chính phủ và cơ quan lập pháp mong muốn UNCITRAL đưa ra bản hướng dẫn khi họ soạn thảo luật về các vấn đề chữ ký điện tử, bao gồm thiết lập cơ sở hạ tầng khoá công khai (PKI), hoặc các dự án khác liên quan trực tiếp đến các vấn đề này (xem A/CN.9/457, đoạn 16). Nhóm làm việc quyết định tập trung vào các vấn đề PKI và thuật ngữ PKI, ảnh hưởng của các mối quan hệ giữa 3 kiểu thành viên (người ký, cơ quan chứng thực và thành viên tin cậy) ứng với một mô hình PKI có thể thực hiện được. Một trong các lợi ích chính của việc tập trung vào các vấn đề PKI là tạo điều kiện cho việc hình thành các quy tắc thống nhất, bằng cách tham chiếu vào 3 chức năng (hoặc tập đặc quyền), thường là chức năng của người phát hành khoá (hoặc thuê bao), chức năng chứng thực và chức năng tin cậy. Nói chung, 3 chức năng này phổ biến trong tất cả các mô hình PKI. Nên thực hiện 3 chức năng này, bất luận chúng do 3 thực thể riêng lẻ thực hiện; hoặc chỉ do một người đảm nhiệm (chẳng hạn, trong trường hợp nhà cung cấp dịch vụ chứng thực cũng là thành viên tin cậy). Thêm vào đó, việc tập trung vào các chức năng điển hình có trong PKI và không có trong bất kỳ mô hình xác định nào giúp cho Nhóm làm việc dễ dàng phát triển một quy tắc đầy đủ trong giai đoạn sau (xem đoạn 68 dưới đây).

22. Sau khi thảo luận, Uỷ ban xác nhận lại các quyết định về tính khả thi của việc soạn thảo các quy tắc thống nhất, đồng thời tin tưởng rằng Nhóm làm việc sẽ hoàn thành công việc tại các phiên họp sắp tới.

23. Nhóm làm việc tiếp tục công việc của mình tại các phiên họp thứ 35 (9/1999) và 36 (2/2000) dựa vào các cơ sở mà Phòng thư ký chuẩn bị (A/CN.9/WG.IV/WP.82 và 84). Tại phiên họp thứ 33 (2000) của mình, Uỷ ban đã nghe Nhóm làm việc báo cáo về 2 phiên họp nêu trên (A/CN.9/465 và 467). Tại phiên họp thứ 36 của mình, Nhóm làm việc đã thông qua mục 1, mục 3 đến mục 12 trong bản dự thảo về các quy tắc thống nhất. Công bố rằng, số vấn đề còn lại đã được làm sáng tỏ và Nhóm làm việc quyết định loại bỏ khái niệm *chữ ký điện tử nâng cao* ra khỏi các quy tắc thống nhất. Đồng thời nhấn mạnh, tuỳ thuộc vào các quyết định về mục 2 và 13 trong bản dự thảo, các điều khoản còn lại trong bản dự thảo có thể cần xem xét lại, nhằm tránh xảy ra tình trạng, trong đó chuẩn (mà các quy tắc thống nhất thiết lập) có thể áp dụng như nhau

cho các chữ ký điện tử có mức an toàn cao và các chứng chỉ giá trị thấp được sử dụng trong phạm vi truyền thông điện tử.

24. Sau khi thảo luận, Uỷ ban đánh giá cao nỗ lực của Nhóm làm việc và tiến triển của việc soạn thảo các quy tắc thống nhất. Uỷ ban mong muốn Nhóm làm việc xúc tiến nhanh hơn nữa để hoàn thành công việc này vào phiên họp thứ 37, đồng thời xem xét bản dự thảo hướng dẫn ban hành do Phòng thư ký chuẩn bị.

25. Nhóm làm việc hoàn thành việc soạn thảo các quy tắc thống nhất trong phiên họp thứ 37 của mình (9/2000). Báo cáo của phiên họp này được lưu trong tài liệu A/CN.9/483. Nhóm làm việc cũng thảo luận về bản dự thảo hướng dẫn ban hành. Phòng thư ký được yêu cầu chuẩn bị bản dự thảo hướng dẫn sửa lại, sao cho nó phản ánh được các quyết định mà Nhóm làm việc đưa ra, dựa trên các quan điểm, các đề xuất và các mối quan tâm khác nhau được đưa ra trong phiên họp này. Do thiếu thời gian, Nhóm làm việc không thể hoàn thành bản dự thảo hướng dẫn ban hành một cách kỹ lưỡng. Uỷ ban mong muốn Nhóm làm việc sẽ hoàn thành công việc này vào phiên họp thứ 38 của mình. Các quy tắc thống nhất (theo dạng dự thảo Luật mẫu về Chữ ký điện tử của UNCITRAL), cùng với bản dự thảo hướng dẫn ban hành được Uỷ ban đệ trình xem xét và thông qua vào phiên họp thứ 34 (2001).

II. LUẬT MẪU LÀ CÔNG CỤ HOÀ HỢP CÁC LUẬT

26. Cũng giống như Luật mẫu về Thương mại điện tử của UNCITRAL, Luật mẫu trên là một dạng văn bản pháp lý, được khuyến nghị đưa vào luật Quốc gia. Không giống như một công ước Quốc tế, Luật mẫu không yêu cầu nước ban hành luật thông báo cho Liên Hợp Quốc hoặc các nước khác có ban hành Luật mẫu này. Tuy nhiên, các nước nên thông báo cho Phòng thư ký của UNCITRAL khi ban hành Luật mẫu này (hoặc các Luật mẫu khác của UNCITRAL).

27. Khi đưa Luật mẫu này vào hệ thống luật của nước mình, nước này có thể sửa đổi hoặc loại bỏ một số điều khoản. Trong trường hợp là một công ước, các nước có thể thay đổi nhưng rất hạn chế (thường là "bảo lưu"), nhưng tính mềm dẻo vốn có của Luật mẫu được thể hiện trong trường hợp một nước có thể sửa đổi luật này trước khi ban hành nó như một luật Quốc gia, sao cho các sửa đổi này phù hợp với hệ thống thủ tục và toà án Quốc gia. Tuy nhiên, điều này cũng có nghĩa là, mức độ hoà hợp đạt được thông qua Luật mẫu có khả năng

thấp hơn so với một công ước. Tuy nhiên, khó khăn này có thể được cân bằng, do số nước ban hành Luật mẫu nhiều hơn số nước tán thành một công ước. Để đạt được mức độ hoà hợp và sự chắc chắn, khuyến nghị rằng, các nước nên tối giản sửa đổi khi đưa Luật mẫu này vào hệ thống luật Quốc gia. Nói chung, khi ban hành Luật mẫu trên (hoặc Luật mẫu về Thương mại điện tử của UNCITRAL), nên tán thành cao nhất đối với chúng để tạo ra luật Quốc gia trong suốt và thân thuộc với người nước ngoài khi họ sử dụng luật Quốc gia.

28. Lưu ý rằng, một số nước quan tâm đến các vấn đề pháp lý liên quan tới việc sử dụng các chữ ký điện tử và đã được giải quyết trong Luật mẫu về Thương mại điện tử của UNCITRAL, không có ý định chấp nhận thêm các quy tắc về chữ ký điện tử cho đến khi các hoạt động thị trường trong lĩnh vực mới mẻ này được thiết lập tốt hơn. Hơn nữa, các nước ban hành Luật mẫu trên (ngoài Luật mẫu về Thương mại điện tử của UNCITRAL) mong muốn có nhiều lợi ích hơn nữa. Tại những nước này, các cơ quan chính phủ và cơ quan lập pháp có nhiệm vụ soạn thảo luật liên quan tới các vấn đề về chữ ký điện tử (bao gồm thiết lập cơ sở hạ tầng khoá công khai), các điều khoản trong Luật mẫu cung cấp hướng dẫn cho các cơ quan này khi soạn thảo văn kiện Quốc tế liên quan tới các vấn đề về PKI và thuật ngữ PKI. Với tất cả các nước, Luật mẫu trên cung cấp một tập các quy tắc cơ bản, có thể áp dụng chúng bên ngoài mô hình PKI, khi chúng chịu ảnh hưởng của hai chức năng có trong mọi chữ ký điện tử (nghĩa là, tạo và tin cậy một chữ ký điện tử) và chức năng thứ 3 có trong các kiểu chữ ký điện tử xác định nào đó (nghĩa là, chứng nhận một chữ ký điện tử). Nên thực hiện 3 chức năng, bất luận chúng do 3 (hoặc nhiều hơn) thực thể đảm nhận (nghĩa là, các khía cạnh khác nhau trong chức năng chứng thực được chia xẻ cho nhiều thực thể); hoặc hai trong số các chức năng này do một người đảm nhận (chẳng hạn, trong trường hợp nhà cung cấp dịch vụ chứng thực cũng là thành viên tin cậy). Do vậy, Luật mẫu cung cấp nền móng chung cho các hệ thống PKI (tin cậy các cơ quan chứng thực độc lập) và các hệ thống chữ ký điện tử (không có thành viên thứ 3 độc lập khi xử lý chữ ký điện tử). Trong mọi trường hợp, Luật mẫu trên cung cấp thêm sự chắc chắn về hiệu lực pháp lý của các chữ ký điện tử, không hạn chế các tiêu chuẩn mềm dẻo có trong mục 7 của Luật mẫu về Thương mại điện tử của UNCITRAL (xem đoạn 67 và 70 đến 75 dưới đây).

III. c¸c ®¸nh gi¸ chung vÒ ch÷ ký ®iÖn tö

29. Mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL dựa vào việc công nhận các chức năng của một chữ ký trên giấy tờ. Trong quá trình soạn thảo Luật mẫu về thương mại điện tử, Nhóm làm việc đã thảo luận chức năng truyền thống của chữ ký viết tay như nhận dạng một người; liên kết người này với nội dung của một tài liệu. Ngoài ra, chữ ký có thể có nhiều chức năng, tuỳ thuộc vào tính chất của tài liệu được ký. Mối quan hệ giữa Luật mẫu trên với mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL được thảo luận trong các đoạn 65, 67 và 70 đến 75 trong bản hướng dẫn này.

30. Trong môi trường điện tử, không thể phân biệt được thông báo gốc và bản sao của nó, không có chữ ký viết tay và trên giấy. Sự giả mạo là điều dễ nhận thấy, việc ngăn chặn và sửa đổi thông tin mà không bị phát hiện là điều không khó. Mục đích của các kỹ thuật hiện có trên thị trường, hoặc đang được phát triển là làm cho các chức năng của chữ ký viết tay có hiệu lực trong môi trường điện tử. Các kỹ thuật này được gọi chung là "các chữ ký điện tử ".

B. Các chữ ký số và các chữ ký điện tử khác

31. Trong quá trình thảo luận về sự mong muốn và tính khả thi của việc soạn thảo Luật mẫu trên; đồng thời, trong quá trình định nghĩa phạm vi của các quy tắc thống nhất, UNCITRAL đã xem xét các kỹ thuật chữ ký điện tử hiện có, hoặc đang trong giai đoạn phát triển. Mục đích chung của các kỹ thuật này là đảm bảo chức năng ngang bằng với (1) các chữ ký viết tay và (2) các kiểu cơ chế xác thực được sử dụng trên giấy (ví dụ, tem hoặc dấu). Chúng có thể thực hiện thêm các chức năng trong thương mại điện tử.

32. Như đã được trình bày ở trên (xem các đoạn 21 và 28), rất nhiều nước mong muốn UNCITRAL hướng dẫn cho các cơ quan chính phủ và cơ quan lập pháp, khi họ soạn thảo luật liên quan đến các vấn đề về chữ ký điện tử - trong đó có thiết lập cơ sở hạ tầng khoá công khai (PKI), hoặc các dự án khác cho các vấn đề liên quan (xem A/CN.9/457, đoạn 16). Quyết định của UNCITRAL tập trung vào các vấn đề về PKI và thuật ngữ PKI, cần lưu ý rằng, ảnh hưởng của mối quan hệ giữa 3 kiểu thành viên (người ký, nhà cung cấp dịch vụ chứng thực và thành viên tin cậy) ứng với một kiểu mô hình PKI có thể thực hiện được, nhưng các mô hình khác cũng được sử dụng phổ biến trên thị trường. Một trong các lợi ích chính của việc tập trung vào các vấn đề của PKI là tạo điều kiện cho việc xây dựng Luật mẫu, dựa vào 3 chức năng (hoặc tập đặc quyền), thường là chức năng ký, chức năng chứng nhận và chức năng tin cậy.

Hai trong số các chức năng này (tạo và tin cậy một chữ ký điện tử) phổ biến trong mọi mô hình PKI. Chức năng thứ 3 (chứng nhận một chữ ký điện tử) có trong nhiều mô hình PKI. 3 chức năng này nên được gắn kết với nhau, bất kể chúng được 3 (hoặc nhiều hơn) thực thể đảm nhận (ví dụ, các mảng khác nhau trong chức năng chứng thực được chia xẻ cho nhiều thực thể); hoặc hai trong số các chức năng này do một người đảm nhận (ví dụ, nhà cung cấp dịch vụ chứng thực cũng là thành viên tin cậy). Việc tập trung vào các chức năng có trong một PKI và không có trong bất kỳ mô hình xác định nào cũng có thể phát triển một quy tắc đầy đủ, nhằm mở rộng các chức năng tương tự có trong công nghệ chữ ký điện tử phi PKI.

1. Các chữ ký điện tử dựa vào kỹ thuật hơn là mật mã khoá công khai

33. Bên cạnh "các chữ ký số" dựa vào mật mã khoá công khai, còn có nhiều thiết bị khác dựa vào các kỹ thuật chữ ký điện tử hiện đang được sử dụng, hoặc dự kiến sử dụng trong tương lai, với dự định đáp ứng một hoặc nhiều chức năng nêu trên của chữ ký viết tay. Ví dụ, các kỹ thuật dựa vào xác thực thông qua một thiết bị sinh trắc học với các chữ ký viết tay. Trong thiết bị này, người ký sử dụng một bút đặc biệt, ký lên màn hình máy tính hoặc bảng số. Sau đó, chữ ký viết tay được máy tính phân tích và lưu giữ như một tập các giá trị số, có thể gắn nó vào một thông báo; hoặc được thành viên tin cậy sử dụng cho các mục đích xác thực. Giả định rằng, trong hệ thống xác thực này, các mẫu chữ ký viết tay đã được phân tích và lưu giữ từ trước trong thiết bị sinh trắc học. Các kỹ thuật khác như sử dụng số hiệu nhận dạng cá nhân (PIN), các mẫu chữ ký viết tay được số hoá và các phương pháp khác, chẳng hạn nhấn vào một "Ok-box".

34. UNCITRAL dự kiến phát triển một luật thống nhất, nhằm tạo điều kiện cho việc sử dụng các chữ ký số và các loại chữ ký điện tử khác. Vì ý định này, UNCITRAL đã cố gắng giải quyết các vấn đề về luật liên quan đến chữ ký điện tử ở một mức trung gian (giữa mức tổng quát trong Luật mẫu về Thương mại điện tử của UNCITRAL và mức yêu cầu xác định dành cho một kỹ thuật ký cho trước). Không nên cho rằng, Luật mẫu trên không khuyến khích sử dụng các phương pháp chữ ký điện tử khác, cho dù chúng hiện đang tồn tại hoặc dự kiến thực hiện trong tương lai.

2. Các chữ ký số dựa vào mật mã khoá công khai

35. Do việc sử dụng các kỹ thuật ký số ngày càng tăng tại một số nước, giới thiệu sau đây mang tính hỗ trợ cho việc sử dụng này.

(a) Các khái niệm kỹ thuật và thuật ngữ

(i) Mật mã

36. Các chữ ký số được tạo ra và kiểm tra bằng mật mã, đúng hơn là, áp dụng toán học để chuyển đổi các thông báo ban đầu sang dạng vô nghĩa và ngược lại, chuyển đổi chúng về dạng ban đầu. Các chữ ký số sử dụng "mật mã khoá công khai", nó thường sử dụng các thuật toán để tạo ra hai "khoá" khác nhau nhưng có liên quan về mặt toán học (có nghĩa là, sinh ra các số lớn bằng cách sử dụng nhiều công thức toán học cho các số nguyên tố). Một khoá được sử dụng để tạo ra chữ ký số hoặc chuyển đổi thông báo sang dạng vô nghĩa, khoá còn lại được sử dụng để kiểm tra chữ ký số hoặc chuyển đổi thông báo ở dạng vô nghĩa thành thông báo gốc ban đầu. Thiết bị máy tính và phần mềm sử dụng những khoá này thường được gọi là các "hệ mật", hoặc cụ thể hơn là các "hệ mật phi đối xứng" và chúng sử dụng các thuật toán không đối xứng.

37. Việc sử dụng mật mã là một trong các đặc điểm chính của chữ ký số, trong thực tế, chữ ký số được sử dụng để xác thực thông báo. Mã hoá là một phương pháp được sử dụng để bảo đảm bí mật cho các cuộc truyền thông, do vậy chỉ có người tạo thông báo và người nhận đích thực mới có thể đọc được thông báo. Tại một số nước, việc sử dụng mật mã cho các mục đích bảo mật do luật pháp quy định vì nó liên quan đến phòng thủ Quốc gia. Tuy nhiên, việc sử dụng mật mã để xác thực (bằng cách tạo ra một chữ ký số) không nhất thiết phải bao hàm việc sử dụng mật mã để bảo mật thông tin trong quá trình truyền thông, chỉ cần gắn chữ ký số được mã hoá vào một thông báo không được mã hoá.

(ii) Các khoá riêng và khoá công khai

38. Khoá được sử dụng để tạo ra các chữ ký số được gọi "khoá riêng", chỉ người ký được phép sử dụng khoá này để tạo ra chữ ký số, "khoá công khai" được biết rộng rãi hơn và thành viên tin cậy sử dụng khoá này để kiểm tra chữ ký số. Người sử dụng cần phải giữ bí mật khoá riêng. Lưu ý rằng, người sử dụng không nhất thiết phải biết khoá riêng, khoá này thường được lưu giữ trong một thẻ thông minh, có thể truy nhập vào nó thông qua số hiệu nhận dạng cá nhân (PIN), hoặc thiết bị nhận dạng sinh trắc học. Nếu nhiều người muốn kiểm tra chữ ký số của người ký, thì khoá công khai phải có hiệu lực,

hoặc phân phối cho tất cả những người này, chẳng hạn bằng cách công bố trong một kho lưu giữ trực tuyến, hoặc một dạng thư mục công khai nào đó, sao cho việc truy nhập vào chúng là hoàn toàn dễ dàng. Các khoá trong cặp khoá có liên quan toán học với nhau, nếu một hệ mật phi đối xứng được tạo ra và thiết lập an toàn, khó có thể biết được khoá riêng từ khoá công khai. Hầu hết các thuật toán dành cho mã hoá sử dụng khoá công khai và khoá riêng đều dựa vào một đặc tính rất quan trọng của các số nguyên tố lớn, đó là một khi nhân chúng với nhau để tạo ra một số mới, chúng ta không thể hoặc mất rất nhiều thời gian để có thể xác định được số nào trong hai số nguyên tố là số mới và là số lớn hơn. Chính vì vậy, mặc dù nhiều người biết khoá công khai nhưng không thể làm giả chữ ký số vì họ không thể khôi phục được khoá riêng cùng cặp, họ chỉ có thể kiểm tra chữ ký số.

39. Tuy nhiên, khái niệm mật mã khoá công khai không nhất thiết phải bao hàm việc sử dụng các thuật toán dựa vào các số nguyên tố được nêu ở trên. Có thể sử dụng hoặc phát triển các phương pháp toán học khác, chẳng hạn các hệ mật dựa vào đường cong ellip, chúng có thể đảm bảo một mức an toàn cao thông qua việc sử dụng các khoá có độ dài giảm đáng kể.

(iii) Hàm băm

40. Ngoài việc sinh ra các cặp khoá, quá trình tạo và kiểm tra chữ ký số cần sử dụng hàm băm. Hàm băm dựa vào một thuật toán, với đầu vào là một thông báo, thông báo ở đầu ra của thuật toán có dạng nén, thường được gọi là "tóm lược thông báo" hoặc "dấu vân tay của thông báo". Độ dài chuẩn của "kết quả băm" thường nhỏ hơn độ dài của thông báo. Khi sử dụng cùng một hàm băm, kết quả băm sẽ khác nhau nếu thông báo ban đầu có bất kỳ thay đổi nào. Trong trường hợp hàm băm được giữ bí mật, nó còn được gọi là "hàm băm một chiều", như vậy trong trường hợp này không thể khôi phục lại được thông báo ban đầu từ kết quả băm. Vì vậy, các hàm băm cho phép phần mềm (tạo các chữ ký số) tính toán trên một khối dữ liệu nhỏ hơn và có thể đoán được, trong khi vẫn đảm bảo sự tương quan với nội dung của thông báo gốc, vì vậy có thể đảm bảo rằng không có sửa đổi nào xảy ra đối với thông báo từ khi nó được ký số.

(iv) Chữ ký số

41. Để ký một tài liệu hoặc một mục thông tin nào đó, trước tiên người ký phân định chính xác những gì cần được ký. Sau đó, hàm băm trong phần mềm

của người ký tính toán một kết quả băm duy nhất đối với thông tin được ký. Tiếp theo, phần mềm của người ký "chuyển đổi" kết quả băm thành chữ ký, bằng cách sử dụng khoá riêng của người ký. Do vậy, chữ ký số được tạo ra là duy nhất đối với thông tin được ký và khoá riêng được sử dụng để tạo ra chữ ký số này.

42. Thông thường, chữ ký số được gắn kèm với một thông báo, được lưu giữ hoặc truyền đi cùng với thông báo. Tuy nhiên, nó cũng có thể được lưu giữ hoặc truyền đi như một dữ liệu riêng lẻ một khi nó duy trì mối liên kết với thông báo tương ứng.

(v) Kiểm tra chữ ký số

43. Kiểm tra chữ ký số là quá trình xem xét chữ ký số với thông báo gốc và một khoá công khai cho trước, bằng cách này có thể xác định: chữ ký số có được tạo ra từ thông báo gốc và khoá riêng tương ứng với khoá công khai này hay không. Việc kiểm tra được bắt đầu bằng cách tính toán một kết quả băm mới cho thông báo nhận được, sử dụng cùng một hàm băm như đã được sử dụng trong quá trình tạo chữ ký. Sau đó, sử dụng khoá công khai và kết quả băm mới để kiểm tra xem chữ ký số có được tạo ra từ khoá riêng tương ứng hay không, so sánh kết quả băm mới được tạo ra và kết quả băm gốc (được trích ra từ chữ ký số) xem chúng có trùng khớp hay không.

44. Phần mềm kiểm tra sẽ xác nhận chữ ký số "đã được kiểm tra" nếu: (1) khoá riêng của người ký được sử dụng để ký thông báo, trong trường hợp chỉ có thể kiểm tra chữ ký số bằng cách sử dụng khoá công khai tương ứng với khoá riêng của người ký; và (2) thông báo không bị sửa đổi, trong trường hợp kết quả băm do người kiểm tra tính toán đồng nhất với kết quả băm được trích ra từ chữ ký số trong quá trình kiểm tra.

(b) Cơ sở hạ tầng khoá công khai và nhà cung cấp dịch vụ chứng thực

45. Để kiểm tra một chữ ký số, người kiểm tra phải có khoá công khai của người ký và đảm bảo rằng nó tương ứng với khoá riêng của người ký. Tuy nhiên, một cặp khoá (khoá công khai và khoá riêng) không có mối liên kết bên trong với bất kỳ người nào; đơn giản, nó chỉ là một cặp số. Cần bổ xung thêm một cơ chế để tạo ra liên kết tin cậy giữa một người hoặc thực thể cụ thể với một cặp khoá. Nếu mật mã khoá công khai được sử dụng cho các mục đích dự định, nó cần sinh ra các khoá có hiệu lực với nhiều người, cho dù người ký không biết những người này, hoặc không có mối quan hệ tin cậy nào giữa các

thành viên. Vì mục đích này, các thành viên tham gia phải tin cậy các khoá công khai và khoá riêng được phát hành.

46. Mức tin cậy có thể tồn tại giữa các thành viên (tin tưởng lẫn nhau), họ giao dịch với nhau trong một khoảng thời gian, truyền thông qua các hệ thống khép kín, tiến hành các hoạt động trong một nhóm khép kín, hoặc cho phép quản lý các giao dịch thông qua hợp đồng, ví dụ, một thoả thuận với đối tác kinh doanh. Trong một phiên giao dịch chỉ có hai thành viên, mỗi thành viên có thể gửi (bằng cách sử dụng một kênh tương đối an toàn, chẳng hạn người đưa thư hoặc máy điện thoại) khoá công khai của mình cho thành viên còn lại. Tuy nhiên, mức độ an toàn này sẽ không đảm bảo nếu các thành viên hiếm khi giao dịch với nhau, truyền thông qua các hệ thống mở (ví dụ, Web trên Internet), không phải là một nhóm khép kín, hoặc không có các thoả thuận với đối tác kinh doanh hoặc luật quản lý khác.

47. Ngoài ra, do mật mã khoá công khai là một công nghệ toán học cao, người sử dụng phải tin cậy vào các kỹ năng, kiến thức và sự chuẩn bị an toàn của các thành viên phát hành các khoá công khai và khoá riêng.

48. Người ký tương lai sẽ đưa ra một công bố, thông báo rằng các chữ ký được kiểm tra bằng cách sử dụng khoá công khai của người ký nên được coi là chữ ký của người ký. Nước ban hành luật sẽ quản lý khuôn dạng và hiệu lực pháp lý của công bố này. Ví dụ, có thể thiết lập hiệu lực của các chữ ký điện tử bằng cách công bố công khai trong một thông cáo chính thức, hoặc trong một tài liệu được các cơ quan công cộng chứng nhận là "đích thực". Tuy nhiên, có thể xảy ra trường hợp, một số thành viên khác không muốn (miễn cưỡng) chấp nhận công bố này. Một thành viên tin cậy vào một công bố không được ủng hộ trong một hệ thống mở, có thể gặp rủi ro lớn do ngẫu nhiên tin cậy một đối tượng mạo danh, hoặc chối bỏ một chữ ký số.

49. Giải pháp để giải quyết các vấn đề trên là sử dụng một hoặc nhiều thành viên thứ 3 để chứng nhận mối liên kết người ký (được nhận dạng) hoặc tên của người ký với một khoá công khai cụ thể. Thành viên thứ 3 này được gọi là "cơ quan chứng thực" hoặc "nhà cung cấp dịch vụ chứng thực" trong hầu hết các chuẩn kỹ thuật và các hướng dẫn (Luật mẫu này sử dụng thuật ngữ "nhà cung cấp dịch vụ chứng thực"). Tại một số nước, các cơ quan chứng thực này được tổ chức theo hệ thống phân cấp và gọi chung là cơ sở hạ tầng khoá công khai

(PKI). Ngoài ra, còn có các giải pháp khác, ví dụ sử dụng các chứng chỉ do các thành viên tin cậy phát hành.

(i) Cơ sở hạ tầng khoá công khai

50. Việc thiết lập cơ sở hạ tầng khoá công khai (PKI) là một cách để đảm bảo rằng: (1) Khoá công khai của người sử dụng không bị làm giả và thực tế nó cùng cặp với khoá riêng của người sử dụng này; (2) Các kỹ thuật mật mã được sử dụng thích hợp. Để đảm bảo điều này, PKI có thể đưa ra một số dịch vụ như sau:(1) Quản lý các khoá được sử dụng cho các chữ ký số; (2) Chứng thực rằng khoá công khai cùng cặp với khoá riêng; (3) Cung cấp khoá cho người sử dụng cuối; (4) Công bố một thư mục an toàn có chứa thông tin về các khoá công khai hoặc chứng chỉ; (5) Quản lý các thẻ bài cá nhân (ví dụ, thẻ thông minh) được sử dụng để nhận dạng người sử dụng thông qua thông tin nhận dạng cá nhân duy nhất; hoặc có thể sinh ra hoặc lưu giữ khoá riêng của một cá nhân; (6) Kiểm tra nhận dạng của người sử dụng cuối và cung cấp các dịch vụ cho họ; (7) Cung cấp các dịch vụ gán nhãn thời gian; (8) Quản lý các khoá mã hoá.

51. Một PKI thường dựa vào các mức phân cấp khác nhau. Ví dụ, các mô hình được xem xét tại một số nước khi thiết lập các PKI bao gồm các mức sau: (1) Một "cơ quan gốc" duy nhất, cơ quan này có thể chứng thực công nghệ và các hoạt động của tất cả các thành viên được phép phát hành các cặp khoá mã hoặc các chứng chỉ, có thể đăng ký các cơ quan chứng thực cấp dưới; (2) Các cơ quan chứng thực là cấp dưới của cơ quan gốc có thể chứng thực khoá công khai (tương ứng với khoá riêng) của người sử dụng; (3) Các cơ quan đăng ký địa phương là cấp dưới của các cơ quan chứng thực. Các cơ quan này có nhiệm vụ nhận yêu cầu về các cặp khoá mã hoặc các chứng chỉ từ phía người sử dụng, yêu cầu bằng chứng nhận dạng của người sử dụng và kiểm tra các nhận dạng đó. Tại một số nước, công chứng viên có thể hỗ trợ hoặc hoạt động như các cơ quan đăng ký địa phương.

52. Các vấn đề của PKI thường liên quan đến hoà hợp Quốc tế. Việc tổ chức một PKI có thể vấp phải nhiều vấn đề như công nghệ, chính sách chung. Những vấn đề này có thể được giải quyết tốt hơn tại mỗi nước riêng lẻ tại thời điểm này. Do vậy, các quyết định do mỗi nước đưa ra khi thiết lập một PKI thường là nên hay không nên quy định: (1) dạng và số mức cơ quan có trong một PKI; (2) chỉ có các cơ quan chứng thực trong PKI được phép phát hành

các cặp khoá hay người sử dụng tự phát hành các cặp khoá; (3) việc chứng nhận "tính hợp lệ" của các cặp khoá do các cơ quan chứng thực là thực thể công cộng hay tư nhân tiến hành; (4) việc một thực thể hoạt động như là một nhà cung cấp dịch vụ chứng thực có cần được nhà nước cấp phép hay sử dụng các phương pháp khác để kiểm soát chất lượng của các cơ quan chứng thực nếu họ được phép hoạt động với quyền hạn xác định; (5) có nên mở rộng việc sử dụng mật mã cho các mục đích bảo mật; và (6) các cơ quan của chính phủ có quyền được biết các thông tin bí mật (đã được mã hoá) thông qua cơ chế "uỷ nhiệm khoá" hoặc bằng cách khác hay không. Luật mẫu này không giải quyết tất cả các vấn đề này.

(ii) Nhà cung cấp dịch vụ chứng thực

53. Để liên kết một cặp khoá với một người ký tương lai (thuê bao), nhà cung cấp dịch vụ chứng thực (hoặc cơ quan chứng thực) phát hành một chứng chỉ, một bản ghi điện tử có chứa khoá công khai cùng với tên của thuê bao (hay chủ thể của chứng chỉ) và có thể xác nhận rằng thuê bao được nhận dạng trong chứng chỉ nắm giữ khoá riêng cùng cặp. Khi "người nhận" muốn kiểm tra chữ ký số của thuê bao (được nhận dạng trong chứng chỉ do cơ quan chứng thực, hoặc nhà cung cấp dịch vụ chứng thực phát hành) trên một thông báo nào đó, có thể sử dụng khoá công khai có trong chứng chỉ để kiểm tra chữ ký số đó. Nếu việc kiểm tra thành công, có thể đảm bảo rằng chữ ký số này là của thuê bao và thông báo không bị sửa đổi sau khi ký.

54. Để đảm bảo tính đích thực cả về nội dung và nguồn gốc của chứng chỉ, nhà cung cấp dịch vụ chứng thực tiến hành ký số lên chứng chỉ. Chữ ký số của nhà cung cấp dịch vụ chứng thực được kiểm tra bằng cách sử dụng khoá công khai của nhà cung cấp dịch vụ chứng thực này nhưng lại được nhà cung cấp dịch vụ chứng thực khác chứng thực, thông qua việc phát hành các chứng chỉ, cứ như vậy, lần lượt kiểm tra cho đến khi chữ ký số được tin cậy hoàn toàn. Tuỳ theo luật của mỗi nước, hiệu lực của các chữ ký này có thể được công bố thông qua một thông cáo chính thức (xem A/CN.9/484, đoạn 41).

55. Một chữ ký số tương ứng với một thông báo. Chữ ký này có thể do thuê bao tạo ra nhằm xác thực một thông báo, hoặc do nhà cung cấp dịch vụ chứng thực tạo ra nhằm xác thực chứng chỉ của họ, nói chung trong trường hợp nào cũng cần gán nhãn thời gian để chỉ ra thời điểm ký, đây cũng là một điều kiện để kiểm tra một chữ ký số.

56. Để thuận tiện cho việc kiểm tra, chứng chỉ có thể được công bố tại một kho lưu giữ, hoặc phương tiện khác. Thông thường, kho lưu giữ là một cơ sở dữ liệu trực tuyến có chứa thông tin liên quan đến chứng chỉ hoặc các thông tin khác, người sử dụng có thể tìm kiếm và sử dụng trong quá trình kiểm tra chữ ký số.

57. Một khi chứng chỉ được phát hành, vẫn có thể xảy ra một số trường hợp chứng chỉ không đáng tin cậy, chẳng hạn như thuê bao gửi cho nhà cung cấp dịch vụ chứng thực nhận dạng sai của mình, hoặc khoá riêng bị lộ, nhà cung cấp dịch vụ chứng thực (theo yêu cầu của thuê bao, hoặc thậm chí không cần sự đồng ý của thuê bao, tuỳ thuộc vào từng hoàn cảnh cụ thể) có thể treo (ngừng hoạt động tạm thời) hoặc huỷ bỏ (chấm dứt hoạt động) đối với chứng chỉ. Ngay sau khi treo hoặc huỷ bỏ một chứng chỉ, nhà cung cấp dịch vụ chứng thực nên công bố công khai tình trạng này.

58. CA có thể do một cơ quan của chính phủ, hoặc nhà cung cấp dịch vụ tư nhân điều hành. Tại một số nước, chỉ có các thực thể của chính phủ mới có quyền hoạt động như là các cơ quan chứng thực. Tại một số nước khác, các nhà cung cấp dịch vụ chứng thực tư nhân được tự do cạnh tranh các dịch vụ chứng thực. Bất luận các cơ quan chứng thực có được điều hành bởi các thực thể công cộng hay các nhà cung cấp dịch vụ chứng thực tư nhân hay không, bất luận các cơ quan chứng thực có cần một giấy phép để hoạt động hay không, nói chung nên có nhiều hơn một nhà cung cấp dịch vụ chứng thực hoạt động trong PKI. Vậy mối quan hệ giữa các CA sẽ ra sao? Các CA trong một PKI có thể được thiết lập theo cấu trúc phân cấp - trong đó, một số CA chỉ chứng thực các CA cung cấp các dịch vụ trực tiếp cho người sử dụng. Theo cấu trúc này, tồn tại các CA là cấp dưới của các CA khác. Trong một số các cấu trúc khác, tất cả các CA có thể hoạt động trên cơ sở quan hệ ngang bằng. Trong một PKI lớn, tồn tại cả CA cấp dưới và cấp trên. Trong một PKI Quốc tế, có thể phát sinh một số vấn đề liên quan tới việc công nhận các chứng chỉ do các CA phát hành tại các Quốc gia khác nhau. Việc công nhận các chứng chỉ của các CA của các nước khác thường được thực hiện thông qua một giải pháp, giải pháp này được gọi là "chứng thực chéo". Trong trường hợp này, cần phải có các CA ngang bằng nhau (hoặc các CA sẽ phải gánh chịu các rủi ro nào đó liên quan tới các chứng chỉ do các CA khác phát hành) công nhận các

dịch vụ do các CA khác cung cấp, vì vậy người sử dụng của các CA khác nhau có thể truyền thông với nhau khi tin cậy các chứng chỉ.

59. Các vấn đề về pháp lý có thể nảy sinh khi tiến hành chứng thực chéo hoặc tạo ra chuỗi các chứng chỉ với nhiều chính sách an toàn. Chẳng hạn, xác định xem ai là người quản lý kém gây ra mất mát và người sử dụng tin cậy vào các biểu diễn nào. Lưu ý, một số nước quy định rằng, người sử dụng nên biết các mức và chính sách an toàn, các cơ quan chứng thực phải chịu trách nhiệm pháp lý trước mọi sơ xuất của mình.

60. Phận sự của nhà cung cấp dịch vụ chứng thực hoặc cơ quan gốc là đảm bảo các yêu cầu chính sách của mình được đáp ứng trên cơ sở phát triển. Việc lựa chọn các CA có thể dựa vào một số yếu tố, chẳng hạn kích thước khoá, nhận dạng của người sử dụng. Sự tin cậy vào nhà cung cấp dịch vụ chứng thực phụ thuộc vào việc thực thi các chuẩn phát hành chứng chỉ, việc đánh giá dữ liệu nhận được từ người sử dụng (người yêu cầu chứng chỉ), trách nhiệm pháp lý của nhà cung cấp dịch vụ chứng thực khi tuân theo chính sách và các yêu cầu an toàn của cơ quan gốc, hoặc nhà cung cấp dịch vụ chứng thực cấp trên. Một nghĩa vụ không kém phần quan trọng của nhà cung cấp dịch vụ chứng thực là hoạt động sao cho phù hợp với các biểu diễn mà họ đưa ra có liên quan đến các chính sách và các hoạt động của họ.

61. Trong quá trình soạn thảo Luật mẫu, các yếu tố sau đây cũng được quan tâm khi tin cậy nhà cung cấp dịch vụ chứng thực: (1) tính độc lập; (2) nguồn tài chính và khả năng tài chính trong việc gánh vác các rủi ro gây mất mát; (3) sự hiểu biết về công nghệ khoá công khai và các thủ tục an toàn; (4) tồn tại lâu năm; (5) phê chuẩn phần mềm và phần cứng; (6) duy trì một vết kiểm toán và việc kiểm toán do một thực thể độc lập tiến hành; (7) lên kế hoạch ứng biến; (8) quản lý và chọn lựa nhân viên; (9) bảo vệ khoá riêng của mình; (11) tiến hành các bước chuẩn bị khi ngừng hoạt động - trong đó, bao gồm cả việc thông báo cho người sử dụng; (12) các biểu diễn; (13) giới hạn trách nhiệm pháp lý; (14) các đảm bảo; (15) chứng thực chéo giữa các CA; (16) các thủ tục huỷ bỏ (trong trường hợp các khoá bị lộ hoặc mất).

(c) Tóm tắt quá trình xử lý chữ ký số

62. Thông thường, quá trình tạo và kiểm tra chữ ký số bao gồm các bước sau đây:

(1) Người ký tạo ra hoặc được cung cấp một cặp khoá;

(2) Người ký chuẩn bị thông báo (ví dụ, theo dạng của một thông báo thư điện tử);

(3) Người ký chuẩn bị một "tóm lược thông báo", bằng cách sử dụng một thuật toán băm bí mật. Quá trình tạo chữ ký số sử dụng một kết quả băm có nguồn gốc và duy nhất đối với cả thông báo được ký và khoá riêng cho trước.

(4) Người ký mã hoá tóm lược thông báo với khoá riêng. Chữ ký số chính là tóm lược thông báo được mã hoá.

(5) Thông thường, người ký gắn chữ ký số vào thông báo.

(6) Người ký gửi chữ ký số và thông báo (đã được mã hoá hoặc không) cho thành viên tin cậy.

(7) Thành viên tin cậy sử dụng khoá công khai của người ký để kiểm tra chữ ký số của người ký. Việc kiểm tra có sử dụng khoá công khai của người ký đảm bảo rằng thông báo có nguồn gốc từ người ký.

(8) Thành viên tin cậy cũng tạo ra một "tóm lược thông báo" từ thông báo nhận được, bằng cách sử dụng cùng một thuật toán băm bí mật.

(9) Thành viên tin cậy có được tóm lược thông báo nguyên thuỷ, bằng cách giải mã chữ ký số nhận được với khoá công khai của người ký. Sau đó, so sánh hai tóm lược thông báo với nhau, nếu chúng trùng khớp thì thành viên tin cậy có thể xác định được rằng thông báo không bị sửa đổi sau khi nó được ký. Chỉ cần một bít trong thông báo gửi đến bị sửa đổi cũng làm cho hai tóm lược thông báo khác nhau.

(10) Khi sử dụng chứng thực, thành viên tin cậy có được chứng chỉ từ nhà cung cấp dịch vụ chứng thực (thông qua người ký hoặc cách khác). Nó xác nhận chữ ký số trên thông báo của người ký (xem A/CN.9.484, đoạn 44). Chứng chỉ có chứa khoá công khai và tên của người ký (và có thể có nhiều thông tin khác), chứng chỉ này được nhà cung cấp dịch vụ chứng thực ký số.

IV. CÁC ĐẶC ĐIỂM CHÍNH CỦA LUẬT MẪU

A. Tính pháp lý của Luật mẫu

63. Luật mẫu trên được chuẩn bị với giả định rằng nó xuất phát trực tiếp từ mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL, nên coi nó là một cách để cung cấp thông tin chi tiết, hay cung cấp khái niệm "phương pháp tin cậy được sử dụng để nhận dạng" một người và "để chỉ ra sự phê chuẩn của một người" đối với thông tin có trong một thông báo dữ liệu (xem A/CN.9/WG.IV/WP.71, đoạn 49).

64. Câu hỏi được đặt ra là dạng văn kiện và mối quan hệ của dạng văn kiện này với nội dung được đưa ra như thế nào. Các hướng tiếp cận khác nhau đã được đề xuất, dạng văn kiện có thể bao gồm các quy tắc hợp đồng, các điều khoản pháp lý, hoặc các hướng dẫn dành cho nước ban hành luật chữ ký điện tử. Nhất trí rằng, văn bản nên được soạn thảo như là một tập các quy tắc pháp lý, cùng với các chú thích, không chỉ đơn thuần là các hướng dẫn (xem A/CN.9/437, đoạn 27; A/CN.9/446, đoạn 25; và A/CN.9/457, các đoạn 51 và 72). Văn bản được phê chuẩn cuối cùng là Luật mẫu (A/CN.9/483, các đoạn 137-138).

B. Mối quan hệ với Luật mẫu về Thương mại điện tử của UNCITRAL

1. Luật mẫu trên là một văn kiện pháp lý

65. Các điều khoản trong Luật mẫu trên có thể kết hợp với phiên bản mở rộng của Luật mẫu về Thương mại điện tử của UNCITRAL. Với quan điểm rõ ràng rằng, có thể ban hành Luật mẫu trên một cách độc lập; hoặc kết hợp với Luật mẫu về Thương mại điện tử của UNCITRAL, vì nó được quyết định soạn thảo như là một văn kiện pháp lý (xem A/CN.9/465, đoạn 37). Quyết định này xuất phát từ thực tế, tại thời điểm Luật mẫu trên đang được hoàn thành, Luật mẫu về Thương mại điện tử của UNCITRAL đã được thực thi thành công tại tại nhiều nước và được thông qua tại nhiều nước khác. Việc soạn thảo phiên bản mở rộng của Luật mẫu về Thương mại điện tử của UNCITRAL có thể đạt được sự thành công như phiên bản ban đầu. Thêm vào đó, việc soạn thảo một phiên bản mới của Luật mẫu về Thương mại điện tử của UNCITRAL có thể làm nhiều nước vừa mới thông qua Luật mẫu này trở nên lúng túng.

2. Luật mẫu trên phù hợp hoàn toàn với Luật mẫu về Thương mại điện tử của UNCITRAL

66. Trong quá trình soạn thảo Luật mẫu trên, mọi nỗ lực được đưa ra nhằm đảm bảo tính nhất quán với nội dung và thuật ngữ trong Luật mẫu về Thương mại điện tử của UNCITRAL (xem A/CN.9/465, đoạn 37). Các điều khoản

chung trong Luật mẫu về Thương mại điện tử của UNCITRAL đã được xem xét lại trong một văn kiện mới. Cụ thể là các mục 1 (Phạm vi ứng dụng), 2(a), (c) và (d) (Các định nghĩa về "thông báo dữ liệu", "người tạo thông báo" và "người nhận"), 3 (Làm sáng tỏ), 4 (Thay đổi thông qua thoả thuận) và 7 (Chữ ký) trong Luật mẫu về Thương mại điện tử của UNCITRAL .

67. Dựa vào Luật mẫu về Thương mại điện tử của UNCITRAL, Luật mẫu trên dự định phản ánh nguyên tắc *phương tiện truyền thông trung lập*; hướng tiếp cận không phân biệt các hoạt động trên giấy tờ truyền thống và môi trường điện tử; và tin cậy vào khả năng tự quyết của thành viên (A/CN.9/WG.IV/WP.84, đoạn 16). Ngoài ra, nó dự định sử dụng cả các chuẩn tối thiểu trong môi trường "mở" (là nơi các thành viên truyền thông với nhau mà không cần thoả thuận từ trước) và các điều khoản hợp đồng hiện đại, hoặc các quy tắc ngầm định trong môi trường "khép kín" (là nơi các thành viên bị giới hạn thông qua các quy tắc và thủ tục hợp đồng tồn tại từ trước, khi truyền thông bằng các phương tiện điện tử).

3. Mối quan hệ với mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL

68. Trong quá trình soạn thảo Luật mẫu trên, quan điểm được nhấn mạnh là việc tham chiếu mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL với mục 6 của Luật mẫu trên cần được làm sáng tỏ, như giới hạn phạm vi của Luật mẫu trên chỉ tập trung vào các trường hợp - trong đó, chữ ký điện tử được đưa ra để đáp ứng yêu cầu bắt buộc của luật pháp, cụ thể, các tài liệu phải được ký vì mục đích *hiệu lực pháp lý*. Theo quan điểm này, hầu hết các Quốc gia đều có yêu cầu như vậy đối với các tài liệu được sử dụng trong giao dịch thương mại, phạm vi của Luật mẫu trên rất hạn hẹp. Chính vì vậy, việc làm sáng tỏ mục 6 (và mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL) không nhất quán với việc làm sáng tỏ các từ "luật" được Uỷ ban thông qua trong đoạn 68 của bản hướng dẫn ban hành Luật mẫu về Chữ ký điện tử của UNCITRAL. Theo bản hướng dẫn này, từ "luật" được hiểu là không chỉ bao hàm luật chế định hoặc luật sửa đổi, mà còn bao hàm cả luật được tạo ra về phương diện pháp lý và luật theo thủ tục khác. Thực tế, phạm vi của mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL và mục 6 Luật mẫu về Chữ ký điện tử của UNCITRAL rất rộng, khi hầu hết các tài liệu được sử dụng trong giao dịch thương mại có thể phải tuân theo các yêu cầu của luật cung cấp bằng chứng trong văn bản (A/CN.9/465, đoạn 67).

C. Các quy tắc "khung" được bổ sung thông qua các hợp đồng và quy định kỹ thuật

69. Để bổ sung thêm cho Luật mẫu về Thương mại điện tử của UNCITRAL, Luật mẫu trên dự định cung cấp các nguyên tắc thiết yếu nhằm tạo điều kiện cho việc sử dụng các chữ ký điện tử. Tuy nhiên, Luật mẫu không tự thiết lập tất cả các quy tắc và quy định cần thiết (bổ sung thêm vào các hợp đồng giữa những người sử dụng) nhằm thực thi các kỹ thuật này tại nước ban hành luật. Hơn nữa, như đã được chỉ ra trong bản hướng dẫn này, Luật mẫu không dự định bao trùm lên tất cả các khía cạnh của việc sử dụng các chữ ký điện tử. Do đó, nước ban hành luật có thể phát hành các quy định nhằm hoàn thiện các thủ tục mà Luật mẫu cho phép, quan tâm đến các trường hợp xác định, có thể thay đổi, xảy ra ở nước ban hành luật mà không bao gồm các mục tiêu của Luật mẫu. Khuyến nghị rằng, khi quyết định phát hành các quy định này, nước ban hành luật nên chú ý tới việc đảm bảo tính mềm dẻo trong hoạt động của các hệ thống chữ ký điện tử. Hoạt động thương mại có sự tín nhiệm lâu đời dựa vào việc xử lý tự giác các chuẩn kỹ thuật. Các chuẩn kỹ thuật này làm cơ sở cho các đặc tả sản phẩm, thiết kế tiêu chuẩn, sự nhất trí trong nghiên cứu và phát triển các sản phẩm tương lai. Để đảm bảo tính mềm dẻo cho các hoạt động thương mại này, đồng thời xúc tiến các chuẩn mở rộng (với quan điểm tạo điều kiện cho khả năng liên vận hành) và hỗ trợ mục tiêu công nhận qua biên giới (đã được trình bày trong mục 12), các nước có quyền quan tâm tới mối quan hệ của các đặc tả được kết hợp bất kỳ, hoặc có trong các quy định Quốc gia và xử lý tự giác các chuẩn kỹ thuật (xem A/CN.9/484, đoạn 46).

70. Lưu ý rằng, các kỹ thuật chữ ký điện tử được quan tâm trong Luật mẫu vượt ra ngoài các vấn đề về thủ tục cần được giải quyết khi thực thi các quy định về kỹ thuật, điều này có thể nảy sinh nhiều câu hỏi pháp lý, không nhất thiết phải tìm kiếm câu trả lời trong Luật mẫu này, nhưng có thể tìm thấy trong các luật cụ thể khác. Ví dụ, các luật này có thể bao gồm luật quản trị có thể áp dụng, hợp đồng, luật về tội phạm và thủ tục - toà án mà Luật mẫu không dự định giải quyết.

D. Làm tăng tính chắc chắn về hiệu lực pháp lý của các chữ ký điện tử

71. Một trong các đặc điểm chính của Luật mẫu trên là làm tăng tính chắc chắn của thực hiện bộ tiêu chuẩn mềm dẻo được đưa ra trong mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL, công nhận chữ ký điện tử có chức

năng ngang bằng với chữ ký viết tay. Mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL như sau:

(1) Khi luật pháp yêu cầu chữ ký của một người, yêu cầu này được đáp ứng trong mối quan hệ với một thông báo dữ liệu, nếu:

(a) sử dụng một phương pháp để nhận dạng người này và chỉ ra rằng, người này đã phê chuẩn thông tin có trong thông báo dữ liệu; và

(b) phương pháp này đáng tin cậy và thích hợp cho mục đích -trong đó, thông báo dữ liệu được tạo ra hoặc truyền đi, dưới ánh sáng của tất cả các trường hợp, bao gồm mọi thoả thuận liên quan.

(2) Đoạn (1) áp dụng khi yêu cầu trong đó mang tính nghĩa vụ, hoặc đơn giản, luật đưa ra hậu quả của việc thiếu chữ ký.

(3) "Các điều khoản của mục này không áp dụng cho [...]".

72. Mục 7 dựa vào việc công nhận các chức năng của một chữ ký trong môi trường giấy tờ, được trình bày trong đoạn 29 ở trên.

73. Với quan điểm đảm bảo rằng, không nên phủ nhận giá trị pháp lý của một thông báo vì lý do duy nhất: nó không được xác thực theo cách thức trên giấy tờ, mục 7 phê chuẩn một hướng tiếp cận toàn diện. Nó thiết lập các điều kiện chung theo thông báo dữ liệu được xác thực đủ tin cậy và có thể chống lại các yêu cầu chữ ký hiện là rào cản của thương mại điện tử. Mục 7 tập trung vào 2 chức năng cơ bản của một chữ ký, đó là nhận dạng người tạo tài liệu và xác nhận rằng người này đã phê chuẩn nội dung của tài liệu đó. Đoạn (1)(a) thiết lập nguyên tắc: trong môi trường điện tử, các chức năng cơ bản của một chữ ký được thực hiện thông qua phương pháp nhận dạng người tạo thông báo dữ liệu và xác nhận rằng anh ta đã phê chuẩn nội dung của thông báo này.

74. Đoạn (1)(b) thiết lập một hướng tiếp cận mềm dẻo cho mức an toàn cần đạt được, thông qua phương pháp nhận dạng được sử dụng trong đoạn (1)(a). Phương pháp được sử dụng trong đoạn (1)(a) nên được tin cậy và phù hợp với mục đích - trong đó, thông báo dữ liệu được tạo ra và truyền đi, dưới ánh sáng của tất cả các trường hợp, bao gồm bất kỳ thoả thuận nào giữa người tạo thông báo và người nhận thông báo.

75. Khi quyết định phương pháp được sử dụng trong đoạn (1) có thích hợp hay không, các yếu tố pháp lý, kỹ thuật và thương mại cần được quan tâm có thể là (1) độ phức tạp của thiết bị do từng thành viên sử dụng; (2) bản chất tự

nhiên của hoạt động kinh doanh; (3) tần xuất giao dịch thương mại có sự tham gia của các thành viên; (4) kiểu và quy mô giao dịch; (5) chức năng của chữ ký trong môi trường luật quy định và sửa đổi; (6) khả năng mở rộng của các hệ thống truyền thông; (7) tuân theo các thủ tục xác thực được thiết lập trong các giai đoạn trung gian; (8) dãy các thủ tục xác thực sẵn sàng trong giai đoạn trung gian bất kỳ; (9) tuân theo các hoạt động và tập quán kinh doanh; (10) tồn tại các cơ chế đảm bảo dựa vào các thông báo không được phép; (11) tầm quan trọng và giá trị của thông tin có trong thông báo dữ liệu; (12) tính sẵn sàng của các phương pháp nhận dạng lựa chọn và chi phí thực hiện; (13) mức độ chấp nhận hoặc không chấp nhận phương pháp nhận dạng trong lĩnh vực liên quan, tại thời điểm phương pháp được chấp thuận và khi thông báo dữ liệu được truyền đi; và (14) các yếu tố liên quan khác (Hướng dẫn ban hành Luật mẫu về Thương mại điện tử của UNCITRAL, các đoạn 53, 56 đến 58).

Điều 76. Khi xây dựng bộ tiêu chuẩn mềm dẻo (được đưa ra trong mục 7 (1)(b) Luật mẫu về Thương mại điện tử của UNCITRAL), mục 6 và 7 của Luật mẫu trên thiết lập một cơ chế, thông qua nó các chữ ký điện tử (thoả mãn tiêu chuẩn tin cậy về kỹ thuật) có thể được tạo ra và có hiệu lực pháp lý. Tuỳ thuộc vào thời điểm đạt được sự chắc chắn, cũng như sự công nhận một chữ ký điện tử có chức năng ngang bằng với một chữ ký viết tay, Luật mẫu trên thiết lập hai chế độ khác nhau. Chế độ đầu tiên rộng hơn và được mô tả trong mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL . Nó công nhận bất kỳ "phương pháp" nào có thể được sử dụng, nhằm đáp ứng yêu cầu pháp lý của một chữ ký viết tay. Hiệu lực pháp lý của "phương pháp" (ngang bằng với một chữ ký viết tay) này phụ thuộc vào việc chứng minh "tính tin cậy" của nó trong thử nghiệm thực tế. Chế độ thứ 2 hẹp hơn, do Luật mẫu trên đưa ra. Nó dự tính các phương pháp chữ ký điện tử được một cơ quan Quốc gia, một thực thể được uỷ quyền, hoặc các thành viên khác công nhận, khi chúng thoả mãn tiêu chuẩn tin cậy về kỹ thuật được đưa ra trong Luật mẫu (xem A/CN.9/484, đoạn 49). Thuận lợi của việc công nhận này là nó có thể mang lại sự chắc chắn cho những người sử dụng các kỹ thuật chữ ký điện tử này, trước khi họ sử dụng chúng trong thực tế.

E. Các quy tắc cơ bản trong việc hướng dẫn các thành viên tham gia

77. Luật mẫu không giải quyết một cách chi tiết các vấn đề về trách nhiệm pháp lý mà có thể ảnh hưởng đến các thành viên khác cùng tham gia hệ thống

chữ ký điện tử. Các vấn đề này có thể được giải quyết trong các luật có thể áp dụng khác. Hơn nữa, Luật mẫu đưa ra tiêu chuẩn, thông qua đó có thể hướng dẫn các thành viên như người ký, thành viên tin cậy và nhà cung cấp dịch vụ chứng thực.

78. Với người ký, Luật mẫu bổ sung thêm vào nguyên tắc cơ bản như sau: người ký nên quan tâm hợp lý tới dữ liệu tạo chữ ký điện tử của mình. Sự quan tâm hợp lý này có thể ngăn chặn việc sử dụng trái phép dữ liệu tạo chữ ký. Tự bản thân chữ ký số không đảm bảo rằng, người tiến hành ký trong thực tế chính là người ký. Trong điều kiện tốt nhất, chữ ký số đảm bảo rằng nó là thuộc tính của người ký (xem A/CN.9/484, đoạn 50). Khi người ký biết hoặc được biết dữ liệu tạo chữ ký bị lộ, người ký nên thông báo ngay lập tức cho bất kỳ ai tin cậy chữ ký, hoặc cung cấp dịch vụ hỗ trợ chữ ký điện tử. Khi sử dụng một chứng chỉ để hỗ trợ chữ ký điện tử, người ký nên quan tâm hợp lý để đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn cần thiết (do người ký tạo ra) liên quan tới chứng chỉ.

79. Thành viên tin cậy cần tiến hành từng bước hợp lý để kiểm tra tính tin cậy của một chữ ký điện tử. Khi chữ ký điện tử được hỗ trợ thông qua một chứng chỉ, thành viên tin cậy nên tiến hành từng bước hợp lý để kiểm tra tính hợp lệ, tình trạng treo hoặc huỷ bỏ của chứng chỉ và tuân theo mọi giới hạn dành cho chứng chỉ.

80. Trách nhiệm chính của nhà cung cấp dịch vụ chứng thực là sử dụng các hệ thống, thủ tục và nguồn tài nguyên con người tin cậy; đồng thời, hoạt động phù hợp với các biểu diễn về chính sách và hoạt động do chính nhà cung cấp dịch vụ chứng thực đưa ra. Thêm vào đó, nhà cung cấp dịch vụ chứng thực cần quan tâm hợp lý để đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn liên quan tới một chứng chỉ. Trong chứng chỉ, nhà cung cấp nên cung cấp các thông tin thiết yếu, từ đó cho phép thành viên tin cậy nhận dạng nhà cung cấp. Đồng thời, biểu diễn rằng: (1) người ký (được nhận dạng trong chứng chỉ) kiểm soát được dữ liệu tạo chữ ký tại thời điểm chứng chỉ được phát hành; (2) dữ liệu tạo chữ ký được kích hoạt tại hoặc trước ngày chứng chỉ được phát hành. Vì lợi ích của thành viên tin cậy, nhà cung cấp dịch vụ chứng thực nên cung cấp thêm các thông tin về: (1) phương pháp được sử dụng để nhận dạng người ký; (2) mọi giới hạn liên quan tới mục đích hoặc giá trị dành cho dữ liệu tạo chữ ký hoặc chứng chỉ có thể được sử dụng; (3) điều kiện kích hoạt dữ liệu

tạo chữ ký; (4) mọi giới hạn liên quan tới phạm vi trách nhiệm pháp lý của nhà cung cấp dịch vụ chứng thực; (5) các hình thức mà người ký sử dụng để thông báo dữ liệu tạo chữ ký bị lộ; và (6) dịch vụ huỷ bỏ kịp thời.

81. Về việc đánh giá mức tin cậy của các hệ thống, thủ tục và nguồn tài nguyên con người mà nhà cung cấp dịch vụ sử dụng, Luật mẫu cung cấp một danh sách không hạn chế các yếu tố chỉ báo.

F. Khung công nghệ trung lập

82. Đứng trước sự đổi mới về công nghệ, Luật mẫu đưa ra tiêu chuẩn công nhận về mặt pháp lý cho các chữ ký điện tử, không kể công nghệ được sử dụng (chẳng hạn như, các chữ ký số dựa vào mật mã phi đối xứng; các thiết bị sinh trắc học (cho phép nhận dạng cá nhân thông qua các đặc điểm vật lý, như bàn tay hoặc khuôn mặt, đọc dấu vân tay, nhận dạng tiếng nói, hoặc quét võng mạc,...); mật mã đối xứng; sử dụng số hiệu nhận dạng cá nhân (PIN); sử dụng "thẻ bài" để xác thực các thông báo dữ liệu, ví dụ thẻ thông minh hoặc thiết bị khác do người ký nắm giữ; các mẫu chữ ký viết tay được số hoá; các phương pháp khác, chẳng hạn nhấn vào một "OK-box"). Các kỹ thuật được liệt kê khác có thể sử dụng kết hợp với nhau, nhằm giảm rủi ro (xem A/CN.9/484, đoạn 52).

G. Không phân biệt các chữ ký điện tử nước ngoài

83. Luật mẫu thiết lập một nguyên tắc cơ bản: nơi tạo ra và sử dụng không phải là yếu tố xác định các chữ ký điện tử hoặc chứng chỉ của nước ngoài được công nhận về mặt pháp lý; hoặc mức độ công nhận này ra sao tại nước ban hành luật (xem A/CN.9/484, đoạn 53). Việc xác định hiệu lực pháp lý của một chứng chỉ hoặc một chữ ký điện tử không phụ thuộc vào nơi chứng chỉ hoặc chữ ký được phát hành (xem A/CN.9/483, đoạn 27), mà phụ thuộc vào mức tin cậy về mặt kỹ thuật của nó. Nguyên tắc cơ bản này được giải thích chi tiết hơn trong mục 12 (xem các đoạn 152-160 dưới đây).

V. SỰ TRỢ GIÚP TỪ PHÒNG THƯ KÝ CỦA UNCITRAL

A. Sự trợ giúp trong quá trình soạn thảo luật

84. Trong phạm vi của các hoạt động trợ giúp và đào tạo, Phòng thư ký của UNCITRAL trợ giúp cho các nước, cùng với các tham khảo về kỹ thuật, khi các nước này soạn thảo luật dựa vào Luật mẫu về Chữ ký điện tử của UNCITRAL. Đồng thời, trợ giúp cho các Chính phủ quan tâm tới luật trên cơ

sở của các Luật mẫu khác của UNCITRAL (như Luật mẫu về Trọng tài Thương mại Quốc tế, Luật mẫu về Chuyển tín dụng Quốc tế, Luật mẫu về Thu mua hàng hoá, xây dựng và dịch vụ, Luật mẫu về Thương mại điện tử và Luật mẫu về Phá sản qua biên giới của UNCITRAL), hoặc quan tâm tới việc tham gia vào một trong các công ước thương mại Quốc tế do UNCITRAL soạn thảo.

85. Các thông tin khác liên quan tới Luật mẫu trên và các Luật mẫu khác, các công ước do UNCITRAL phát triển, có thể yêu cầu Phòng thư ký cung cấp theo địa chỉ sau:

International Trade Law Branch, Office of Legal Affairs

United Nations

Viennna International Centre

P.O.Box 500

A-1400, Vienna, Austria

Telephone: (+43-1) 26060 - 4060 hoặc 4061

Telecopy: (+43-1) 26060 - 5813

E-mail: uncitral@uncitral.org

Internet Home Page: http://www.uncitral.org

B. Thông tin về việc làm sáng tỏ luật dựa vào Luật mẫu

86. Phòng thư ký mong chờ nhận được những lời nhận xét về Luật mẫu, bản hướng dẫn và những thông tin liên quan đến việc ban hành luật dựa vào Luật mẫu. Một khi đã ban hành, Luật mẫu sẽ nằm trong hệ thống thông tin CLOUT, nó được sử dụng để chọn lựa và phổ biến thông tin trong trường hợp luật liên quan tới các công ước và Luật mẫu do UNCITRAL đưa ra. Mục đích của hệ thống thông tin này là xúc tiến nhận thức về các văn bản pháp lý Quốc tế do UNCITRAL đưa ra; tạo điều kiện làm sáng tỏ và áp dụng thống nhất. Phòng thư ký phát hành (bằng 6 ngôn ngữ chính thức của Liên Hợp Quốc) bản tóm tắt về các quyết định và làm cho chúng có hiệu lực. Hệ thống được giải thích trong sách hướng dẫn người dùng do Phòng thư ký cung cấp (xem A/CN.9/SER.C/GUIDE/1) và trang chủ trên Internet của UNCITRAL.

Chương II

GIẢI THÍCH CHI TIẾT CÁC MỤC TRONG LUẬT MẪU

87. Trong quá trình soạn thảo, văn kiện này xuất phát từ Luật mẫu về Thương mại điện tử của UNCITRAL, nó cần có vị trí ngang bằng và hợp pháp như Luật mẫu về Thương mại điện tử của UNCITRAL.

Mục 1: Phạm vi ứng dụng

Luật này áp dụng cho các chữ ký điện tử được sử dụng trong phạm vi* hoạt động thương mại**. Tuân thủ mục đích bảo vệ các khách hàng.

* Uỷ ban đề nghị đoạn văn bản dưới đây dành cho các nước mong muốn mở rộng khả năng áp dụng đối với luật này:

" Luật này áp dụng khi các chữ ký điện tử được sử dụng, ngoại trừ trong các trường hợp riêng của Quốc gia áp dụng."

** Thuật ngữ "thương mại" nên được làm sáng tỏ để bao trùm lên các vấn đề xuất phát từ các mối quan hệ tự nhiên của thương mại, cho dù có hợp đồng hay không. Các quan hệ tự nhiên của thương mại bao gồm các giao dịch sau, nhưng không chỉ giới hạn trong đó: mọi giao dịch được thực hiện để cung cấp hoặc trao đổi hàng hoá hoặc dịch vụ; thoả thuận phân phối; đại diện hoặc đại lý thương mại; phương pháp đại lý; thuê tài sản; tư vấn; kỹ thuật; đăng ký; đầu tư; tài chính; ngân hàng; bảo hiểm; thoả thuận hoặc đặc quyền khai thác; liên doanh và các dạng hợp tác kinh doanh; vận chuyển hàng hoá hoặc hành khách thông qua các hình thức như hàng không, đường biển, đường sắt hoặc đường bộ.

Nhận xét chung

88. Mục đích của mục 1 là chỉ ra phạm vi ứng dụng của Luật mẫu. Hướng tiếp cận được sử dụng trong Luật mẫu là đảm bảo nguyên tắc bao trùm lên tất cả các trường hợp thực tế - nơi áp dụng các chữ ký điện tử, không kể chữ ký điện tử hoặc kỹ thuật xác thực riêng được sử dụng. Trong quá trình soạn thảo Luật mẫu cũng loại trừ các khả năng gây khó khăn, hoặc hạn chế phạm vi áp dụng của Luật mẫu, Nhóm làm việc về thương mại điện tử của UNCITRAL tôn trọng nguyên tắc công nghệ trung lập, mặc dù "các chữ ký số" (là các chữ ký điện tử được tạo ra, bằng cách áp dụng mật mã khoá công khai) được nhìn nhận là một công nghệ áp dụng đặc biệt rộng rãi (xem A/CN.9/484, đoạn 54).

Chú thích **

89. Luật mẫu nên chỉ rõ rằng, Luật mẫu tập trung vào các kiểu trường hợp xảy ra trong lĩnh vực thương mại, cơ sở của nó là các mối quan hệ trong thương mại và tài chính. Vì lý do này, mục 1 ám chỉ "các hoạt động thương mại" và cung cấp chỉ báo về các hoạt động này, trong chú thích **. Để đảm bảo tính chặt chẽ, các chỉ báo này (đặc biệt hữu ích cho một số nước không có luật thương mại riêng) được đưa vào các chú thích trong mục 1 Luật mẫu về trọng tài thương mại Quốc tế của UNCITRAL (hay trong chú thích **** mục 1 Luật mẫu về Thương mại điện tử của UNCITRAL). Hiện có một số nước, việc sử dụng chú thích trong một văn bản luật quy định không được xem là hoạt động lập pháp được chấp nhận. Do vậy, các cơ quan Quốc gia ban hành Luật mẫu có thể quan tâm hợp lý tới phần chú thích trong văn bản luật.

*Chú thích **

90. Luật mẫu được áp dụng cho tất cả các kiểu thông báo dữ liệu có gắn chữ ký điện tử hợp pháp, không có điều gì trong Luật mẫu cản trở nước ban hành luật mở rộng phạm vi của Luật mẫu ra ngoài lĩnh vực thương mại. Ví dụ, Luật mẫu không tập trung vào các quan hệ giữa những người sử dụng chữ ký điện tử và cơ quan công cộng, Luật mẫu không được dự định áp dụng cho các quan hệ này. Chú thích* là cách diễn đạt lựa chọn, các nước ban hành luật có thể sử dụng nếu chúng phù hợp cho việc mở rộng phạm vi của Luật mẫu ra ngoài lĩnh vực thương mại.

Bảo vệ khách hàng

91. Một số nước có các luật bảo vệ khách hàng riêng, chúng quản lý các khía cạnh nào đó của việc sử dụng hệ thống thông tin. Về luật bảo vệ khách hàng, cụ thể là các văn kiện trước đó của UNCITRAL (như Luật mẫu về chuyển nhượng tín dụng Quốc tế và Luật mẫu về Thương mại điện tử của UNCITRAL), nên đưa ra chỉ báo: Luật mẫu được soạn thảo nhưng không tập trung đặc biệt vào các vấn đề phát sinh trong phạm vi bảo vệ khách hàng. Tại cùng thời điểm, có ý kiến cho rằng, không có lý do gì để loại trừ các trường hợp, trong đó có sự tham gia của các khách hàng, ra khỏi phạm vi của Luật mẫu. Các điều khoản của Luật mẫu có thể tìm ra lợi ích của việc bảo vệ khách hàng tuỳ thuộc vào việc ban hành luật tại mỗi nước. Mục 1 công nhận rằng, các luật bảo vệ khách hàng như vậy có thể có quyền ưu tiên cao hơn các điều khoản trong

Luật mẫu. Các nhà làm luật nên đưa ra các cách giải quyết khác nhau về hiệu lực của Luật mẫu trong các giao dịch khách hàng.

Sử dụng các chữ ký điện tử trong các giao dịch Quốc tế và nội địa

92. Khuyến nghị rằng, khả năng áp dụng Luật mẫu không bị hạn chế. Nên đưa ra cảnh báo cụ thể khi loại trừ khả năng áp dụng của Luật mẫu, vì điều này làm ảnh hưởng đến các mục tiêu của Luật mẫu. Luật mẫu cần thiết cho thương mại Quốc tế và nội địa. Sự phân biệt giữa các chữ ký điện tử được sử dụng trong nước và các chữ ký điện tử được sử dụng cho các giao dịch thương mại Quốc tế có thể gây ra sự không đồng nhất trong việc quản lý, điều này cản trở nghiêm trọng việc sử dụng các kỹ thuật này (xem A/CN.9/484, đoạn 55).

Các tài liệu tham khảo của UNCITRAL

A/CN.9/484, các đoạn 54-55;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 87-91;

A/CN.9/467, các đoạn 22-24;

A/CN.9/WG.IV/WP.84, đoạn 22;

A/CN.9/465, các đoạn 36-42;

A/CN.9/WG.IV/WP.82, đoạn 21;

A/CN.9/457, các đoạn 53-64.

Mục 2. Các định nghĩa

Phù hợp với các mục đích của luật này:

(a) Chữ ký điện tử

Là dữ liệu được lưu giữ ở dạng điện tử, được gắn vào một thông báo để nhận dạng người ký, chỉ ra rằng thông tin có trong thông báo đã được người ký phê chuẩn.

(b) Chứng chỉ

Là thông báo hoặc bản ghi, được sử dụng để xác nhận mối liên kết giữa người ký và dữ liệu tạo chữ ký.

(c) Thông báo dữ liệu

Là thông tin được tạo ra, gửi/nhận, lưu giữ bằng các hình thức điện tử, quang học, hoặc các hình thức khác như EDI (trao đổi dữ liệu điện tử), thư tín điện tử, điện tín, telex.

(d) Người ký

Là người nắm giữ dữ liệu tạo chữ ký, đại diện cho chính bản thân người ký hoặc đại diện cho người khác.

(e) Nhà cung cấp dịch vụ chứng thực

Là người phát hành các chứng chỉ và có thể cung cấp các dịch vụ khác liên quan đến các chữ ký điện tử.

(f) Thành viên tin cậy

Là người có thể hoạt động dựa vào chứng chỉ hoặc chữ ký điện tử.

Định nghĩa "chữ ký điện tử"

Chữ ký điện tử có chức năng ngang bằng với chữ ký viết tay

93. Khái niệm "chữ ký điện tử" được dự định bao trùm lên tất cả các sử dụng truyền thống của một chữ ký viết tay có hiệu lực pháp lý, nhận dạng người ký và các hướng tiếp cận "chữ ký" được tìm thấy trong các hệ thống pháp lý khác nhau. Các chức năng của một chữ ký viết tay được thảo luận trong quá trình soạn thảo mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL . Định nghĩa không coi nhẹ yếu tố thực tế: các công nghệ thường được xem như là "các chữ ký điện tử" có thể được sử dụng cho các mục đích khác, ngoài việc tạo ra một chữ ký đủ hợp pháp. Đơn giản, định nghĩa nhấn mạnh Luật mẫu đã tập trung vào việc sử dụng các chữ ký điện tử có chức năng ngang bằng với chữ ký viết tay (xem A/CN.9/483, đoạn 62).

Các sử dụng khác của một chữ ký điện tử

94. Nên phân biệt giữa khái niệm pháp lý của "chữ ký" và khái niệm kỹ thuật của "chữ ký điện tử". Trong quá trình soạn thảo Luật mẫu, có ý kiến cho rằng, người sử dụng quan tâm tới các rủi ro là kết quả của việc sử dụng cùng một công cụ kỹ thuật cho việc tạo ra một chữ ký hợp pháp và cho các chức năng xác thực, hoặc nhận dạng khác.

Định nghĩa "chứng chỉ"

95. Thuật ngữ "chứng chỉ" được sử dụng trong phạm vi của các kiểu chữ ký điện tử xác định và được định nghĩa trong Luật mẫu. Chứng chỉ (được nói đến ở đây) được sử dụng trong môi trường điện tử, không phải trên giấy tờ (xem A/CN.9/484, đoạn 56). Tuy nhiên, do định nghĩa chung về "chứng chỉ" không tồn tại các hệ thống pháp lý hoặc trong tất cả các ngôn ngữ, định nghĩa này hữu ích trong phạm vi của Luật mẫu (xem A/CN.9/483, đoạn 65).

Mục đích của chứng chỉ

96. Mục đích của chứng chỉ là công nhận, biểu diễn hoặc xác nhận liên kết giữa dữ liệu tạo chữ ký và người ký. Liên kết này được tạo ra khi dữ liệu tạo chữ ký được sinh ra (xem đoạn 67).

"Dữ liệu tạo chữ ký"

97. Trong phạm vi của các chữ ký điện tử (không phải là các chữ ký số), thuật ngữ "dữ liệu tạo chữ ký" chỉ các khoá bí mật, các chương trình hoặc các yếu tố khác trong quá trình tạo chữ ký điện tử, cung cấp một liên kết an toàn giữa chữ ký và người ký. Ví dụ, với các chữ ký điện tử dựa vào thiết bị sinh trắc học, yếu tố thiết yếu là chỉ báo sinh trắc học, chẳng hạn dấu vân tay hoặc đặc điểm võng mạc. Sự mô tả này chỉ bao trùm lên các yếu tố hạt nhân có vai trò trong việc đảm bảo bí mật, chất lượng của quá trình ký, loại bỏ các yếu tố khác (mặc dù chúng có tham gia vào quá trình ký) và cho phép xem xét các yếu tố này vì không ảnh hưởng tới tính tin cậy của chữ ký điện tử. Nói cách khác, trong phạm vi của các chữ ký số dựa vào mật mã phi đối xứng, yếu tố hạt nhân chính là cặp khoá. Với các chữ ký số, khoá riêng và khoá công khai được liên kết với người ký. Mục đích cơ bản của một chứng chỉ là xác nhận liên kết giữa khóa công khai và người ký, khoá công khai được chứng nhận thuộc quyền sở hữu của người ký. Để tránh rắc rối, định nghĩa "chứng chỉ" trong mục 2 (b) nên bao gồm cả việc xác nhận liên kết giữa người ký và khoá công khai của người ký. Yếu tố không nằm trong mô tả này là văn bản được ký số, mặc dù nó đóng một vai trò rất quan trọng trong quá trình tạo chữ ký (thông qua một hàm băm hoặc cách khác). Mục 6 nhấn mạnh rằng dữ liệu tạo chữ ký nên được liên kết với người ký và không một ai khác.

Định nghĩa "thông báo dữ liệu"

98. Định nghĩa "thông báo dữ liệu" được đưa ra trong mục 2 Luật mẫu về Thương mại điện tử của UNCITRAL là một khái niệm bao hàm tất cả các thông báo được tạo ra trong phạm vi thương mại điện tử, bao gồm cả thương mại dựa trên Web (xem đoạn 69). Khái niệm "thông báo dữ liệu" không bị giới hạn trong truyền thông, nhưng nó cũng bao hàm các bản ghi được tạo ra trên máy tính cho dù các bản ghi này không được dự định sử dụng trong truyền thông. Do vậy, khái niệm thông báo bao gồm cả khái niệm "bản ghi".

99. Tham chiếu "Phương tiện tương tự" được sử dụng để phản ánh thực tế: Luật mẫu không chỉ được áp dụng trong phạm vi của các kỹ thuật truyền thông hiện có, mà còn được sử dụng để hỗ trợ các phát triển kỹ thuật trong tương lai.

Mục đích của định nghĩa "thông báo dữ liệu" là chỉ ra các kiểu thông báo được tạo ra, lưu giữ hoặc truyền đi theo một khuôn dạng không hoàn toàn giống trên giấy tờ. Vì mục đích này, tất cả các phương tiện truyền thông hoặc lưu giữ thông tin có thể thực hiện các chức năng tương đương với các chức năng do các công cụ được liệt kê trong định nghĩa thực hiện. Vì mục đích này, từ "tương tự" có nghĩa là "ngang bằng về chức năng".

100. Định nghĩa "thông báo dữ liệu" còn được áp dụng trong trường hợp huỷ bỏ hoặc sửa đổi. Một thông báo dữ liệu có nội dung thông tin cố định, nhưng nó có thể bị thông báo dữ liệu khác huỷ bỏ hoặc sửa đổi (Bản hướng dẫn ban hành Luật mẫu về Thương mại điện tử của UNCITRAL, các đoạn từ 30-32).

Định nghĩa "người ký"

"một người"

101. Để phù hợp với hướng tiếp cận được đưa ra trong Luật mẫu về Thương mại điện tử của UNCITRAL, bất kỳ tham chiếu nào chỉ tới "một người" trong Luật mẫu trên nên được hiểu là nó bao trùm lên tất cả các kiểu người hoặc thực thể, cho dù là thực thể vật lý, tổ chức hoặc pháp nhân khác (xem A/CN.9/483, đoạn 86).

"Đại diện cho một người"

102. Các chữ ký viết tay thường không phù hợp với các thuận lợi mà công nghệ hiện đại mang lại. Ví dụ, nói đúng ra, trong môi trường giấy tờ, các thực thể hợp pháp không thể là người ký các tài liệu được thảo ra nhân danh mình, vì chỉ con người mới có thể đưa ra các chữ ký viết tay đích thực. Tuy nhiên, các chữ ký điện tử có thể được xem là thuộc tính của các công ty, hoặc các thực thể hợp pháp khác (bao gồm các cơ quan của chính phủ và cơ quan công cộng khác) và có thể xảy ra các trường hợp - trong đó, định danh của một người (thực tế đã tạo ra chữ ký) không thích hợp với các mục đích dành cho chữ ký được tạo ra (xem đoạn 85).

103. Tuy nhiên, theo Luật mẫu trên, khái niệm "người ký" không phải là người, hoặc thực thể đã thực sự tạo ra chữ ký, vì một trong các nghĩa vụ của người ký là kiểm soát dữ liệu tạo chữ ký. Tuy nhiên, để bao trùm lên các trường hợp - trong đó, người ký hoạt động đại diện cho người khác, cụm từ "thay mặt cho người khác" cũng nằm trong định nghĩa "người ký". Vấn đề "thay mặt" này được giải quyết tuỳ thuộc vào luật quản lý, được xem là quan

hệ hợp pháp và thích hợp giữa người ký và người có chữ ký điện tử thay mặt cho mình. Vấn đề này, cũng như các vấn đề khác liên quan tới giao dịch cơ sở, như các vấn đề về đại lý và các câu hỏi liên quan khác về người chịu trách nhiệm pháp lý sau cùng do lỗi người ký gây ra, tuân theo các nghĩa vụ trong mục 8 (cho dù anh ta là người ký hay là người được người ký đại diện) nằm ngoài phạm vi của Luật mẫu (xem các đoạn 86-87).

Định nghĩa "nhà cung cấp dịch vụ chứng thực"

104. Tối thiểu, nhà cung cấp dịch vụ chứng thực (như đã được định nghĩa ở trên, phù hợp với các mục đích của Luật mẫu) phải cung cấp các dịch vụ chứng thực, ngoài ra có thể kết hợp với các dịch vụ khác (xem đoạn 100).

105. Như đã được trình bày rõ trong Luật mẫu, không phân biệt các trường hợp - trong đó, nhà cung cấp dịch vụ chứng thực thực hiện điều khoản về các dịch vụ chứng thực như là hoạt động chính của mình, có thể thường xuyên hoặc không thường xuyên, trực tiếp hoặc thông qua nhà thầu phụ. Định nghĩa bao trùm lên tất cả các thực thể cung cấp dịch vụ chứng thực trong phạm vi của Luật mẫu, có nghĩa là, "trong phạm vi của các hoạt động thương mại". Tuy nhiên, để phù hợp với phạm vi ứng dụng của Luật mẫu, nếu thực thể phát hành các chứng chỉ vì mục đích bên trong và không phải là các mục đích thương mại, thì không được liệt vào loại "nhà cung cấp dịch vụ chứng thực" theo định nghĩa trong mục 2 (xem các đoạn 94-99).

Định nghĩa "thành viên tin cậy"

106. Định nghĩa "thành viên tin cậy" được đưa ra để đảm bảo tính đối xứng với các định nghĩa thành viên khác, cùng tham gia vào quá trình hoạt động của các lược đồ chữ ký điện tử theo Luật mẫu (xem đoạn 107). Vì các mục đích của định nghĩa này, "hoạt động" nên được làm sáng tỏ hơn, không chỉ bao trùm lên một hoạt động tích cực, mà còn bao trùm lên các hoạt động bị bỏ sót (xem đoạn 108).

Các tài liệu tham khảo của UNCITRAL

A/CN.9/484, các đoạn 56-57;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 92-105;

A/CN.9/483, các đoạn 59-109;

A/CN.9/WG.IV/WP.84, các đoạn 23-36;

A/CN.9/465, đoạn 42;

A/CN.9/WG.IV/WP.82, các đoạn 22-33;

A/CN.9/457, các đoạn 22-47;66-67;89;109;

A/CN.9/WG.IV/WP.80, các đoạn 7-10;

A/CN.9/WG.IV/WP.79, đoạn 21;

A/CN.9/454, đoạn 20;

A/CN.9/WG.IV/WP.76, các đoạn 16-20;

A/CN.9/446, các đoạn 27-46 (dự thảo mục 1), 62-70 (dự thảo mục 4), 113-131 (dự thảo mục 8), 132-133 (dự thảo mục 9);

A/CN.9/WG.IV/WP.73, các đoạn 16-27, 37-38, 50-57 và 58-60;

A/CN.9/437, các đoạn 29-50 và 90-113 (dự thảo mục A, B và C); và

A/CN.9/WG.IV/WP.71, các đoạn 52-60.

Mục 3: Đối xử bình đẳng đối với các công nghệ chữ ký

Không có điều gì trong Luật này, ngoại trừ mục 5, được áp dụng để loại trừ, giới hạn hoặc lấy đi phương pháp tạo ra chữ ký điện tử mà thoả mãn các yêu cầu được đưa ra trong mục 6 (1), hoặc đáp ứng các yêu cầu của luật có thể áp dụng.

Tính trung lập của công nghệ

107. Mục 3 đưa ra một nguyên tắc cơ bản: không phân biệt đối xử với bất kỳ phương pháp tạo chữ ký điện tử nào, có nghĩa là, tất cả các công nghệ này đều có cơ hội đáp ứng các yêu cầu trong mục 6. Do vậy, các thông báo được ký điện tử và các tài liệu giấy tờ có chữ ký viết tay, hoặc giữa các kiểu thông báo được ký điện tử, được đối xử bình đẳng, miễn là chúng đáp ứng các yêu cầu trong mục 6 (1) Luật mẫu trên, hoặc trong luật có thể áp dụng khác. Ví dụ, các yêu cầu này có thể bắt buộc sử dụng một kỹ thuật chữ ký được thiết kế đặc biệt trong các trường hợp cụ thể nào đó, hoặc có thể thiết lập một chuẩn cao hơn hoặc thấp hơn so với chuẩn đã được đưa ra trong mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL (và mục của Luật mẫu trên). Nguyên tắc cơ bản này được dự định áp dụng chung. Tuy nhiên, cần lưu ý rằng, nguyên tắc này không làm ảnh hưởng tới khả năng tự quyết trong hợp đồng được công nhận trong mục 5. Trong phạm vi luật cho phép, các thành viên nên duy trì khả năng tự quyết trong việc loại trừ các kỹ thuật chữ ký điện tử nào đó, thông qua các thoả thuận. Bằng cách phát biểu "không có điều gì trong Luật này được áp

dụng nhằm loại trừ, giới hạn hoặc lấy đi phương pháp tạo ra chữ ký điện tử", mục 3 chỉ ra rằng, một chữ ký điện tử không được sử dụng chỉ vì lý do hiệu lực pháp lý. Tuy nhiên, mục 3 không nên bị hiểu sai là thiết lập hiệu lực pháp lý của bất kỳ kỹ thuật chữ ký nào, hoặc hiệu lực pháp lý của bất kỳ thông tin được ký điện tử nào.

Các tài liệu tham khảo của UNCITRAL

A/CN.9/WG.IV/WP.88, phụ lục, đoạn 106;

A/CN.9/467, các đoạn 25-32;

A/CN.9/WG.IV/WP.84, đoạn 37;

A/CN.9/465, các đoạn 43-48;

A/CN.9/WG.IV/WP.82, đoạn 34;

A/CN.9/457, các đoạn 53-64.

Mục 4: Làm sáng tỏ

(1) Khi làm sáng tỏ Luật này, mối quan tâm là nguồn gốc Quốc tế của nó, không có sự phân biệt trong việc xúc tiến ứng dụng và tuân theo thiện ý.

(2) Những câu hỏi liên quan đến các vấn đề mà Luật này chi phối (không được giải quyết triệt để trong luật này) sẽ được giải quyết phù hợp với các nguyên tắc chung mà Luật này dựa vào.

Nguồn

108. Mục 4 khởi nguồn từ mục 7 Công ước Liên Hợp Quốc về Bán hàng Quốc tế; đồng thời, mô phỏng theo mục 3 Luật mẫu về Thương mại điện tử của UNCITRAL . Mục này cung cấp hướng dẫn làm sáng tỏ Luật mẫu trên, thông qua toà án, trọng tài và các cơ quan quản trị Quốc gia hoặc địa phương. Hiệu lực mong muốn của mục 4 là hạn chế phạm vi - trong đó, một văn bản thống nhất chỉ được làm sáng tỏ bằng cách tham chiếu vào các khái niệm có trong luật địa phương, một khi nó được đưa vào luật địa phương.

Đoạn (1)

109. Mục đích của đoạn (1) là đưa ra thực tế: các điều khoản của Luật mẫu (hoặc các điều khoản của văn kiện thực thi Luật mẫu) nên được làm sáng tỏ, bằng cách tham chiếu vào nguồn gốc Quốc tế của Luật mẫu khi nó được ban hành như một luật Quốc gia, nhằm đảm bảo tính thống nhất trong việc làm sáng tỏ Luật mẫu tại các nước ban hành.

Đoạn (2)

110. Một số các nguyên tắc chung mà Luật mẫu dựa vào là (1) tạo điều kiện thương mại điện tử trong và giữa các Quốc gia; (2) phê chuẩn các giao dịch được thiết lập thông qua các biện pháp công nghệ thông tin mới; (3) xúc tiến và khuyến khích việc sử dụng các công nghệ thông tin mới nói chung và các chữ ký điện tử nói riêng; (4) xúc tiến việc thống nhất luật; và (5) hỗ trợ hoạt động thương mại. Do mục đích chung của Luật mẫu là tạo điều kiện cho việc sử dụng các chữ ký điện tử, không nên phân tích các sử dụng này bằng bất cứ cách nào.

Các tài liệu tham khảo của UNCITRAL

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 107-109;

A/CN.9/467, các đoạn 33-35;

A/CN.9/WG.IV/WP.84, đoạn 88;

A/CN.9/465, các đoạn 49-50;

A/CN.9/WG.IV/WP.82, đoạn 35;

Mục 5: Thay đổi thông qua thoả thuận

Các điều khoản trong Luật này có thể giảm đi hoặc hiệu lực của chúng có thể được thay đổi thông qua thoả thuận, trừ khi thoả thuận này không hợp lệ, hoặc có hiệu lực theo luật có thể áp dụng.

Tôn trọng luật có thể áp dụng

111. Thực tế, quyết định soạn thảo Luật mẫu dựa vào sự công nhận: giải pháp cho các khó khăn pháp lý (xuất phát từ việc sử dụng các phương tiện truyền thông hiện đại) phần lớn đạt được thông qua các hợp đồng. Do vậy, Luật mẫu ủng hộ nguyên tắc về khả năng tự quyết của thành viên. Tuy nhiên, luật (có thể áp dụng) có thể đưa ra các giới hạn cho việc áp dụng nguyên tắc này. Không nên hiểu là mục 5 cho phép các thành viên có thể giảm bớt các quy tắc bắt buộc, chẳng hạn như các quy tắc được thông qua vì lý do chính sách chung. Nên hiểu là mục 5 khuyến khích các nước thiết lập luật bắt buộc, nhằm giới hạn khả năng tự quyết của thành viên về chữ ký điện tử; hoặc khuyến khích các nước giới hạn khả năng tự quyết của các thành viên, nhằm có được tiếng nói chung giữa các thành viên trong vấn đề thực hiện các yêu cầu quản lý truyền thông.

112. Nguyên tắc về *khả năng tự quyết của các thành viên* được thể hiện trong tất cả các điều khoản của Luật mẫu. Luật mẫu không có bất kỳ điều khoản bắt buộc nào. Nguyên tắc này cũng được áp dụng trong phạm vi của mục 13 (1). Vì vậy, mặc dù toà án hoặc các cơ quan chịu trách nhiệm áp dụng Luật mẫu này tại nước ban hành luật không nên chối bỏ hoặc huỷ bỏ hiệu lực pháp lý của một chứng chỉ nước khác vì lý do nơi phát hành chứng chỉ, mục 13(1) không giới hạn khả năng tự quyết của các thành viên tham gia giao dịch thương mại chấp nhận sử dụng các chứng chỉ có nguồn gốc từ nơi khác (xem A/CN.9/483, đoạn 112).

Các thoả thuận minh bạch hoặc ngầm định

113. Nguyên tắc về khả năng tự quyết của thành viên được thể hiện rõ ràng trong mục 5, trong quá trình soạn thảo Luật mẫu thừa nhận rằng, việc thay đổi thông qua thoả thuận có thể là minh bạch hoặc ngầm định. Mọi diễn đạt trong mục 5 được giữ đúng như mục 6 Công ước Liên Hợp Quốc về Hợp đồng Bán hàng Quốc tế (xem A/CN.9/467, đoạn 38).

Các thoả thuận song phương hoặc đa phương

114. Mục 5 không chỉ được áp dụng trong phạm vi của các quan hệ - giữa người gửi và người nhận thông báo dữ liệu, mà còn được áp dụng trong phạm vi của các quan hệ - giữa những người đóng vai trò trung gian. Vì vậy, các điều khoản trong Luật mẫu có thể thay đổi thông qua các thoả thuận song phương hoặc đa phương - giữa các thành viên, hoặc thông qua các quy tắc mang tính hệ thống được các thành viên chấp nhận. Điển hình, luật (có thể áp dụng) có thể giới hạn khả năng tự quyết của thành viên về quyền và nghĩa vụ, nhằm tránh mọi ngầm định về quyền và nghĩa vụ của các thành viên.

<u>Các tài liệu tham khảo của UNCITRAL</u>

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 110-113;

A/CN.9/467, các đoạn 36-43;

A/CN.9/WG.IV/WP.84, các đoạn 39-40;

A/CN.9/465, các đoạn 51-61;

A/CN.9/WG.IV/WP.82, các đoạn 36-40;

A/CN.9/457, các đoạn 53-64.

Mục 6: Phù hợp với yêu cầu dành cho một chữ ký

1) Khi luật yêu cầu chữ ký của một người, yêu cầu này được thoả mãn, thông qua quan hệ với một thông báo dữ liệu nếu một chữ ký điện tử tin cậy được sử dụng tin cậy, phù hợp với mục đích -trong đó, thông báo dữ liệu được tạo ra và truyền đi, dưới ánh sáng của tất cả các trường hợp, bao gồm mọi thoả thuận liên quan.

2) Đoạn (1) áp dụng khi yêu cầu nằm trong giao ước hoặc luật đưa ra hậu quả của việc thiếu chữ ký.

3) Một chữ ký điện tử được xem là tin cậy cho mục đích thoả mãn yêu cầu được đưa ra trong đoạn (1) nếu:

(a) dữ liệu tạo chữ ký (trong phạm vi nó được sử dụng) được liên kết với người ký, ngoài ra không có người nào khác;

(b) tại thời điểm ký, không người nào khác ngoài người ký kiểm soát dữ liệu tạo chữ ký;

(c) có thể phát hiện được mọi sửa đổi đối với chữ ký điện tử sau thời điểm ký; và

(d) vì mục đích của yêu cầu pháp lý đối với một chữ ký là đảm bảo tính toàn vẹn của thông tin liên quan tới chữ ký, có thể phát hiện được mọi sửa đổi đối với thông tin này sau thời điểm ký.

4) Đoạn (3) không hạn chế khả năng của mọi người:

(a) trong việc thiết lập sự tin cậy của một chữ ký điện tử theo các cách khác, với mục đích đáp ứng yêu cầu được đưa ra trong đoạn (1);

(b) trong việc đưa ra bằng chứng về sự không tin cậy của một chữ ký điện tử.

5) Các điều khoản của mục này không áp dụng cho [...] sau đây.

Tầm quan trọng của mục 6

115. Mục 6 là một trong các điều khoản hạt nhân của Luật mẫu. Mục 6 dựa vào mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL ; đồng thời, cung cấp hướng dẫn thử nghiệm tính tin cậy có thể đáp ứng được trong mục 7(1)(b). Khi làm sáng tỏ mục 6, nên lưu ý mục đích của điều khoản này là đảm bảo rằng, việc sử dụng một chữ ký điện tử tin cậy có cùng hậu quả pháp lý như khi sử dụng một chữ ký viết tay.

Các đoạn (1), (2) và (5)

116. Các đoạn (1), (2) và (5) của mục 6 trình bày các điều khoản được soạn ra từ mục 7(1)(b), (2) và (3) Luật mẫu về Thương mại điện tử của UNCITRAL . Mọi diễn đạt khởi nguồn từ mục 7(1)(a) Luật mẫu về Thương mại điện tử của UNCITRAL có trong định nghĩa về "chữ ký điện tử" trong mục 2(a).

Các khái niệm "định danh" và "nhận dạng"

117. Nhóm làm việc nhất trí rằng, vì mục đích của định nghĩa "chữ ký điện tử" trong Luật mẫu, thuật ngữ "nhận dạng" có thể rộng hơn, không chỉ đơn thuần là nhận dạng người ký thông qua tên. Khái niệm định danh hoặc nhận dạng bao gồm phân biệt người này với người khác thông qua tên hoặc bằng cách khác; và có thể tham khảo các đặc điểm quan trọng, chẳng hạn chức vụ hoặc cơ quan, có thể kết hợp với tên hoặc không. Do vậy, không cần thiết phải phân biệt định danh hoặc các đặc điểm quan trọng khác, không cần giới hạn Luật mẫu vào các trường hợp - trong đó, chỉ có các chứng chỉ sử dụng tên người ký.

Hiệu lực của Luật mẫu thay đổi theo mức tin cậy về mặt kỹ thuật

118. Trong quá trình soạn thảo Luật mẫu, Nhóm làm việc nhấn mạnh rằng (hoặc tham chiếu vào khái niệm "chữ ký điện tử nâng cao", hoặc tiêu chuẩn thiết lập mức tin cậy về mặt kỹ thuật đối với một chữ ký điện tử cho trước), mục đích kép của mục 6 nên thiết lập: các hiệu lực pháp lý là kết quả của việc ứng dụng các kỹ thuật chữ ký điện tử này được công nhận là tin cậy; và (2) ngược lại, không hiệu lực pháp lý nào xuất phát từ việc sử dụng các kỹ thuật có độ tin cậy thấp hơn. Tuy nhiên, có ý kiến cho rằng, cần phân biệt hơn nữa giữa các kỹ thuật chữ ký điện tử khác nhau có thể thực hiện được, trong khi Luật mẫu tránh phân biệt bất kỳ dạng chữ ký điện tử nào, không phức tạp và không an toàn mặc dù nó có thể xuất hiện trong một số trường hợp xác định. Vì vậy, mọi kỹ thuật chữ ký điện tử được sử dụng cho mục đích ký thông báo dữ liệu (theo mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL) có thể đưa ra các hiệu lực pháp lý, đảm bảo rằng nó đủ tin cậy, dưới ánh sáng của mọi trường hợp, bao gồm bất kỳ thoả thuận nào giữa các thành viên. Tuy nhiên, theo mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL, việc xác định những gì tạo thành một phương pháp ký tin cậy, dưới ánh sáng của mọi trường hợp, chỉ có thể do toà án hoặc người xét xử sự kiện can thiệp *ex post* đưa ra, có thể rất lâu sau khi chữ ký được sử dụng. Ngược lại, Luật mẫu trên được mong đợi tạo ra lợi ích từ các kỹ thuật được ủng hộ và được công nhận đặc biệt tin

cậy, không kể các trường hợp chúng được sử dụng. Đây chính là mục đích của đoạn (3), mong muốn có thể tạo ra tính chắc chắn (thông qua một quy tắc giả định hoặc thực chất), ngay tại hoặc trước thời điểm kỹ thuật chữ ký điện tử này được sử dụng (*ex ante*), việc sử dụng một kỹ thuật được công nhận sẽ tạo ra các hiệu lực pháp lý ngang bằng với một chữ ký viết tay. Do vậy, đoạn (3) là một điều khoản thiết yếu nếu Luật mẫu trên tuân thủ mục đích cung cấp thêm tính chắc chắn về hiệu lực pháp lý mà Luật mẫu về Thương mại điện tử của UNCITRAL đưa ra, khi sử dụng các kiểu chữ ký điện tử đặc biệt tin cậy (xem A/CN.9/465, đoạn 64).

Quy tắc giả định hoặc thực chất

119. Để đảm bảo tính chắc chắn về hiệu lực pháp lý của việc sử dụng một chữ ký điện tử như được định nghĩa trong mục 2, đoạn (3) thiết lập chính xác các hiệu lực pháp lý có thể là kết quả của việc kết hợp các đặc tính kỹ thuật nào đó của một chữ ký điện tử (xem A/CN.9/484, đoạn 58). Làm thế nào để thiết lập các hiệu lực pháp lý này, tuỳ thuộc vào luật dân sự và thủ tục thương mại của Quốc gia, các nước ban hành luật nên được tự do trong việc chấp thuận cơ sở giả định, hoặc tiếp tục bằng cách xác nhận trực tiếp liên kết giữa các đặc tính kỹ thuật nào đó và hiệu lực pháp lý của một chữ ký (xem A/CN.9/467, các đoạn 61-62).

Dự định của người ký

120. Câu hỏi đặt ra là hiệu lực pháp lý của việc sử dụng các kỹ thuật chữ ký điện tử có thể được tạo ra, mà không cần ý nghĩa rõ ràng của người ký (người có quyền phê chuẩn các thông tin được ký điện tử) hay không. Trong mọi trường hợp như vậy, chức năng thứ 2 được trình bày trong mục 7(1)(a) Luật mẫu về Thương mại điện tử của UNCITRAL không được thực hiện - khi không "dự định chỉ báo bất kỳ sự phê chuẩn nào đối với thông tin có trong thông báo dữ liệu". Hướng tiếp cận được đưa vào Luật mẫu là các hậu quả pháp lý của việc sử dụng một chữ ký viết tay nên được lặp trong môi trường điện tử. Do vậy, bằng cách gắn chữ ký vào một thông tin nào đó, người ký nên được coi là đã phê chuẩn liên kết giữa định danh của mình với thông tin đó. Liên kết này có nên đưa ra hiệu lực pháp lý (theo hợp đồng hoặc cách khác) theo tính chất của thông tin được ký và trong các trường hợp khác, được đánh giá tuỳ thuộc vào luật có thể áp dụng, ngoài Luật mẫu hay không. Trong phạm vi này, Luật mẫu không dự định can thiệp vào luật về các hợp đồng hoặc nghĩa

vụ
(xem A/CN.9/465, đoạn 65).

Tiêu chuẩn về độ tin cậy kỹ thuật

121. Các đoạn nhỏ từ (a) tới (d) của đoạn (3) nhấn mạnh tiêu chuẩn về độ tin cậy kỹ thuật của các chữ ký điện tử. Đoạn nhỏ (a) tập trung vào các đặc tính chính của dữ liệu tạo chữ ký, nó phải "được liên kết với người ký và không một ai khác". Từ quan điểm kỹ thuật này, dữ liệu tạo chữ ký chỉ có thể liên kết duy nhất với người ký. Liên kết giữa dữ liệu tạo chữ ký và người ký là một yếu tố thiết yếu (xem A/CN.9/467, đoạn 63). Trong trường hợp, dữ liệu tạo chữ ký được chia xẻ cho nhiều cá nhân khác nhau, ví dụ những người làm công cùng sử dụng dữ liệu tạo chữ ký của một công ty, dữ liệu này phải có khả năng nhận dạng rõ ràng từng cá nhân, trong phạm vi của từng chữ ký điện tử.

Một mình người ký kiểm soát dữ liệu tạo chữ ký

122. Đoạn nhỏ (b) giải quyết các trường hợp sử dụng dữ liệu tạo chữ ký. Tại thời điểm dữ liệu tạo chữ ký được sử dụng, không một ai khác, ngoài người ký kiểm soát được nó. Với khái niệm một mình người ký kiểm soát, một câu hỏi đặt ra là người ký có thể cho phép người khác sử dụng dữ liệu tạo chữ ký thay mặt mình hay không. Trường hợp này có thể xảy ra khi dữ liệu tạo chữ ký được sử dụng trong phạm vi một công ty, mỗi thực thể trong đó đều có thể là người ký, nhưng có thể yêu cầu một số người khác ký thay mặt mình (xem A/CN.9/467, đoạn 66). Một ví dụ khác trong các ứng dụng thương mại, dữ liệu tạo chữ ký tồn tại trong một mạng và nhiều người có thể sử dụng nó. Trong trường hợp này, mạng có thể gắn liền với một thực thể xác định là người ký và duy trì được kiểm soát đối với dữ liệu tạo chữ ký. Luật mẫu không bao trùm lên các trường hợp - trong đó, dữ liệu tạo chữ ký có hiệu lực rộng rãi (xem A/CN.9/467, đoạn 67). Khi nhiều người cùng sử dụng một khoá, trong phạm vi của lược đồ "khoá chia xẻ" hoặc "khoá dùng chung", "người ký" được hiểu là "những người này" (xem A/CN.9/483, đoạn 152).

Đại lý

Đoạn 123. Các đoạn nhỏ (a) và (b) đảm bảo rằng dữ liệu tạo chữ ký chỉ được một người sử dụng tại một thời điểm xác định, chủ yếu là thời điểm ký và không một người nào khác được sử dụng nó (xem đoạn 103 ở trên). Câu hỏi về

đại lý và cho phép sử dụng dữ liệu tạo chữ ký được đưa ra trong định nghĩa "người ký" (xem A/CN.9/467, đoạn 68).

Tính toàn vẹn

124. Các đoạn nhỏ (c) và (d) giải quyết các vấn đề về tính toàn vẹn của chữ ký điện tử và thông tin được ký điện tử. Có thể kết hợp 2 điều khoản này để nhấn mạnh: khi chữ ký được gắn vào một tài liệu, tính toàn vẹn của tài liệu và tính toàn vẹn của chữ ký có liên quan chặt chẽ với nhau. Tuy nhiên, khi xem xét Luật mẫu về Thương mại điện tử của UNCITRAL, mặc dù các công nghệ này đảm bảo cả xác thực (mục 7 Luật mẫu về Thương mại điện tử của UNCITRAL) và toàn vẹn (mục 8 Luật mẫu về Thương mại điện tử của UNCITRAL), các khái niệm này có thể được xem là các khái niệm pháp lý khác nhau và được đối xử như các khái niệm pháp lý. Do chữ ký viết tay không đảm bảo tính toàn vẹn đối với tài liệu có gắn chữ ký và cũng không đảm bảo mọi sửa đổi trên tài liệu bị phát hiện, hướng tiếp cận chức năng ngang bằng yêu cầu: không nên giải quyết các khái niệm này trong một điều khoản đơn lẻ. Mục đích của đoạn (3) (c) là thiết lập tiêu chuẩn cần phải thoả mãn, nhằm chứng minh một phương pháp chữ ký điện tử đủ tin cậy để đáp ứng một yêu cầu luật về chữ ký. Yêu cầu này có thể được đáp ứng mà không cần chứng minh tính toàn vẹn của toàn bộ tài liệu (xem A/CN.9/467, các đoạn 72-80).

125. Ban đầu, đoạn nhỏ (d) được dự định áp dụng cho một số nước (hiện ban hành các quy tắc pháp lý về quản lý sử dụng chữ ký viết tay) không thể phân biệt giữa tính toàn vẹn của chữ ký và tính toàn vẹn của thông tin được ký. Tại một số nước khác, đoạn nhỏ (d) có thể tạo ra một chữ ký tin cậy hơn chữ ký viết tay và vượt xa khái niệm ngang bằng về mặt chức năng với một chữ ký. Trong một số phạm vi quyền hạn, hiệu lực của đoạn nhỏ (d) có thể tạo ra sự ngang bằng về mặt chức năng với một tài liệu gốc (xem A/CN.9/484, đoạn 62).

Chữ ký điện tử là một phần của thông báo

126. Trong đoạn nhỏ (d), liên kết cần thiết giữa chữ ký và thông tin được ký được đưa ra để tránh sự ngầm định: chữ ký điện tử được áp dụng cho tất cả các nội dung của một thông báo dữ liệu. Trong nhiều ví dụ thực tế, thông tin được ký chỉ là một phần trong thông báo dữ liệu. Ví dụ, một chữ ký điện tử chỉ liên quan tới thông tin được gắn vào thông báo vì các mục đích truyền dữ liệu.

Thay đổi thông qua thoả thuận

127. Đoạn (3) không dự định giới hạn việc áp dụng mục 5 và mọi luật có thể áp dụng công nhận khả năng tự quyết của các thành viên, nhằm quy định (trong bất kỳ thoả thuận liên quan nào) rằng, mọi kỹ thuật chữ ký đều được đối xử bình đẳng và có sự tin cậy ngang bằng với một chữ ký viết tay.

128. Đoạn (4)(a) cung cấp cơ sở pháp lý cho hoạt động thương mại - trong đó, các đối tác thương mại có thể quy định các mối quan hệ về sử dụng chữ ký điện tử, thông qua hợp đồng (xem A/CN.9/484, đoạn 63).

Có thể đưa ra bằng chứng về sự không tin cậy của một chữ ký điện tử

129. Đoạn (4)(b) có thể làm rõ ý: Luật mẫu không giới hạn bất kỳ khả năng nào có thể có trong việc bác bỏ các giả định được đưa ra trong đoạn (3) (xem A/CN.9/484, đoạn 63).

Các loại trừ khỏi phạm vi của mục 6

130. Nguyên tắc được đưa ra trong đoạn (5) là nước ban hành luật có thể loại trừ một số trường hợp (được xác định trong bản ban hành Luật mẫu) ra khỏi phạm vi áp dụng của mục 6. Nước ban hành luật có thể loại trừ các kiểu trường hợp, tuỳ thuộc vào mục đích - trong đó chính thức yêu cầu thiết lập một chữ ký viết tay.

131. Đoạn (5) được đưa ra với hy vọng nâng cao khả năng chấp nhận Luật mẫu. Nó công nhận rằng, việc xác định các loại trừ nên do nước ban hành luật tiến hành, vì mỗi nước quan tâm tới các trường hợp khác nhau. Tuy nhiên, cần lưu ý rằng, các mục tiêu của Luật mẫu sẽ không thể đạt được nếu đoạn (5) được sử dụng để thiết lập các loại trừ chung; và cơ hội mà đoạn (5) đưa ra nên bị ngăn chặn. Nhiều loại trừ có thể gây ra các cản trở không cần thiết cho việc phát triển các chữ ký điện tử, vì trong Luật mẫu có rất nhiều nguyên tắc cơ bản và các hướng tiếp cận được mong đợi áp dụng chung (xem A/CN.9/484, đoạn 63).

<u>Các tài liệu tham khảo của UNCITRAL</u>

A/CN.9/484, các đoạn 58-63;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 114-126;

A/CN.9/467, các đoạn 44-87;

A/CN.9/WG.IV/WP.84, các đoạn 41-47;

A/CN.9/465, các đoạn 62-82;

A/CN.9/WG.IV/WP.82, các đoạn 42-44;

A/CN.9/457, các đoạn 48-52;

A/CN.9/WG.IV/WP.80, các đoạn 11-12;

Mục 7: Thoả mãn mục 6

(1) *[Mọi người, cơ quan, hoặc công cộng hoặc cá nhân, được xác định trong phạm vi nước ban hành luật]* có thể quyết định những loại chữ ký điện tử nào thoả mãn các điều khoản trong mục 6.

(2) Mọi quyết định được đưa ra trong đoạn (1) nên phù hợp với các chuẩn Quốc tế được công nhận.

(3) Không có điều gì trong mục này ảnh hưởng đến việc sử dụng các quy tắc trong tư pháp Quốc tế.

Xác định trước tình trạng của chữ ký điện tử

132. Mục 7 trình bày vai trò của nước ban hành luật trong việc thiết lập, hoặc công nhận thực thể có thể phê chuẩn việc sử dụng các chữ ký điện tử, hoặc chứng nhận chất lượng của chúng. Giống như mục 6, mục 7 dựa vào quan niệm những gì được yêu cầu để tạo điều kiện phát triển thương mại điện tử là chắc chắn và có thể khẳng định trước, tại thời điểm khi các đối tác thương mại sử dụng các kỹ thuật chữ ký điện tử, không phải tại thời điểm tranh cãi trước toà. *Khi một kỹ thuật chữ ký có thể đáp ứng các yêu cầu về an toàn và tin cậy ở mức độ cao, nên có một phương tiện để đánh giá các khía cạnh kỹ thuật của sự tin cậy và an toàn; đồng thời tuỳ thuộc vào dạng kỹ thuật chữ ký được công nhận.*

Mục đích của mục 7

133. Mục đích của mục 7 là làm sáng tỏ: Nước ban hành luật có thể thiết kế một tổ chức, hoặc cơ quan có quyền quyết định những công nghệ nào có thể có lợi từ quy tắc được thiết lập trong mục 6. Mục 7 không phải là một điều khoản thiết lập tất yếu mà nước ban hành luật có thể hoặc sẽ ban hành. Tuy nhiên, nó truyền đạt một thông báo rõ ràng: tính chắc chắn và khẳng định trước có thể đạt được, bằng cách xác định kỹ thuật chữ ký điện tử thoả mãn tiêu chuẩn tin cậy trong mục 6, miễn sao các quyết định này được đưa ra phù hợp với các chuẩn Quốc tế. Không nên làm sáng tỏ mục 7 là quy định các hiệu lực pháp lý bắt buộc trong sử dụng các kiểu kỹ thuật chữ ký nào đó, hoặc giới hạn sử dụng công nghệ cho các kỹ thuật này để đáp ứng các yêu cầu về độ tin cậy trong mục 6. Ví dụ, các thành viên được tự do sử dụng các kỹ thuật không thoả mãn mục 6, nếu đó là những gì mà họ chấp thuận thực hiện. Họ cũng được tự do trình bày, trước toà hoặc trọng tài phân xử, phương pháp chữ ký mà họ chọn để sử dụng và nó thoả mãn các yêu cầu của mục 6.

Đoạn (1)

134. Đoạn (1) trình bày rõ: thực thể có thể phê chuẩn việc sử dụng các chữ ký điện tử, hoặc chứng nhận chất lượng của chúng, không nhất thiết phải là một cơ quan nhà nước. Không nên xem đoạn (1) là một khuyến nghị về *phương tiện duy nhất đạt được sự công nhận đối với các công nghệ chữ ký* dành cho các nước, đúng hơn là một chỉ báo về các giới hạn nên áp dụng nếu các nước mong muốn thông qua hướng tiếp cận này.

Đoạn (2)

135. Với đoạn (2), khái niệm "chuẩn" không nên bị giới hạn trong các chuẩn do các tổ chức như Tổ chức Tiêu chuẩn hoá Quốc tế (ISO) và Tổ công tác kỹ thuật Internet (IETF) phát triển, hoặc các chuẩn kỹ thuật khác. Từ "các chuẩn" nên được làm sáng tỏ với nghĩa rộng hơn, nó có thể bao gồm các hoạt động công nghiệp và sử dụng thương mại, các văn bản của các tổ chức Quốc tế như Phòng Thương mại Quốc tế, các thực thể tín dụng địa phương hoạt động dưới sự bảo hộ của ISO (xem A/CN.9/484, đoạn 66), Tập đoàn mạng thế giới (W3C) và UNCITRAL (bao gồm Luật mẫu về Thương mại điện tử và Luật mẫu về Chữ ký điện tử của UNCITRAL). Không nên để tình trạng thiếu vắng các chuẩn liên quan cản trở các cá nhân, hoặc cơ quan có thẩm quyền đưa ra các quyết định được đưa ra trong đoạn (1). Với các chuẩn "được công nhận", câu hỏi được đặt ra là "sự công nhận" được hình thành từ những gì và ai đòi hỏi sự công nhận này (xem A/CN.9/465, đoạn 94). Câu hỏi này được thảo luận trong mục 12 (xem đoạn 159 dưới đây).

Đoạn (3)

136. Đoạn (3) giải thích rõ ràng hơn mục đích của mục 7 là không can thiệp vào việc sử dụng các quy tắc trong tư pháp Quốc tế (xem A/CN.9/467, đoạn 94). Nếu thiếu điều khoản này, mục 7 có thể được làm sáng tỏ là khuyến khích các nước ban hành luật đối xử phân biệt với các chữ ký điện tử của nước khác, trên cơ sở không tuân theo các quy tắc được cá nhân và cơ quan liên quan thiết lập trong đoạn (1).

<u>Các tài liệu tham khảo của UNCITRAL</u>

A/CN.9/484, các đoạn 64-66;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 127-131;

A/CN.9/467, các đoạn 90-95;

A/CN.9/WG.IV/WP.84, các đoạn 49-51;

A/CN.9/465, các đoạn 90-98;

A/CN.9/WG.IV/WP.82, đoạn 46;

A/CN.9/457, các đoạn 48-52;

A/CN.9/WG.IV/WP.80, đoạn 15.

Mục 8: Hướng dẫn người ký

(1) Khi dữ liệu tạo chữ ký được sử dụng để tạo ra một chữ ký có hiệu lực pháp lý, người ký nên:

(a) Quan tâm một cách hợp lý nhằm tránh việc sử dụng trái phép dữ liệu tạo chữ ký.

(b) Không được chậm trễ, thông báo ngay cho đối tượng tin cậy vào người ký hoặc cung cấp dịch vụ hỗ trợ chữ ký điện tử khi:

(i) Người ký biết dữ liệu tạo chữ ký bị lộ; hoặc

(ii) Người ký được biết đã gây ra rủi ro đáng kể do dữ liệu tạo chữ ký bị lộ;

(c) Khi chứng chỉ được sử dụng để hỗ trợ chữ ký điện tử, người ký cần quan tâm hợp lý để đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn cần thiết do người ký đưa ra, liên quan tới chứng chỉ trong suốt thời gian tồn tại của nó, hoặc các biểu diễn nằm trong chứng chỉ.

(2) Người ký cần phải chịu trách nhiệm pháp lý do không thực hiện các yêu cầu trong đoạn (1).

Tiêu đề

137. Ban đầu, mục 8 (và các mục 9, 11) dự định bao gồm các quy tắc về nghĩa vụ và trách nhiệm pháp lý của các thành viên khác nhau (người ký, thành viên tin cậy và nhà cung cấp dịch vụ chứng thực). Tuy nhiên, do sự thay đổi nhanh chóng làm ảnh hưởng đến các khía cạnh kỹ thuật và thương mại của thương mại điện tử, đồng thời, do vai trò tự điều chỉnh trong lĩnh vực thương mại điện tử tại nhiều nước, việc nhất trí về nội dung của các quy tắc này gặp khó khăn. Các mục này được soạn thảo, bao gồm tối thiểu một "quy tắc hướng dẫn" đối với các thành viên. Chẳng hạn, trong mục 9 Hướng dẫn nhà cung cấp dịch vụ chứng thực (xem đoạn 144 dưới đây). Luật mẫu ủng hộ giải pháp liên

kết các nghĩa vụ (được thiết lập trong mục 8 và 9) với việc tạo ra các chữ ký điện tử hợp pháp (xem A/CN.9/483, đoạn 117). Nguyên tắc người ký phải chịu trách nhiệm pháp lý vì không thực hiện các yêu cầu trong đoạn (1) được thiết lập trong đoạn (2); ngoài ra, người ký phải chịu trách nhiệm pháp lý do không tôn trọng quy tắc hướng dẫn trong các luật có thể áp dụng, ngoài Luật mẫu (xem đoạn 141 dưới đây).

Đoạn (1)

138. Các đoạn nhỏ (a) và (b) được áp dụng chung cho tất cả các chữ ký điện tử, đoạn nhỏ (c) chỉ được áp dụng cho các chữ ký điện tử có chứng chỉ hỗ trợ. Nói riêng, nghĩa vụ trong đoạn (1)(a) là một nghĩa vụ cơ bản, nó thường có trong các thoả thuận về sử dụng thẻ tín dụng. Theo chính sách được phê chuẩn trong đoạn (1), nghĩa vụ này cũng nên được áp dụng cho bất kỳ dữ liệu tạo chữ ký nào. Tuy nhiên, điều khoản *thay đổi thông qua thoả thuận* trong mục 5 cho phép thay đổi các chuẩn (được thiết lập trong mục 8) trong các lĩnh vực có thể bị coi là không phù hợp, hoặc gây ra các hậu quả khó lường.

139. Đoạn (1)(b) đưa ra khái niệm "người tin cậy vào người ký hoặc cung cấp dịch vụ hỗ trợ chữ ký điện tử". Tuỳ thuộc vào công nghệ được sử dụng, "thành viên tin cậy" không chỉ là người tìm kiếm sự tin cậy vào chữ ký, mà còn là nhà cung cấp dịch vụ chứng thực, nhà cung cấp dịch vụ thông báo tình trạng thu hồi chứng chỉ và mọi thành viên liên quan khác.

140. Đoạn (1)(c) áp dụng khi chứng chỉ được sử dụng để hỗ trợ dữ liệu tạo chữ ký. "Thời hạn tồn tại" của chứng chỉ được làm sáng tỏ rộng hơn, bao trùm lên khoảng thời gian bắt đầu xin cấp chứng chỉ, hoặc tạo chứng chỉ với khoảng thời gian hết hạn hoặc huỷ bỏ chứng chỉ.

Đoạn (2)

141. Đoạn (2) không xác định các hậu quả, hoặc các giới hạn trách nhiệm pháp lý, hoặc cả hai trong luật Quốc gia. Tuy nhiên, đoạn (2) xác định rõ, các nước ban hành luật phải chịu trách nhiệm pháp lý nếu không tuân theo các yêu cầu nghĩa vụ trong đoạn (1). Đoạn (2) dựa vào các kết luận do Nhóm làm việc đưa ra trong phiên họp thứ 35, chúng ta có thể gặp khó khăn khi tìm kiếm sự nhất trí về các hậu quả phát sinh từ việc người ký vi phạm trách nhiệm pháp lý. Đoạn (2) chỉ thiết lập nguyên tắc: người ký nên chịu trách nhiệm pháp lý do không thực hiện các yêu cầu trong đoạn (1) và trong luật có thể áp dụng khác.

Luật mẫu tại mỗi nước ban hành luật giải quyết các hậu quả pháp lý này (xem A/CN.9/465, đoạn 108).

Các tài liệu tham khảo của UNCITRAL

A/CN.9/484, các đoạn 67-69;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 132-136;

A/CN.9/467, các đoạn 96-104;

A/CN.9/WG.IV/WP.84, các đoạn 52-53;

A/CN.9/465, các đoạn 99-108;

A/CN.9/WG.IV/WP.82, các đoạn 50-55;

A/CN.9/457, các đoạn 65-98;

A/CN.9/WG.IV/WP.80, các đoạn 18-19.

Mục 9: Hướng dẫn nhà cung cấp dịch vụ chứng thực

(1) Khi nhà cung cấp dịch vụ chứng thực cung cấp các dịch vụ nhằm hỗ trợ một chữ ký điện tử, muốn chữ ký này có hiệu lực hợp pháp như là một chữ ký, nhà cung cấp dịch vụ chứng thực nên:

(a) Hoạt động phù hợp với các biểu diễn về chính sách và hoạt động do chính nhà cung cấp đưa ra;

(b) Quan tâm hợp lý nhằm đảm bảo tính chính xác và đầy đủ của tất cả các biểu diễn cần thiết do nhà cung cấp đưa ra, liên quan tới chứng chỉ trong suốt thời gian tồn tại của nó, hoặc các biểu diễn nằm trong chứng chỉ.

(c) Cung cấp các phương tiện có khả năng truy nhập được, cho phép thành viên tin cậy có thể xác định từ chứng chỉ:

(i) Nhận dạng của nhà cung cấp dịch vụ chứng thực;

(ii) Người ký (được nhận dạng trong chứng chỉ) kiểm soát được dữ liệu tạo chữ ký tại thời điểm chứng chỉ được phát hành;

(iii) Dữ liệu tạo chữ ký hợp lệ tại thời điểm hoặc trước thời điểm chứng chỉ được phát hành;

(d) Cung cấp các phương tiện có khả năng truy nhập được, cho phép thành viên tin cậy xác định từ chứng chỉ, hoặc bằng cách khác:

(i) Phương pháp được sử dụng để nhận dạng người ký;

(ii) Mọi giới hạn về mục đích hoặc giá trị đối với dữ liệu tạo chữ ký hoặc chứng chỉ có thể được sử dụng;

(iii) Dữ liệu tạo chữ ký hợp lệ và không bị lộ;

(iv) Mọi giới hạn về phạm vi hoặc mức trách nhiệm pháp lý mà nhà cung cấp dịch vụ chứng thực đặt ra;

(v) Phương tiện mà người ký sử dụng để đưa ra thông báo theo đúng mục 8 (1) (b);

(vi) Dịch vụ thu hồi được đưa ra đúng lúc;

(e) Đưa ra các dịch vụ theo (d) (v), cung cấp cho người ký phương tiện thông báo theo đúng mục 8 (1) (b) và đưa ra các dịch vụ theo (d) (vi), đảm bảo tính sẵn sàng của dịch vụ thu hồi đúng lúc;

(f) Sử dụng các nguồn tài nguyên hệ thống, thủ tục và con người tin cậy khi thực hiện các dịch vụ.

(2) Nhà cung cấp dịch vụ chứng thực cần phải chịu trách nhiệm pháp lý do không thực hiện các yêu cầu trong đoạn (1).

Đoạn (1)

142. Đoạn nhỏ (a) nhấn mạnh quy tắc cơ bản sau: nhà cung cấp dịch vụ chứng thực nên tôn trọng các biểu diễn và các cam kết do chính nhà cung cấp đưa ra, ví dụ, trong quy định hoạt động chứng thực (CPS) hoặc trong các kiểu công bố chính sách khác.

143. Đoạn nhỏ (c) định nghĩa các nội dung thiết yếu và hiệu lực của bất kỳ chứng chỉ nào theo Luật mẫu. Lưu ý, trong trường hợp của các chữ ký số, cần phải xác định liên kết giữa người ký với khoá công khai, cũng như khoá riêng (xem A/CN.9/484, đoạn 71). Đoạn nhỏ (d) liệt kê các yếu tố bổ sung có trong một chứng chỉ, hoặc các yếu tố có hiệu lực với thành viên tin cậy hoặc thành viên tin cậy có thể truy nhập vào. Đoạn nhỏ (e) không dự định áp dụng cho các chứng chỉ giao dịch chỉ sử dụng 1 lần, hoặc các chứng chỉ chi phí thấp dành cho các ứng dụng rủi ro thấp, hoặc cả hai.

144. Nhà cung cấp dịch vụ chứng thực và người phát hành các chứng chỉ "giá trị cao" được mong đợi thực hiện các trách nhiệm và nghĩa vụ được đưa ra trong mục 9. Tuy nhiên, Luật mẫu không đòi hỏi ở người ký, hoặc nhà cung cấp dịch vụ chứng thực mức độ siêng năng hoặc tin cậy do không có mối quan hệ hợp lý với các mục đích trong đó chữ ký điện tử hoặc chứng chỉ được sử

dụng (xem đoạn 137 ở trên). Luật mẫu ủng hộ giải pháp liên kết các nghĩa vụ (được thiết lập trong mục 8 và 9) với việc tạo ra các chữ ký điện tử hợp pháp (xem A/CN.9/483, đoạn 117). Bằng cách giới hạn phạm vi của mục 9 vào các trường hợp - trong đó, các dịch vụ chứng thực được cung cấp để hỗ trợ một chữ ký điện tử có hiệu lực pháp lý, Luật mẫu không dự định tạo ra các kiểu hiệu lực pháp lý mới cho các chữ ký (xem đoạn 119).

Đoạn (2)

145. Đoạn (2) để cho luật Quốc gia xác định các hậu quả của trách nhiệm pháp lý (xem A/CN.9/484, đoạn 73). Tuỳ thuộc vào các quy tắc có thể áp dụng trong luật Quốc gia, không nên làm sáng tỏ đoạn (2) như một quy tắc trách nhiệm pháp lý tuyệt đối. Đoạn (2) có thể loại trừ các khả năng - trong đó, nhà cung cấp dịch vụ chứng thực chứng minh mình không có lỗi hoặc bất cẩn.

146. Các dự thảo mục 9 gần đây có thêm 1 đoạn, đoạn này đưa ra các hậu quả của trách nhiệm pháp lý được thiết lập trong đoạn (2). Trong quá trình soạn thảo Luật mẫu, người ta nhận thấy rằng, câu hỏi về trách nhiệm pháp lý của nhà cung cấp dịch vụ chứng thực không được đưa ra một cách đầy đủ, nếu chỉ phê chuẩn 1 điều khoản đơn lẻ cùng với đoạn (2). Đoạn (2) có thể phát biểu một nguyên tắc thích hợp áp dụng cho người ký, nhưng nó không đủ để giải quyết các hoạt động thương mại và chuyên nghiệp mà mục 9 bao trùm. Một cách để bù đắp sự thiếu vắng này là liệt kê (trong văn bản Luật mẫu) các yếu tố cần phải quan tâm khi đánh giá sự tổn thất do nhà cung cấp dịch vụ chứng thực gây ra. Quyết định cuối cùng là đưa vào bản hướng dẫn này một danh sách không hạn chế các yếu tố chỉ báo. Khi đánh giá trách nhiệm pháp lý của nhà cung cấp dịch vụ chứng thực, cần quan tâm đến các yếu tố sau, không kể những cái khác: (a) chi phí để có được chứng chỉ; (b) tính chất của thông tin được chứng thực; (c) sự tồn tại và phạm vi của mọi giới hạn về mục đích sử dụng chứng chỉ; (d) sự tồn tại của mọi công bố về giới hạn phạm vi hoặc chừng mực trách nhiệm pháp lý của nhà cung cấp dịch vụ chứng thực; và (e) mọi hướng dẫn cộng tác của thành viên tin cậy. Trong quá trình soạn thảo Luật mẫu, người ta cũng nhất trí rằng, khi nước ban hành luật xác định các mất mát có thể khôi phục được, gánh nặng được đặt vào các quy tắc quản lý giới hạn trách nhiệm pháp lý tại nước có thiết lập nhà cung cấp dịch vụ chứng thực, hoặc tại nước khác có áp dụng luật theo các quy tắc xung đột luật pháp liên quan (xem A/CN.9/484, đoạn 74).

Các tài liệu tham khảo của UNCITRAL

A/CN.9/484, các đoạn 70-74;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 137-141;

A/CN.9/483, các đoạn 114-127;

A/CN.9/467, các đoạn 105-129;

A/CN.9/WG.IV/WP.84, các đoạn 54-60;

A/CN.9/465, các đoạn 123-142 (dự thảo mục 12);

A/CN.9/WG.IV/WP.82, các đoạn 59-68 (dự thảo mục 12);

A/CN.9/457, các đoạn 108-119;

A/CN.9/WG.IV/WP.80, các đoạn 22-24.

Mục10: Sự tin cậy

Phù hợp với các mục đích của mục 9 (1) (f), khi xác định các nguồn tài nguyên hệ thống, thủ tục và con người mà nhà cung cấp dịch vụ chứng thực sử dụng có tin cậy hay không, nên quan tâm đến các yếu tố sau đây:

(a) Các nguồn tài chính và con người, bao gồm cả các tài sản;

(b) Chất lượng của các hệ thống phần mềm và phần cứng;

(c) Các thủ tục xử lý chứng chỉ và các ứng dụng dành cho chứng chỉ, duy trì các bản ghi;

(d) Tính sẵn sàng của các thông tin dành cho người ký (được nhận dạng trong chứng chỉ) và các thành viên tin cậy;

(e) Kiểm toán định kỳ hoặc mở rộng do một thực thể độc lập tiến hành;

(f) Sự công bố của một nước, thực thể được uỷ nhiệm hoặc nhà cung cấp dịch vụ chứng thực về việc tuân thủ hoặc sự tồn tại của những gì đã đề cập ở trên; hoặc

(g) Bất kỳ yếu tố liên quan khác.

Tính mềm dẻo của khái niệm "sự tin cậy"

147. Ban đầu, mục 10 được soạn thảo là một phần của mục 9. Sau đó, nó được soạn thảo thành một mục riêng nhưng chủ yếu trợ giúp làm sáng tỏ khái niệm "các hệ thống, thủ tục và nguồn tài nguyên con người tin cậy" trong mục 9(1)(f). Mục 10 đưa ra một danh sách không hạn chế các yếu tố cần quan tâm khi xác định sự tin cậy. Danh sách này dự định cung cấp khái niệm mềm dẻo

về *sự tin cậy*, nó có thể thay đổi nội dung tuỳ thuộc vào những gì người ta mong đợi ở chứng chỉ trong phạm vi chứng chỉ này được tạo ra.

Các tài liệu tham khảo của UNCITRAL

A/CN.9/WG.IV/WP.88, phụ lục, đoạn 142;

A/CN.9/483, các đoạn 128-133;

A/CN.9/467, các đoạn 114-119.

Mục 11: Hướng dẫn thành viên tin cậy

Thành viên tin cậy phải gánh chịu hậu quả pháp lý do không:

(a) Tiến hành các bước hợp lý để kiểm tra sự tin cậy của một chữ ký điện tử, hoặc:

(b) Khi chữ ký điện tử được hỗ trợ thông qua một chứng chỉ,

(i) Kiểm tra khoảng thời gian tồn tại hợp lệ, tình trạng treo hoặc huỷ bỏ của chứng chỉ; và

(ii) Tuân theo mọi giới hạn về chứng chỉ.

Sự tin cậy hợp lý

148. Mục 11 phản ánh ý tưởng, một thành viên (người dự định tin cậy một chữ ký điện tử) nên đặt câu hỏi: sự tin cậy này là hợp lý trong trường hợp nào và ở chừng mực nào, dưới ánh sáng của tất cả các trường hợp. Nó không dự định giải quyết vấn đề về tính hợp lệ của một chữ ký điện tử. Vấn đề này được đưa ra trong mục 6 và không nên phụ thuộc vào hướng dẫn thành viên tin cậy. Vấn đề về tính hợp lệ của một chữ ký điện tử nên được tách riêng, khác với vấn đề xác định thành viên tin cậy có tin cậy hợp lý vào một chữ ký không thoả mãn tiêu chuẩn được thiết lập trong mục 6 hay không.

Vấn đề khách hàng

149. Khi mục 11 có thể đặt gánh nặng vào các thành viên tin cậy, đặc biệt trong trường hợp thành viên này là các khách hàng, nên nhớ rằng, Luật mẫu không có dự định gạt bỏ bất kỳ quy tắc bảo vệ khách hàng nào. Tuy nhiên, Luật mẫu có thể đóng một vai trò hữu ích trong việc giáo dục tất cả các thành viên, trong đó có thành viên tin cậy, về chuẩn hướng dẫn hợp lý cần tuân theo đối với các chữ ký điện tử. Thêm vào đó, việc thiết lập một chuẩn hướng dẫn, trong đó thành viên tin cậy nên kiểm tra sự tin cậy của chữ ký thông qua các

phương tiện có thể truy nhập dễ dàng, có thể được xem là yêu cầu thiết yếu khi phát triển bất kỳ hệ thống cơ sở hạ tầng khoá công khai nào.

Khái niệm "thành viên tin cậy"

150. Phù hợp với định nghĩa này, khái niệm "thành viên tin cậy" dự định bao trùm lên bất kỳ thành viên nào có thể tin cậy một chữ ký điện tử. Do vậy, tuỳ thuộc vào các trường hợp, một "thành viên tin cậy" có thể là một người có hoặc không có quan hệ hợp đồng với người ký; hoặc nhà cung cấp dịch vụ chứng thực. Cần nhận thức rằng, nhà cung cấp dịch vụ chứng thực hoặc người ký có thể tự trở thành "thành viên tin cậy". Tuy nhiên, khái niệm rộng hơn về "thành viên tin cậy" không nên có nghĩa vụ kiểm tra sự hợp lệ của chứng chỉ mua được từ nhà cung cấp dịch vụ chứng thực.

Không tuân theo các yêu cầu của mục 11

151. Về ảnh hưởng của việc thiết lập nghĩa vụ chung, cụ thể là thành viên tin cậy nên kiểm tra hiệu lực pháp lý của chữ ký điện tử hoặc chứng chỉ, một câu hỏi được đặt ra là thành viên tin cậy không tuân theo các yêu cầu của mục 11 thì làm thế nào. Nếu thành viên tin cậy không tuân theo các yêu cầu của mục 11, không nên loại trừ thành viên tin cậy ra khỏi việc sử dụng chữ ký hoặc chứng chỉ nếu việc kiểm tra hợp lý không thể phát hiện ra chữ ký hoặc chứng chỉ không hợp lệ. Các yêu cầu trong mục 11 không dự định yêu cầu tuân theo các giới hạn hoặc kiểm tra thông tin mà thành viên tin cậy không thể truy nhập một cách dễ dàng. Có thể giải quyết trường hợp này thông qua luật có thể áp dụng, ngoài Luật mẫu. Hơn nữa, hậu quả của việc thành viên tin cậy không tuân theo các yêu cầu của mục 11 do luật có thể áp dụng, ngoài Luật mẫu quản lý (xem A/CN.9/484, đoạn 75).

<u>Các tài liệu tham khảo của UNCITRAL</u>

A/CN.9/484, đoạn 75;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 143-146;

A/CN.9/467, các đoạn 130-143;

A/CN.9/WG.IV/WP.84, các đoạn 61-63;

A/CN.9/465, các đoạn 109-122 (dự thảo mục 10 và 11);

A/CN.9/WG.IV/WP.82, các đoạn 56-58 (dự thảo mục 10 và 11);

A/CN.9/457, các đoạn 99-107;

A/CN.9/WG.IV/WP.80, các đoạn 20-21.

Mục 12: Công nhận chứng chỉ và chữ ký điện tử của các nước khác

(1) Khi xác định một chứng chỉ hoặc một chữ ký điện tử có hiệu lực pháp lý hay không, không cần phải quan tâm tới:

(a) Vị trí địa lý - nơi chứng chỉ được phát hành; hoặc nơi chữ ký điện tử được tạo ra và sử dụng; hoặc

(b) Vị trí địa lý - nơi kinh doanh của người phát hành hoặc người ký.

(2) Một chứng chỉ được phát hành bên ngoài [*Nước ban hành luật*] nên có cùng hiệu lực pháp lý như một chứng chỉ được phát hành trong [*Nước ban hành luật*] nếu nó đảm bảo mức tin cậy ngang bằng.

(3) Một chữ ký điện tử được tạo ra hoặc sử dụng bên ngoài [*Nước ban hành luật*] nên có cùng hiệu lực pháp lý như một chữ ký điện tử được tạo ra và sử dụng trong [*Nước ban hành luật*] nếu nó đảm bảo mức tin cậy ngang bằng.

(4) Khi xác định một chứng chỉ hoặc một chữ ký điện tử có đưa ra một mức tin cậy ngang bằng hay không, theo đoạn (2) và (3), vấn đề cần được quan tâm là các chuẩn Quốc tế được công nhận và các yếu tố liên quan khác.

(5) Trong đoạn (2), (3) và (4), tuy các thành viên tự thoả thuận với nhau trong việc sử dụng một số kiểu chữ ký điện tử hoặc chứng chỉ nào đó, thoả thuận này nên được công nhận, phù hợp với các mục đích công nhận qua biên giới, trừ khi thoả thuận này không hợp lệ hoặc không có hiệu lực đối với luật có thể áp dụng.

Quy tắc chung về sự không phân biệt

152. Đoạn (1) được dự định phản ánh nguyên tắc cơ bản: nguồn gốc xuất xứ không nên là yếu tố xác định các chứng chỉ hoặc chữ ký điện tử của nước khác có được công nhận về hiệu lực pháp lý hay không và chừng mực công nhận như thế nào. Việc xác định một chữ ký điện tử hoặc chứng chỉ có hiệu lực pháp lý hay không và chừng mực công nhận ra sao không nên phụ thuộc vào vị trí - nơi chứng chỉ hoặc chữ ký điện tử được phát hành (xem A/CN.9/483, đoạn 27) mà phụ thuộc vào tính tin cậy kỹ thuật.

"Mức tin cậy ngang bằng "

153. Mục đích của đoạn (2) là cung cấp tiêu chuẩn chung về công nhận qua biên giới đối với các chứng chỉ, sao cho nhà cung cấp dịch vụ chứng thực không phải chịu gánh nặng vô lý để có được các giấy phép phạm vi quyền hạn. Vì mục đích này, đoạn (2) thiết lập một *ngưỡng* đánh giá sự ngang bằng về mặt kỹ thuật đối với các chứng chỉ nước ngoài, bằng cách kiểm tra tính tin cậy của chúng, dựa vào các yêu cầu về sự tin cậy do nước ban hành luật thiết lập, chiểu theo Luật mẫu (đoạn 31). Tiêu chuẩn này là áp dụng trong phạm vi quyền hạn, không cần quan tâm tới tính chất của lược đồ chứng thực mà từ đó thu được chứng chỉ hoặc chữ ký (đoạn 29).

Mức tin cậy thay đổi theo phạm vi quyền hạn

154. Bằng cách tham chiếu vào khái niệm "mức tin cậy ngang bằng", đoạn (2) thừa nhận rằng, ở đây có sự khác nhau giữa các yêu cầu về phạm vi quyền hạn cá nhân. Yêu cầu ngang bằng, như đã được sử dụng trong đoạn (2), không có nghĩa là mức tin cậy của một chứng chỉ nước ngoài nên đồng nhất chính xác với mức tin cậy dành cho một chứng chỉ trong nước (xem đoạn 32).

Mức tin cậy thay đổi trong một phạm vi quyền hạn

155. Thêm vào đó, nên lưu ý rằng, trong thực tế, nhà cung cấp dịch vụ chứng thực phát hành các chứng chỉ với các mức tin cậy khác nhau, tuỳ thuộc vào các mục đích - trong đó, chứng chỉ được các khách hàng dự định sử dụng. Tuỳ thuộc vào mức tin cậy riêng của từng chứng chỉ, các chứng chỉ và chữ ký điện tử có thể đưa ra các hiệu lực pháp lý khác nhau, cả trong nước và nước ngoài. Vì vậy, đối với việc áp dụng khái niệm ngang bằng được sử dụng trong đoạn (2), nên ghi nhớ rằng, sự ngang bằng được thiết lập giữa các chứng chỉ có thể so sánh về mặt chức năng. Tuy nhiên, Luật mẫu không dự định thiết lập sự tương ứng giữa các chứng chỉ có các kiểu khác nhau, do các nhà cung cấp dịch vụ chứng thực khác nhau phát hành và trong các phạm vi quyền hạn khác nhau. Luật mẫu được soạn thảo nhằm vào hệ thống phân cấp có thể giữa các kiểu chứng chỉ khác nhau. Trong thực tế, yêu cầu một toà án hoặc trọng tài phân xử quyết định hiệu lực pháp lý của một chứng chỉ nước ngoài và cố gắng cân bằng nó với mức tương ứng gần nhất tại nước ban hành luật (xem A/CN.9/483, đoạn 33).

Đối xử ngang bằng với các chứng chỉ và các kiểu chữ ký điện tử khác

156. Quy tắc đối xử với các chữ ký điện tử được trình bày trong đoạn (3) giống như quy tắc đối xử với các chứng chỉ trong đoạn (2) (đoạn 41).

Việc công nhận hiệu lực pháp lý phù hợp với luật từng nước

157. Đoạn (2) và (3) liên quan tới việc kiểm tra tính tin cậy qua biên giới, các đoạn này được áp dụng khi đánh giá sự tin cậy của một chứng chỉ hoặc chữ ký điện tử của nước ngoài. Tuy nhiên, trong quá trình soạn thảo Luật mẫu, cần ghi nhớ rằng, các nước ban hành luật có thể không muốn kiểm tra tính tin cậy đối với các chữ ký hoặc chứng chỉ xác định khi nước ban hành luật được thuyết phục rằng, luật về phạm vi quyền hạn (chữ ký hoặc chứng chỉ có nguồn gốc từ đó) cung cấp một chuẩn tin cậy ngang bằng. Về các kỹ thuật hợp pháp, qua nó công nhận sự tin cậy đối với các chứng chỉ và chữ ký theo luật của từng nước có thể do nước ban hành luật đưa ra (ví dụ, một hiệp ước hoặc công bố đơn phương), Luật mẫu không có đề xuất cụ thể (xem các đoạn 39 và 42).

Các yếu tố cần quan tâm khi đánh giá sự ngang bằng thực tế của các chữ ký và chứng chỉ nước ngoài

158. Trong quá trình soạn thảo Luật mẫu, ban đầu đoạn (4) được đưa vào một danh sách các yếu tố cần quan tâm khi xác định một chứng chỉ hoặc chữ ký điện tử có mức tin cậy ngang bằng, phù hợp với các mục đích của đoạn (2) và (3) hay không. Sau đó, người ta nhận ra rằng, hầu hết các yếu tố này đã được liệt kê trong các mục 6, 9 và 10. Việc bắt đầu lại các yếu tố này trong phạm vi của mục 12 là không cần thiết. Việc bổ xung lần lượt các tham khảo được trình bày quá phức tạp, liên quan tới tiêu chuẩn công nhận qua biên giới vào đoạn (4) làm cho nó trở thành một tham khảo không riêng biệt (cụ thể, xem A/CN.9/483, các đoạn 43-49). Thêm vào đó, việc đánh giá mức độ ngang bằng của các chứng chỉ nước ngoài khác với việc đánh giá tính tin cậy của nhà cung cấp dịch vụ chứng thực theo mục 9 và 10. Vì vậy, tham khảo được thêm vào đoạn (4) là "các chuẩn Quốc tế được công nhận".

Các chuẩn Quốc tế được công nhận

159. Khái niệm "Các chuẩn Quốc tế được công nhận" nên được làm sáng tỏ rộng hơn, bao trùm lên các chuẩn kỹ thuật và thương mại Quốc tế, các chuẩn và quy tắc do các thực thể chính phủ hoặc liên chính phủ thông qua (xem đoạn 49). "Các chuẩn Quốc tế được công nhận" có thể là các công bố về kỹ thuật, pháp lý hoặc hoạt động thương mại được chấp nhận, có thể do các thực thể cá nhân hoặc công cộng phát triển (hoặc cả hai), mang tính quy phạm hoặc giải thích, chúng được chấp nhận áp dụng Quốc tế. Các chuẩn này có thể theo dạng

các yêu cầu, các khuyến nghị, hướng dẫn, quy tắc hướng dẫn, hoặc các công bố về các hoạt động hoặc quy tắc tốt nhất (các đoạn 101-104).

Việc công nhận các thoả thuận giữa các thành viên liên quan

160. Đoạn (5) công nhận các thoả thuận về sử dụng một số kiểu chữ ký điện tử hoặc chứng chỉ giữa các thành viên liên quan, làm nền móng cho việc công nhận các chữ ký và chứng chỉ qua biên giới (xem đoạn 54). Nên lưu ý rằng, để phù hợp với mục (5), đoạn (5) không dự định thay thế các luật bắt buộc mà nước ban hành luật mong muốn áp dụng, đặc biệt là luật bắt buộc yêu cầu chữ ký viết tay (xem đoạn 113). Đoạn (5) cần mang lại hiệu lực cho các quy định hợp đồng được các thành viên chấp thuận, nhằm công nhận việc sử dụng một số chữ ký điện tử hoặc chứng chỉ (được coi là của nước ngoài tại một số hoặc tất cả các nước, nơi các thành viên tìm kiếm sự công nhận pháp lý đối với các chữ ký điện tử hoặc các chứng chỉ này), không cần các chữ ký điện tử hoặc các chứng chỉ này trải qua cuộc kiểm tra đánh giá mức độ ngang bằng thực tế (được thiết lập trong các đoạn (2), (3) và (4). Đoạn (5) không ảnh hưởng đến vị trí hợp pháp của các thành viên thứ 3 (xem đoạn 56).

<u>Các tài liệu tham khảo của UNCITRAL</u>

A/CN.9/484, các đoạn 76-78;

A/CN.9/WG.IV/WP.88, phụ lục, các đoạn 147-155;

A/CN.9/483, các đoạn 25-58 (mục 12);

A/CN.9/ WG.IV/WP.84, các đoạn 61-68; (dự thảo mục 13);

A/CN.9/465, các đoạn 21-35;

A/CN.9/WG.IV/WP.82, các đoạn 69-71;

A/CN.9/454, đoạn 173;

A/CN.9/446, các đoạn 196-207 (dự thảo mục 19);

A/CN.9/WG.IV/WP.73, đoạn 75;

A/CN.9/437, các đoạn 74-89 (dự thảo mục 1); và

A/CN.9/WG.IV/WP.71, các đoạn 73-75.

TÀI LIỆU THAM KHẢO

1. *G.P.SCHNEISER and J.T.Perry, "Electronic Commerce", Course Technology, 2000.*
2. *D.Stinson, "Cryptography: Theory and Practice", CRC Press, 1995.*
3. *B.Schneider, "Applied Cryptography", 2nd edition, Wiley, 1995.*
4. *U.S.Department of Commerce, "Digital Signature Standard (DSS)", Federal Information Processing Standards Publication FIPS PUB 186, 1994.*
5. *UNCITRAL (United Nations Commission on International Trade Law) Model Law on Electronic Signatures (2001).*
6. *Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001).*