

TS. NGUYỄN NAM HẢI
KS. ĐÀO THỊ HỒNG VÂN
TS. PHẠM NGỌC THUY

CHỨNG THỰC TRONG THƯƠNG MẠI ĐIỆN TỬ



NHÀ XUẤT BẢN
KHOA HỌC VÀ KỸ THUẬT

Ts. Nguyễn Nam Hải - Ks. Đào Thị Hồng Vân - Ts. Phạm Ngọc Thuý

CHỨNG THỰC TRONG THƯƠNG MẠI ĐIỆN TỬ



**NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT
HÀ NỘI**

LỜI NÓI ĐẦU

Chúng thực trong các giao dịch điện tử là một hoạt động vô cùng quan trọng nhằm đảm bảo sự tồn tại và phát triển của Thương mại điện tử. Đây là một nội dung rất mới không chỉ với nước ta mà cả trên thế giới. Nó liên quan đến nhiều nội dung như bảo mật, chữ ký số, cơ sở hạ tầng khoá công khai, cơ quan chứng thực và nhiều nội dung khác nữa.

Cuốn sách trình bày tổng quan những vấn đề an toàn đặt ra cho thương mại điện tử. Cơ sở khoa học cho an toàn thương mại điện tử nói chung và chứng thực điện tử nói riêng đã được xem xét đến trong tài liệu. Để hoạt động chứng thực điện tử có thể triển khai trong thực tiễn cần phải giải quyết cả vấn đề công nghệ và vấn đề pháp lý. Những vấn đề này đã lần lượt được xem xét giải quyết trong các chương 4, 5, 6, 7. Những trình bày trong các chương này cho ta một cái nhìn đầy đủ hơn khi triển khai hoạt động thực chứng điện tử trong thực tế.

Cuốn sách này là một tài liệu tham khảo tốt cho tất cả những ai muốn tiến hành thương mại điện tử một cách an toàn, tin cậy. Nó cũng có thể sử dụng là tài liệu tham khảo cho các giáo viên và sinh viên đang giảng dạy, học tập trong những ngành liên quan cũng như cho cán bộ công tác trong các cơ quan quản lý nhà nước liên quan tới lĩnh vực này. Chúng tôi hy vọng và tin tưởng bạn đọc sẽ nhận được nhiều thông tin bổ ích từ cuốn sách này.

Vì đây là một vấn đề tương đối mới với Việt Nam, lại được biên soạn trong thời gian có hạn, nên dù chúng tôi cố gắng lựa chọn những thuật ngữ đã được sử dụng nhiều và tương đối quen thuộc nhưng chắc chắn vẫn không thể tránh khỏi việc sử dụng một số thuật ngữ chưa thật chính xác. Rất mong nhận được sự quan tâm đóng góp ý kiến của bạn đọc.

Hà Nội tháng 10 năm 2003

CHƯƠNG I

CÁC HIỂM HOẠ ĐỐI VỚI AN TOÀN THƯƠNG MẠI ĐIỆN TỬ

1.1 THƯƠNG MẠI ĐIỆN TỬ LÀ GÌ ?

Đối với nhiều người, thuật ngữ thương mại điện tử còn được gọi tắt là *e-commerce*, có nghĩa là mua bán trên Internet hay còn gọi là mua bán qua mạng (Web). Theo nghĩa rộng hơn, thương mại điện tử bao gồm nhiều hoạt động kinh doanh hơn là chỉ mua bán trên Web. Một số người và một số nhà kinh doanh sử dụng thuật ngữ kinh doanh điện tử (*electronic business*, viết tắt *e-business*) khi nói về thương mại điện tử. Tuy nhiên, các thuật ngữ thương mại điện tử và kinh doanh điện tử nói chung có thể dùng thay thế cho nhau.

Trong tài liệu này, thuật ngữ thương mại điện tử được sử dụng theo định nghĩa ở trên. Trước hết, chúng ta tìm hiểu thương mại truyền thống và các hoạt động của nó. Sau đó, sẽ tìm hiểu thương mại điện tử được tiến hành như thế nào trong thực tế.

Mặc dù, Web mới được tạo ra để trợ giúp cho việc mua bán của các nhà kinh doanh và các cá nhân, nhưng thực ra thương mại điện tử đã tồn tại trong nhiều năm. Trong nhiều thập kỷ qua, các ngân hàng đã sử dụng chuyển tiền điện tử (EFT), đây là hình thức chuyển giao điện tử các thông tin trao đổi tài khoản trên các mạng truyền thông cá nhân.

Các nhà kinh doanh cũng đã và đang tiến hành một hình thức thương mại điện tử khác trong nhiều năm qua, đó là trao đổi dữ liệu điện tử (EDI). EDI xảy ra khi một nhà kinh doanh truyền dữ liệu đọc được bằng máy tính theo một khuôn dạng chuẩn cho một nhà kinh doanh khác. Vào những năm 1960, các nhà kinh doanh nhận ra rằng nhiều tài liệu họ muốn trao đổi có liên quan đến việc vận chuyển hàng hoá bằng tàu thủy - như đơn đặt hàng, hoá đơn

bán hàng, hoá đơn vận chuyển và toàn bộ thông tin tương tự cho hầu hết mọi cuộc giao dịch. Họ cũng nhận ra rằng họ đã tốn khá nhiều thời gian và tiền để nhập những dữ liệu này vào các máy tính, in các mẫu giấy, sau đó phải nhập lại dữ liệu. Mặc dù đơn đặt hàng, hoá đơn bán hàng, hoá đơn vận chuyển cho mỗi giao dịch bao gồm nhiều thông tin tương tự nhau - như mục số lượng, chủng loại, giá cả và chất lượng - mỗi mẫu giấy có khuôn dạng duy nhất dùng để biểu diễn thông tin này. Nhờ tạo ra một tập hợp các khuôn dạng chuẩn dành cho việc truyền tin điện tử, các nhà kinh doanh có khả năng giảm các sai sót, tránh chi phí cho việc in ấn và không cần phải nhập lại dữ liệu.

Các nhà kinh doanh tiến hành EDI với các đối tác thương mại của mình. Các khuôn dạng chuẩn được sử dụng trong EDI chứa cùng thông tin mà các nhà kinh doanh ghi trong các tài liệu về các đơn đặt hàng, hoá đơn bán hàng, hoá đơn vận chuyển. Các hãng như General Electric và Wal-Mart đã đi tiên phong trong việc sử dụng EDI để cải thiện các quy trình mua bán của họ và mối quan hệ của họ với các nhà cung cấp. Các hãng khác, ví dụ như Sterling, Commerce One và Harbinger, đóng một vai trò quan trọng trong việc làm cho EDI trở nên thuận tiện hơn giữa các hãng bằng cách phát triển các phần mềm cần thiết.

Một vấn đề quan tâm lớn mà các nhà sử dụng EDI phải đối mặt là chi phí cho việc thiết lập cao. Cho đến thời gian gần đây, việc sử dụng EDI đồng nghĩa với việc phải mua phần mềm và phần cứng máy tính với giá cao, sau đó thiết lập các kết nối mạng trực tiếp (sử dụng các đường điện thoại thuê bao) với tất cả các thành viên thương mại hoặc đặt thuê bao với một mạng giá trị gia tăng (VAN). VAN là một hãng độc lập, cung cấp kết nối và các dịch vụ giao dịch EDI cho người mua và người bán. Trước khi Internet tồn tại như ngày hôm nay, VAN cung cấp hầu hết các kết nối giữa các thành viên thương mại và đảm bảo bí mật cho dữ liệu truyền. VAN yêu cầu trả phí hàng tháng cố định cộng với phí cho từng cuộc giao dịch. Nhiều hãng nhỏ hơn không có đủ khả năng tham gia EDI và mất các khách hàng quan trọng, các khách hàng này sẽ đến nơi khác để mua.

OpenMarket là một trong số các hãng đầu tiên đưa EDI lên Internet. Đồng thời còn có nhiều hãng phát triển phần mềm và tư

vấn EDI khác cũng đã tham gia theo hướng này. Các nhà chuyên môn ước tính hoạt động giao dịch EDI trên Internet có thể vượt qua con số 800 tỷ USD vào năm 2003.

Cùng với việc mua và bán trực tiếp, các hãng còn tiến hành nhiều hoạt động trợ giúp. Ví dụ, một người bán một sản phẩm phải xác định được nhu cầu, quảng cáo sản phẩm này cho những người mua hàng, chấp nhận các yêu cầu, phân phối sản phẩm, quảng cáo và chấp nhận bồi thường cho sản phẩm, khuyến khích các khách hàng sử dụng sản phẩm sau khi mua. Trong nhiều trường hợp, người bán sẽ làm theo yêu cầu của khách hàng hoặc tạo ra một sản phẩm theo yêu cầu của khách hàng. Người bán sản phẩm cũng tiến hành các hoạt động truyền thông. Họ phải xác định nhu cầu, sản phẩm có thể đáp ứng được yêu cầu của họ, định giá các sản phẩm này. Tiếp theo, người mua phải yêu cầu sản phẩm mà họ đã chọn, thỏa thuận giá cả, yêu cầu phân phối. Trong nhiều trường hợp, người mua cần duy trì liên lạc với người bán để bảo hành và bảo dưỡng đối với sản phẩm. Tất nhiên, người bán và người mua có thể tiến hành các giao dịch của họ không chỉ dành cho các sản phẩm mà còn dành cho các dịch vụ. Khi bạn hiểu về thương mại, bạn có thể thấy nó có thể bao gồm nhiều cá nhân, các hãng thương mại, các tổ chức phi lợi nhuận và các thực thể thuộc chính phủ hoạt động với tư cách như những người bán và người mua.

Một cách tốt để hiểu đầy đủ thương mại điện tử là tìm hiểu những hoạt động mà các công ty thực hiện khi họ tiến hành bất kỳ kiểu kinh doanh nào và sau đó tìm hiểu các công ty này có thể tiến hành các hoạt động điện tử như thế nào. Trong hai mục tiếp theo, chúng ta tìm hiểu các yếu tố của thương mại truyền thống và sau đó xem các yếu tố này được thực hiện như thế nào trong thương mại điện tử.

Thương mại điện tử

Qua hàng ngàn năm, con người tiến hành hoạt động thương mại thông qua các công cụ và các kỹ thuật có hiệu quả. Ví dụ, việc cập bến của những con thuyền từ xa xưa mở ra các con đường mới trong thương mại cho các nhà buôn bán. Nhiều tiến bộ kỹ thuật như máy in, động cơ hơi nước và điện thoại đã giúp cho con người

tiến hành và phát triển các hoạt động thương mại.

Các hãng đã sử dụng nhiều công cụ truyền thông điện tử trong các thập kỷ qua để tiến hành các loại giao dịch thương mại khác nhau. Các ngân hàng đã và đang sử dụng hình thức chuyển tiền điện tử (EFT) để chuyển tiền của các khách hàng đi khắp thế giới; các nhà kinh doanh sử dụng EDI để đưa ra các yêu cầu và gửi các hóa đơn cho khách hàng và các thương nhân sử dụng quảng cáo trên các phương tiện thông tin đại chúng để có được các yêu cầu đặt hàng cho tất cả các loại hàng hoá của họ.

Một định nghĩa hoàn hảo về thương mại điện tử có thể được đề cập đến như việc sử dụng truyền dữ liệu điện tử để thiết lập hoặc nâng cao quy trình thương mại bất kỳ. Một số người sử dụng thuật ngữ thương mại Internet, có nghĩa là thương mại điện tử đặc biệt sử dụng Internet hoặc Web làm phương tiện để truyền dữ liệu. Khi lĩnh vực thương mại điện tử vẫn còn mới, nhiều thuật ngữ khác nhau đã được sử dụng cho thương mại điện tử. Ví dụ, IBM đã định nghĩa kinh doanh điện tử là "sự biến đổi của các quy trình kinh doanh chủ chốt thông qua việc sử dụng các kỹ thuật Internet".

Trong phần này chúng ta sẽ xem xét các kỹ thuật truyền dữ liệu điện tử được sử dụng như thế nào. Chúng là một phần chủ yếu của Internet và Web để nâng cao các quy trình kinh doanh hiện đang tồn tại và xác định các cơ hội kinh doanh mới. Một phần quan trọng của thương mại điện tử là hiểu được các hãng đã sử dụng nó như thế nào để thích ứng với sự thay đổi. Lĩnh vực thương mại ngày nay thay đổi rất nhanh. Có nhiều cuốn sách đã trình bày các kỹ thuật, tập trung chủ yếu vào kinh doanh của thương mại điện tử và các kỹ thuật giúp cho quy trình kinh doanh có thể thực hiện được.

Một chức năng quan trọng của phần này là giúp bạn xác định các quy trình kinh doanh mà các hãng thực hiện rất hiệu quả nhờ công nghệ thương mại điện tử. Trong nhiều trường hợp, các quy trình kinh doanh sử dụng các hoạt động thương mại truyền thống rất hiệu quả, các quy trình này không thể nâng cấp thông qua kỹ thuật. Các sản phẩm mà những người mua yêu cầu nắm bắt, ngửi, hoặc kiểm tra trực tiếp trở nên khó khăn khi bán bằng cách sử dụng thương mại điện tử. Ví dụ, các khách hàng có thể miễn

cường khi mua hàng quần áo hợp thời trang và các thực phẩm dễ ôi thiu, như thịt hoặc sản vật, nếu họ không thể kiểm tra trực tiếp sản phẩm trước khi đồng ý trả tiền mua.

Tuy nhiên, có nhiều loại hàng hoá và các sản phẩm, chẳng hạn như sách hoặc các CD, có thể được bán dễ dàng bằng cách sử dụng thương mại điện tử. Đó là vì một bản sao của một cuốn sách mới giống hệt với các bản sao khác và vì khách hàng không quan tâm đến mức thích hợp, tính chất mới, hoặc chất lượng, các khách hàng sẽ chỉ yêu cầu đầu đề sách mà không cần kiểm tra bản sao họ sẽ nhận được. Trong phần này chúng ta xem xét những thuận lợi và những khó khăn khi sử dụng thương mại điện tử cho các quy trình kinh doanh đặc trưng.

Bảng 1.1 trình bày 12 ví dụ quy trình kinh doanh. Bốn trong số chúng thích hợp cho thương mại điện tử và 4 thích hợp cho thương mại truyền thống. Bốn quy trình kinh doanh trong cột cuối cùng thích hợp cho việc kết hợp cả hai hướng. Tất nhiên, cách phân loại này phụ thuộc vào tình trạng hiện thời của các kỹ thuật có sẵn và có thể thay đổi cùng với sự phát triển của các công cụ mới dành cho việc thiết lập thương mại điện tử. Các qui trình kinh doanh như bảng 1.1.

Bảng 1.1. Sự phù hợp giữa quy trình kinh doanh và hình thức thương mại

<i>Thương mại điện tử (TMĐT)</i>	<i>Thương mại truyền thống (TMTT)</i>	<i>Kết hợp TMĐT và TMTT</i>
Bán/mua sách và CD	Bán/mua quần áo hợp thời trang	Bán/mua xe ô tô
Phân phối trực tiếp phần mềm	Bán/mua các sản phẩm thức ăn dễ hỏng	Thanh toán ngân hàng trực tuyến
Các dịch vụ quảng cáo và khuyến mại du lịch	Các giao dịch mệnh giá tiền tệ nhỏ	Các dịch vụ chung
Kiểm tra trực tiếp vận chuyển bằng tàu	Bán đồ trang sức và đồ cổ đắt tiền	Bán/mua các sản phẩm bảo hành và đầu tư

Việc kết hợp các chiến lược thương mại điện tử và thương mại truyền thống là việc làm tốt nhất khi quy trình kinh doanh bao gồm cả các yếu tố hàng hóa và kiểm tra cá nhân. Ví dụ, nhiều người tìm hiểu thông tin về ô tô trên Web, nhưng ít người có thể mua một chiếc xe ô tô để sử dụng mà không tự tay lái và kiểm tra. Trong trường hợp này, thương mại điện tử cung cấp một cách thức khá hay cho người mua để có được thông tin về các mẫu mới, các tùy chọn và giá cả, nhưng người mua phải tự mình kiểm tra và lái thử thực tế, không thể có một cuộc lái thử xe trên Web. Hai phần tiếp theo tập trung vào những khó khăn và thuận lợi của thương mại điện tử.

Những thuận lợi của thương mại điện tử

Các hãng quan tâm đến thương mại điện tử đơn giản vì nó có thể giúp tăng lợi nhuận. Tất cả những thuận lợi của thương mại điện tử đối với các thực thể kinh doanh có thể được tổng kết trong một câu như sau: *thương mại điện tử có thể tăng khả năng bán hàng và giảm chi phí.*

Nếu tiến hành quảng cáo tốt trên Web thì có thể các thông báo quảng cáo của một hãng nhỏ cũng có thể tới được các khách hàng ở mọi quốc gia trên thế giới. Một hãng có thể sử dụng thương mại điện tử để tìm kiếm các khu vực thị trường hẹp nhưng dàn trải rộng về mặt địa lý. Internet và Web đặc biệt hữu ích trong việc tạo ra các cộng đồng ảo, đó là tập hợp một nhóm người có thể chia sẻ các mối quan tâm chung, nhưng thay vì việc tập hợp xảy ra ở môi trường tự nhiên thì điều đó lại xảy ra trên Internet.

Chi phí cho việc xử lý kiểm tra bán hàng, cung cấp báo giá và quyết định sản phẩm sẽ giảm đi nhờ sử dụng thương mại điện tử. Vào năm 1998, hãng Cisco bán được 72% thiết bị máy tính thông qua Web mà không cần sự trợ giúp của bất kỳ một đại lý dịch vụ khách hàng nào, Cisco ước tính điều này có thể giúp tránh được việc xử lý 500.000 cuộc gọi trong một tháng và hàng năm có thể tiết kiệm được trên 500 triệu USD.

Thương mại điện tử không chỉ làm tăng các cơ hội bán hàng đối với người bán mà nó còn làm tăng cơ hội mua hàng đối với người mua. Các nhà kinh doanh có thể sử dụng thương mại điện tử trong các quy trình mua để tìm ra nhà cung cấp mới. Việc thương

lượng giá cả và phân phối hàng hoá trở nên đơn giản hơn trong thương mại điện tử, vì Web có thể cung cấp các thông tin chào hàng một cách rất hiệu quả. Thương mại điện tử tăng tốc độ và độ chính xác, trong đó các nhà kinh doanh có thể thay đổi thông tin, làm giảm chi phí cho cả hai phía giao dịch.

Thương mại điện tử cung cấp cho người mua nhiều sự lựa chọn hơn thương mại truyền thống, vì họ có thể quan tâm đến nhiều sản phẩm và dịch vụ khác nhau từ những người bán khác nhau. Các thông tin này có thể tìm kiếm được 24 giờ một ngày và tất cả các ngày. Thương mại điện tử cung cấp thông tin cho người mua một cách khá dễ dàng và họ có thể tùy chọn mức độ chi tiết của thông tin về cuộc mua bán sắp tới. Thay vì việc ngồi chờ các catalog hoặc tờ rơi nói về các đặc tính của sản phẩm được gửi tới qua đường bưu điện, hoặc nhanh hơn cũng hàng mấy phút cho một cuộc truyền fax, những người mua có thể ngay lập tức truy nhập để lấy được thông tin chi tiết trên Web. Một số sản phẩm, như phần mềm, các audio clip, hoặc ảnh, thậm chí có thể được phân phối qua Internet, làm giảm thời gian cho người mua vì không phải mất công chờ đợi trước khi bắt đầu cuộc mua bán.

Lợi ích của thương mại điện tử cũng được mở rộng tới phúc lợi xã hội nói chung. Chi trả điện tử đối với việc hoàn lại thuế, trợ cấp hưu trí, trợ cấp phúc lợi, giúp đến nơi an toàn và nhanh chóng khi truyền qua Internet.

Hơn nữa, chi trả điện tử có thể dễ dàng kiểm tra và quản lý hơn là chi trả thông thường (hoá đơn, giấy tờ), tránh được tham ô và biến thủ. Mở rộng hơn nữa, thương mại điện tử cho phép mọi người có thể làm việc tại nhà, giảm tắc nghẽn giao thông và ô nhiễm. Thương mại điện tử có thể làm cho các sản phẩm và các dịch vụ trở nên có giá trị ở những khu vực xa xôi. Ví dụ, giáo dục từ xa giúp cho mọi người có thể học được các kỹ năng và có thể thi lấy bằng mà không quan tâm đến họ ở đâu và mất bao nhiêu lâu để họ có thể học được.

Những khó khăn của thương mại điện tử

Một số quy trình kinh doanh có thể không bao giờ thích hợp với thương mại điện tử. Ví dụ, thực phẩm dễ ôi thiu và hàng hoá giá cả cao như đồ trang sức, đồ cổ không thích hợp với việc kiểm tra từ

xa. Hầu hết các khó khăn của thương mại điện tử ngày nay xuất phát từ tính chất mới lạ và việc phát triển nhanh chóng của các kỹ thuật cơ bản. Những khó khăn này sẽ biến mất và thương mại điện tử trở nên có giá trị hơn, được đại đa số dân chúng chấp nhận. Nhiều sản phẩm và các dịch vụ đã được đại số người mua khó tính chấp nhận và có ý định mua qua Internet. Ví dụ, Peapod (buôn bán tạp phẩm) chỉ phân phối các dịch vụ ở một số thành phố. Nhiều khách hàng của Peapod đã liên lạc qua Internet và bắt đầu cảm thấy thoải mái với việc mua bán trực tuyến, nó có khả năng mở rộng ra nhiều vùng khác nhau.

Các nhà kinh doanh thường tính toán ngược lại con số đầu tư trước khi quyết định đầu tư vào bất kỳ một kỹ thuật mới nào. Điều này trở nên khó khăn cho việc đầu tư vào thương mại điện tử, bởi vì chi phí và lợi nhuận khó có thể xác định rõ ràng. Chi phí là một hàm số của kỹ thuật, có thể thay đổi đột ngột, thậm chí trong các dự án thiết lập tồn tại trong thời gian ngắn, do các kỹ thuật cơ bản cũng thay đổi nhanh chóng. Nhiều hãng gặp phải rắc rối trong việc tuyển người, giữ những người làm công có tay nghề về kỹ thuật, thiết kế và các kỹ năng kinh doanh cần thiết để tạo ra tính hiệu quả của thương mại điện tử. Một vấn đề nữa mà các hãng phải đối mặt khi muốn kinh doanh trên Internet là việc tích hợp các cơ sở dữ liệu đang tồn tại và phần mềm xử lý giao dịch được thiết kế dành cho thương mại truyền thống vào phần mềm dành cho thương mại điện tử.

Nhiều nhà kinh doanh phải đối mặt với phong tục tập quán và các luật cản trở đối với thương mại điện tử. Một số khách hàng có phần e ngại việc gửi số thẻ tín dụng của họ lên Internet. Một số khách hàng khác đơn giản không nhất trí việc thay đổi và cảm thấy không hài lòng khi xem xét hàng hoá trên màn hình máy tính. Về môi trường quản lý thương mại điện tử, luật lệ nhiều lúc còn thiếu rõ ràng và có khi mâu thuẫn. Trong nhiều trường hợp, sự điều chỉnh của Chính phủ không theo kịp các công nghệ mới. Các luật quản lý thương mại phải được đưa ra và ký duyệt sao cho phù hợp với bất kỳ loại giao dịch kinh doanh nào. Khi nhiều nhà kinh doanh và các cá nhân nhận thức được các lợi ích của thương mại điện tử, thì những khó khăn trên sẽ dần biến mất.

Thương mại điện tử quốc tế

Internet giúp cho mọi người từ nhiều quốc gia trên thế giới xích lại gần nhau hơn, làm giảm đi khoảng cách giữa mọi người. Ngôn ngữ chiếm ưu thế trên Web là tiếng Anh. Một khi rào cản ngôn ngữ được vượt qua, thương mại điện tử sẽ cho phép tiến hành kinh doanh giữa các ngành kinh doanh với nhau hoặc giữa các khách hàng ở mọi nơi trên thế giới.

Đáng tiếc là cơ chế chính trị của thế giới không theo kịp kỹ thuật Internet, vì vậy việc tiến hành thương mại quốc tế gặp phải một số thách thức. Quy định về việc chuyển tiền, thuế, giới hạn xuất và nhập khẩu, phong tục tập quán kinh doanh địa phương và luật của mỗi quốc gia, nơi mà những thành viên thương mại cư trú có thể làm cho thương mại điện tử quốc tế trở nên khó khăn.

Nhiều vấn đề quốc tế mang tính cá nhân, pháp lý phát sinh. Mỗi quốc gia có quyền bỏ qua các luật và đánh thuế vào các ngành kinh doanh trong phạm vi quyền hạn của họ. Nhiều nước ở châu Âu có luật rất cứng rắn hạn chế việc thu thập và sử dụng thông tin cá nhân mà các công ty thu được trong quá trình tiến hành kinh doanh với các khách hàng. Ở các quốc gia khác, thuế giá trị gia tăng và doanh thu bán hàng đánh vào tất cả các hoạt động kinh doanh. Tìm hiểu chi tiết, chúng ta sẽ thấy các vấn đề mang tính cá nhân, pháp lý có thể phát sinh khi quản lý thương mại điện tử.

Sự phát triển công nghệ chính là làm cho thương mại điện tử phát triển vượt xa sự khởi đầu của nó trong EFT và EDI, đây cũng chính là sự nổi bật của Internet và Web.

1.2 CÁC HIỂM HỌA ĐỐI VỚI AN TOÀN THƯƠNG MẠI ĐIỆN TỬ

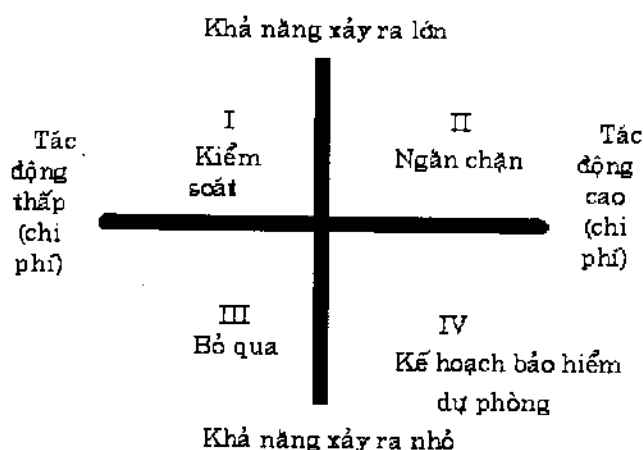
1.2.1 Giới thiệu chung

Khi Internet mới hình thành, 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, liệu 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 họa còn lớn hơn. Internet càng ngày càng phát triển và các cách mà chúng ta sử dụng nó cũng đa dạng

hơn. Do vậy nếu 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, các mối quan tâm về an toàn thông tin 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. Cách đây 30 năm 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 cũng như các giải pháp hiện thời.



Hình 1.1 Mô hình quản lý rủi ro

An toàn máy tính: Chính là việc bảo vệ các tài sản không bị truy nhập, sử dụng, hoặc phá hủy 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 họa”.

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 họa. Các biện pháp đối phó thường biến đổi, phụ thuộc vào tầm quan trọng của tài sản trong rủi ro. Các hiểm họa 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 họa này vượt quá giá trị của tài sản cần được bảo vệ. Mô hình quản lý rủi ro được trình bày trong hình 1.1.

Có 4 hoạt động chung mà bạn có thể tiến hành, phụ thuộc vào chi phí và khả năng xảy ra của các hiểm họa vật lý.

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 họa vật lý và logic. 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 họa và đưa ra các cách nhằm bảo vệ các tài sản khỏi bị hiểm họa đó.

Phân loại an toàn máy tính

Các chuyên gia trong lĩnh vực này 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 ngưng trệ 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

họa 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 tính 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. Các hiểm họa đối với tính sẵn sàng xảy ra khá thường xuyên hơn. 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 họa. Chính sách an toàn phải được phát triển liên tục, công ty hoặc văn phòng an toàn phải tra cứu và cập nhật định kỳ.

Để có được một chính sách an toàn, chúng ta phải bắt đầu từ

việc xác định những thứ cần phải bảo vệ. Sau đó, xác định người nào có quyền truy nhập vào 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, các tài nguyên phần mềm và phần cứng (tự tạo hoặc mua lại) chịu trách nhiệm thực hiện chính sách an toàn. Ví dụ, nếu chính sách an toàn xác định rằng, không một ai được phép truy nhập trái phép vào thông tin khách hàng và các thông tin như số thẻ tín dụng, profile của tín dụng, chúng ta phải viết phần mềm đảm bảo bí mật từ đầu này tới đầu kia 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 hủy 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 họa đối với thông tin số, đầu tiên là các hiểm họa đối với sở hữu trí tuệ.

1.2.2 Các hiểm họa đối với sở hữu trí tuệ

Các hiểm họa 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 là 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 rất 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. 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, số 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 chú tâm sao chép một sản phẩm đã được bảo vệ và gửi nó trên Web.

Mặc dù luật bản quyền đã được ban hành trước khi Internet hình thành, Internet đã làm rắc rối các ràng buộc bản quyền. Việc sao chép trái phép một văn bản khá dễ dàng, còn việc ngăn cấm 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 đã giới thiệu một khoá học có tiêu đề "Sở hữu trí tuệ trong không gian máy tính". Khoá học nhằm giải quyết các vấn đề về bản quyền, gửi các nhóm tin và sử dụng hợp pháp. Việc sử dụng hợp pháp cho phép sử dụng giới hạn các tài liệu có bản quyền sau khi đáp ứng 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 đăng ký tên miền (*Cybersquatting*). *Cybersquatting* là một hoạt động đăng ký tên miền, đúng hơn là đăng ký thương hiệu của một cá nhân hay công ty khác và người chủ sở hữu sẽ trả một số tiền khá lớn để có được địa chỉ URL.

1.2.3 Các hiểm họa 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, đường truyền dẫn, các máy chủ Web và máy chủ thương mại. Chẳng hạn 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. Do vậy, các giao dịch thương mại chỉ có thể an toàn chừng nào tất cả các yếu tố của hệ thống đều an toàn. Các mục tiếp theo sẽ trình bày về các hiểm họa và cách bảo vệ từng khâu trong “dây chuyền thương mại điện tử”. Trước hết chúng ta xem xét các hiểm họa đối với các máy khách.

Các mối hiểm họa đối với máy khách

Thời kỳ đầu của Internet các trang Web thường ở trạng thái tĩnh dùng để biểu diễn nội dung và cung cấp các liên kết đến các thông tin bổ sung khác. Tuy nhiên, với sự hỗ trợ của nội dung động (*active content*), các trang Web đã trở nên sống động và hấp dẫn hơn nhiều.

Khi nói đến nội dung động, người ta muốn nói đến các chương trình được cài vào các trang Web (một cách trong suốt đối với người dùng) và tạo ra các hoạt động. Nội dung động có thể hiển thị hình ảnh động, tải về và phát lại âm thanh, hoặc thực hiện các chương trình bằng tính dựa vào Web. Nội dung động 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 và chi phí xử lý. Các nhà phát triển nắm lấy nội dung động vì nó tận dụng tối đa chức năng của HTML (Ngôn ngữ đánh dấu siêu văn bản) và bổ sung 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 nhờ gánh nặng này được chuyển bớt sang cho các máy khách nhận rồi của người sử dụng.

Nội dung động được cung cấp theo một số dạng, các dạng nội dung động được biết đến nhiều nhất là Applets, ActiveX controls, JavaScript và VBScript.

JavaScript và VBScript cung cấp tập các lệnh hoặc các lệnh có thể thực hiện được một chức năng nào đó, 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 nội dung động, nhưng chúng không phổ biến với nhiều người, chẳng hạn như các trình đồ họa và các trình duyệt Web plug-ins. Các tệp đồ họa có thể chứa các 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 lệnh được tìm thấy trong chương trình đồ họa, một số khuôn dạng khác có thể tạo ra các lệnh không có lợi (ẩn trong các lệnh đồ họa) và chúng cũng được thực hiện. Plug-ins là các chương trình biên dịch hoặc thực hiện các lệnh, được nhúng vào trong các hình ảnh, âm thanh tải về.

Nội dung động mang lại 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. Nội dung động mang lại sự sống động cho các trang Web tĩnh.

Nội dung động 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 nội dung động. 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 môđun nội dung động được cài 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 nội dung động 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 Troia 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 xóa bỏ thông tin trên một máy khách (một hình thức xâm phạm tính toàn vẹn).

Việc đưa nội dung động 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 tệp đặc biệt, các tệp này được gọi là cookie (các khai báo yêu cầu). Các cookie được sử dụng để nhớ các thông tin yêu cầu của khách hàng, hoặc tên người dùng và mật khẩu. Nhiều nội dung động gây hại có thể lan truyền thông qua các Cookie, chúng có thể phát hiện được nội dung của các tệp phía máy khách, hoặc thậm chí có thể huỷ bỏ các tệp 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 trình duyệt Web. 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 như Cookie Crusher (kiểm soát các cookie trước khi chúng được lưu giữ trên ổ cứng của máy tính) và Cookie Pal.

Các mối hiểm họa 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 họa 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 (*Defense Advanced Research*

Projects Agency) 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 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 và an toàn. Một thông báo được gửi đi từ Manchester, nước Anh tới Cairo, Ai cập cho một thương nhân có thể đi qua máy tính của một đối tượng cạnh tranh, chẳng hạn ở Libăng. Vì chúng ta không thể kiểm soát được đường dẫn và không biết được các gói thông tin đang ở đâu, những đối tượng trung gian có thể đọc các thông báo, 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 bí mật, tính toàn vẹn và tính sẵn sàng. Chúng ta sẽ xem xét chi tiết các mối hiểm họa đối với an toàn kênh trên Internet dựa vào sự phân loại này.

Các mối hiểm họa đối với tính bí mật

Đe dọa tính bí mật là một trong những mối hiểm họa 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 tùy tiện hay không. 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 đối với 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 thiết bị định tuyến trên đường đi từ nguồn tới đích. Chương trình đánh hơi gần giống với việc móc nối vào một đường điện thoại và ghi lại cuộc hội thoại. Các chương trình đánh hơi 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, ngoài ra 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 cũng 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 USD).

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 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 khai báo như tên, địa chỉ và địa chỉ thư tín điện tử của bạn. Khi bạn điền vào các hộp khai báo 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 khai báo, 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 (Giao thức truyền siêu văn bản) 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.other.com*. Máy chủ Other.com có thể chọn để thu thập các trang Web để 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 đã tới site. Bằng cách ghi lại địa chỉ URL anybiz.com, Other.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 đến Amazon.com, Anonymizer sẽ đưa ra URL như sau:

<http://www.anonymizer.com:8080/http://www.amazon.com>

Các hiểm họa đối với tính toàn vẹn

Mối hiểm họa 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 họa đối với tính bí mật (người xem đơn giản chỉ muốn xem thông tin), các hiểm họa 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 có thể xóa 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 kẻ hở trong máy chủ 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 kẻ hở trong DNS để thay thế địa chỉ IP giả của tin tặc vào địa chỉ IP thực của Widgets Inter-national. 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 họa 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 họa đối với tính sẵn sàng

Mục đích của các hiểm họa đối với tính sẵn sàng 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 họa 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 1 giây, 2 giây lên tới 30 giây, người sử dụng sẽ không muốn 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 xóa bỏ toàn bộ hoặc loại bỏ một phần các thông tin trong một tệp hoặc một cuộc truyền thông. Như đã biết, Quicken là một chương trình tính toán, nó có thể được cài đặt vào tất cả các máy tính nhằm làm chệch hướng tiền gửi đến tài khoản của một ngân hàng khác. Tấn công chối bỏ sẽ phủ nhận số tiền gửi của những người chủ hợp pháp của số tiền đó. Tấn công Robert Morris Internet Worm là một ví dụ điển hình về tấn công chối bỏ.

Các mối hiểm họa 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 hủy, 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 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 giao diện cửa chung (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 có khả năng kiểm soát tất cả các phần của một hệ thống thương mại điện tử.

Các hiểm họa đối với máy chủ Web

Phần mềm máy chủ Web được thiết kế để chuyển các trang Web cho các yêu cầu của HTTP. 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. 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 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, chỉ 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 họa 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 tệp 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.

SSI (*Server Side Include*) 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 tệp mật khẩu, hoặc gửi ngược trở lại một vị trí đặc biệt.

Chương trình FTP (Giao thức truyền tệp) có thể phát hiện các mối hiểm họa 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 khách 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 chủ Web. Việc làm này không có gì khó nếu thiếu sự 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 duyệt của một đối tác khác đối với một danh mục đơn lẻ.

Một trong các tệp nhạy cảm nhất trên máy chủ Web (nếu tồn tại) chứa mật khẩu và tên người dùng của máy chủ Web. Nếu tệp này bị khám phá, bất kỳ ai cũng có thể thâm nhập vào các vùng có 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 điểm yếu dễ bị tấn công. 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 của người đó. Người ta gọi việc đoán nhận mật khẩu thông qua một chương trình lập 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 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 không thiết lập an toàn mà hoàn toàn và dựa vào máy

chủ Web dễ 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 dạng con ngựa thành Troia 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.

Có một số lượng lớn các trang Web 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 "Các hiểm họa đối với cơ sở dữ liệu máy chủ SQL" trong Online Companion trình bày các mối hiểm họa đối với máy chủ SQL, nhưng chúng cũng có thể xảy ra đối với 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 họa 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 nội dung động 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 chứa trình duyệt bạn đang làm việc. Do CGI là các chương trình, khi chúng bị lạm dụng sẽ xảy ra một hiểm họa 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 tài nguyên của hệ thống, chúng có khả năng làm cho hệ thống không hoạt động, xóa các tệp, 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 tài nguyên của máy chủ Web này. Không giống với JavaScript, CGI script không chạy trong một vòng bảo vệ an toàn.

Các hiểm họa 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 tệp 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 tệp 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 vào và ra. 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 viết chương trình sai) chính là các tấn công chổi bổ. Tấn công kiểu sâu Internet (*Internet Worm*) là một chương trình như vậy. Nó gây tràn bộ nhớ, phá hỏng tất cả các 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 quyền rất cao. Việc chiếm dụng chương trình dẫn đến các tệp 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. Liên kết "Các 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 đọng 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 họa an toàn.

1.2.4 CERT

Từ một thập kỷ trước, nhiều 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, một bộ phận của Cơ quan an toàn Quốc gia Mỹ, là 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 họa 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.

1.3 TÓM TẮT

Thương mại điện tử là sự ứng dụng các công nghệ mới, đặc biệt là công nghệ Internet và Web, nhằm giúp các cá nhân, nhà kinh doanh và các tổ chức khác điều khiển công việc kinh doanh tốt hơn. Không phải tất cả các hoạt động thương mại đều thích ứng với việc cải tiến các kỹ thuật này, nhưng nhiều hoạt động thì có. Nhờ sử dụng thương mại điện tử, nhiều nhà kinh doanh có khả năng tạo ra những sản phẩm và dịch vụ mới, cải thiện việc xúc tiến sản xuất, tiếp thị và phân phối theo yêu cầu. Nhiều hãng cũng tìm ra nhiều cách để sử dụng thương mại điện tử để cải thiện

các hoạt động mua bán và cung cấp, tìm ra các khách hàng mới và tiến hành các hoạt động tài chính, quản trị và quản lý tài nguyên con người hiệu quả hơn.

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. Bất kỳ một chính sách an toàn thương mại nào cũng phải bao gồm tính bí mật, tính toàn vẹn, tính sẵn sàng và quyền sở hữu trí tuệ.

Các hiểm họa đối với thương mại có thể xảy ra ở bất kỳ mắt xích nào trong dây chuyền thương mại, từ máy khách tới các máy chủ thương mại. Các thông tin về tấn công của 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 họa 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 kịch bản 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 họa 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 xuất hiện trong năm 1998 là một ví dụ điển hình về hiểm họa an toàn, nó sử dụng Internet như là một công cụ để 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 họa an toàn. Trầm trọng hơn, các hiểm họa 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 mà 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 họa 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 họa 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 II

NHỮNG MỤC TIÊU CỦA AN TOÀN THƯƠNG MẠI ĐIỆN TỬ

2.1 GIỚI THIỆU

Bảo vệ các tài sản điện tử (bao gồm các hệ thống thương mại điện tử) không phải là một tùy chọn, nó thực sự cần thiết nếu thương mại ngày càng phát triển. Thế giới điện tử sẽ phải thường xuyên đối mặt với virus, sâu, con ngựa thành Troia, đối tượng nghe trộm và các chương trình gây hại, mà mục đích của chúng là thu thập, phá vỡ, làm trễ hoặc từ chối dịch vụ giữa khách hàng và nhà cung cấp. Để tránh nguy cơ mất hàng tỷ USD, chúng ta cần tăng cường việc bảo vệ 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 đó có thể bảo vệ các máy khách, Internet và máy chủ thương mại.

2.2 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 quan trọng. Các khách hàng cần có được sự tin cậy, các giao dịch của họ phải được an toàn, không bị nghe trộm và sửa đổi. Ngày nay, kinh doanh thương mại trực tuyến rất lớn mạnh và sẽ còn không ngừng phát triển trong những 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.

Ba mươi năm trước, an toàn có nghĩa là đảm bảo an toàn vật lý, chẳng hạn như cửa ra vào, 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. Trong thời kỳ này, các tương tác giữa con người và

máy tính đều thông qua các thiết bị đầu cuối 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 đó 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 lúc này vẫn còn 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 tài nguyên máy tính, bởi vì họ có thể ở bất cứ nơi nào trên thế giới. 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 yêu cầu đặt hàng, xác nhận đặt hàng, hóa đơn và sổ thẻ tín dụng) 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 dọa đối với 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 nhóm nghiên cứu để phát triển các nguyên tắc an toàn máy tính, quản lý các thông tin được phân loại trong máy tính. Kết quả mà nhóm này đạt được là cuốn "Bộ tiêu chuẩn đánh giá hệ thống máy tính tin cậy" (*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 tiêu chuẩn được thiết lập 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 đưa ra được các tài sản cần bảo vệ, cần những gì để bảo vệ các tài sản này, phân tích các mối đe dọa 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 dọa 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...". Rõ ràng, an toàn là yếu tố sống còn đối với sự tồn tại và phát triển của thương mại điện tử.

2.3 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 họa 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, nó đòi hỏi cần thực hiện một số biện pháp nhằm cung cấp một mức bảo vệ và trách nhiệm nào đó đối với bản quyền.

WIPO (Tổ chức sở hữu trí tuệ thế giới) 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 (Hội công nghệ thông tin Mỹ) 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 thông qua công nghệ số. Các giải pháp này chưa được chi tiết nhưng dù sao nó cũng cung cấp một khả năng bảo vệ nào đó.

2.4 BẢO VỆ CÁC MÁY KHÁCH

Các máy khách (thông thường là các PC) phải được bảo vệ nhằm chống lại các đe dọa 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 khách theo yêu cầu của trình duyệt Web. Các nội dung động cũng được chuyển qua Internet thông qua các trang Web động. Chúng có thể là một trong các mối đe dọa nghiêm trọng nhất đối với các máy khách.

Nội dung động bao gồm nhiều chương trình được nhúng vào các trang Web, tạo nên sự sống động cho các trang Web. Tuy nhiên, một nội dung động giả có vẻ vô hại nhưng lại gây ra các thiệt hại khi chúng chạy trên máy tính của bạn. Bên cạnh các mối đe dọa xuất phát từ các chương trình bên trong các trang Web, thì các trình đồ họa, các trình duyệt gài sẵn (trình duyệt plug-ins) và các phần đính kèm thư điện tử cũng là các mối đe dọa có thể gây hại cho các máy khách khi các chương trình ẩn này được thực hiện.

Nhiều nội dung động 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 dọa khác đối với máy khách là một 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 được 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 họa xảy ra đối với máy khách.

Giám sát nội dung động

Các trình duyệt Navigator của Netscape và Internet Explorer của Microsoft được trang bị để nhận biết các trang Web có chứa nội dung động 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 máy khách và máy

chủ khi xác thực.

Các chứng chỉ số

Chứng chỉ số (hay ID số) là phần đính kèm với một thông báo thư điện tử hoặc một chương trình được nhúng vào một trang Web nhằm kiểm tra tính đích thực của người sử dụng hoặc Web site. 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 mà bạn tin cậy.

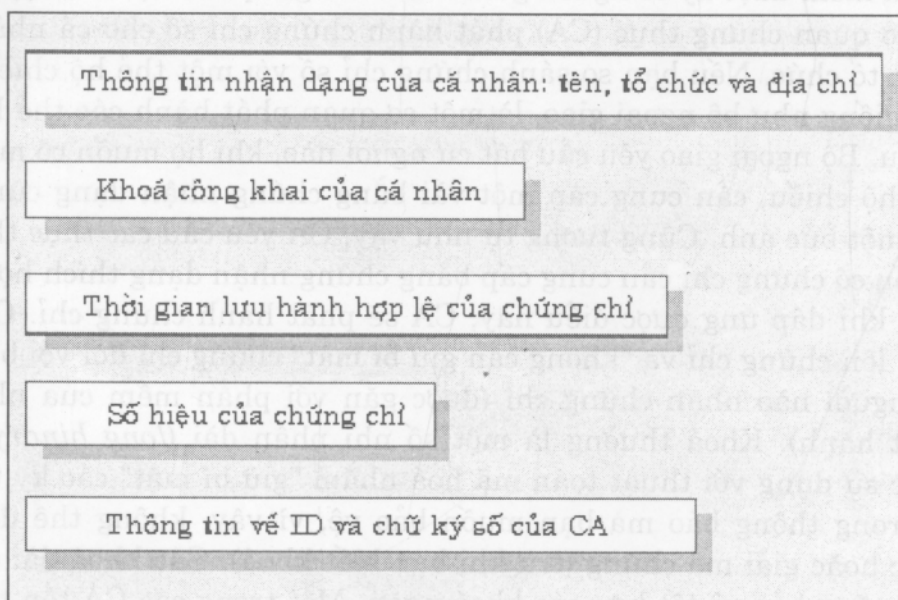
Cơ quan chứng thực (CA) phát hành chứng chỉ số cho cá nhân hoặc tổ chức. Nếu bạn so sánh chứng chỉ số với một thẻ hộ chiếu, CA giống như bộ ngoại giao, là một cơ quan phát hành các thẻ hộ chiếu. Bộ ngoại giao yêu cầu bất cứ người nào, khi họ muốn có một thẻ hộ chiếu, cần cung cấp một vài bằng chứng nhận 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 chứng chỉ. CA "ký" lên chứng chỉ và "không cần giữ bí mật" chứng chỉ đối với bất kỳ người nào nhận chứng chỉ (được gắn với phần mềm của nhà phát hành). Khoá 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 dấu vân tay. Các chứng chỉ được phân loại thành các lớp đảm bảo 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 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 họa cấu trúc tổng quát của một chứng chỉ VeriSign. Vấn đề khi nào và làm thế nào để trao đổi các chứng chỉ giữa máy khách và máy chủ sẽ lần lượt được trình bày trong những mục sau.

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.



Hình 2.1 Cấu trúc một chứng chỉ của VeriSign

Trình duyệt Internet của Microsoft (Microsoft Internet Explorer)

Internet Explorer cung cấp quyền bảo vệ máy khách trong các trình duyệt. Ngoài việc đưa ra các cảnh báo nhằm ngăn chặn không cho trẻ em truy nhập vào các site không lành mạnh, Internet Explorer còn đối phó lại các nội dung động dựa vào Java

và ActiveX. Internet Explorer sử dụng kỹ thuật mã xác thực (*Authenticode*) của Microsoft để kiểm tra nhận dạng của các nội dung động 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 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 nội dung động, 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 nội dung động từ các công ty cá nhân hay không.

Nếu bạn định tải về một trang Web có chứa nội dung động, nhưng nội dung động này chưa được ký, sẽ xuất hiện một hộp thoại chỉ báo rằng ở đây không có chứng chỉ hợp lệ. Việc Internet Explorer cố 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 sẽ quyết định Internet Explorer quản lý các chương trình và các tệp mà nó tải xuống như thế nào, phụ thuộc vào nguồn gốc

các tệp. 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 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: thấp (*Low*), trung bình thấp (*Medium-Low*), trung bình (*Medium*), cao (*High*).

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 tùy 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 nội dung động xuống máy tính của bạn. Nếu bạn cho phép Netscape Navigator tải xuống nội dung động, 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. Bạn có thể 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 nội dung động viết bằng Java và JavaScript, bạn sẽ thường xuyên nhận được một thông báo từ Netscape Navigator. Thông báo cho biết nội dung động đã được ký hay chưa, cho phép bạn xem chúng chỉ đi kèm để xác định nên chấp nhận hay từ chối tải xuống các nội dung động.

Lưu ý rằng, Netscape Navigator đánh giá rủi ro cao. Khi nhấn vào "Details" trên khung cảnh báo an toàn, bạn 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 nội dung động) 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 tùy 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 gọi 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 tùy 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 tệp dữ liệu chống virus hiện thời. Các tệp 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 tệp dữ liệu chống virus một cách định kỳ, nhờ vậy mới có thể phát hiện và loại trừ các virus mới nhất.

2.5 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 tức cố gắng truy nhập vào một hệ thống máy tính thông qua các kênh truyền thông không an toàn. 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 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 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

Một khi bạn không ngăn chặn được đối tượng nghe trộm đánh hơi (một kiểu tấn công trên Internet), công việc kinh doanh phải sử dụng các kỹ thuật nhằm ngăn chặn đối tượng nghe trộm biết được 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 nguy trang ký. Nguy trang ký làm cho mật 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 bit, 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.

Chương trình chuyển đổi văn bản rõ sang văn bản mã 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 chủ định, chương trình giải mã sẽ chuyển đổi văn bản mã thành văn bản rõ ban đầu. 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 số các thuật toán này là bất hợp pháp. Điều này đã ảnh hưởng đến một số công ty của 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) đã 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 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 hoặc thuật toán 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 thì các thông báo sẽ khó bị phát hiện.

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

- Mã băm
- Mã hoá đối xứng
- Mã hoá phi đối xứng

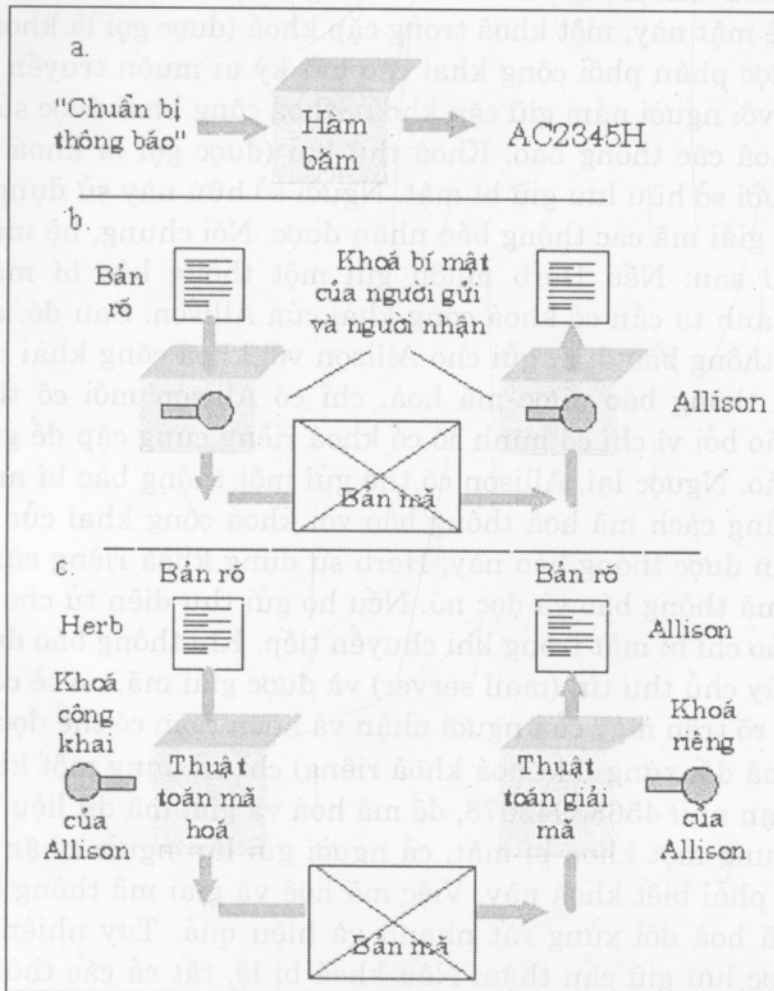
Mã băm là một quá trình sử dụng thuật toán băm để tính toán một số, được gọi là giá trị băm, từ một thông báo có độ dài bất kỳ. Nó chính là "dấu vân tay" của một thông báo vì nó gần như duy nhất đối với mỗi thông báo. Do sinh ra các thuật toán băm chất lượng tốt, khả năng xảy ra tình trạng hai thông báo khác nhau có cùng kết quả băm là vô cùng nhỏ. Mã hoá kết quả 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.

Với mã hoá phi đối xứng (mã hoá khoá công khai), việc mã hoá và giải mã các thông báo được thực hiện bằng cách sử dụng một cặp khoá. Năm 1977, Ronald Rivest, Adi Shamir và Leonard Adleman đã phát minh ra hệ mật khoá công khai RSA (lấy các chữ cái đầu tiên trong tên của các tác giả đặt tên cho thuật toán). Trong hệ mật này, một khoá trong cặp khoá (được gọi là khoá công khai) được phân phối công khai cho bất kỳ ai muốn truyền thông an toàn với người nắm giữ cặp khoá. Khoá công khai được sử dụng để mã hoá các thông báo. Khoá thứ hai (được gọi là khoá riêng) được người sở hữu lưu giữ bí mật. Người sở hữu này sử dụng khoá riêng để giải mã các thông báo nhận được. Nói chung, hệ mật làm việc như sau: Nếu Herb muốn gửi một thông báo bí mật cho Allison, anh ta cần có khoá công khai của Allison. Sau đó, anh ta mã hoá thông báo định gửi cho Allison với khoá công khai của cô. Một khi thông báo được mã hoá, chỉ có Allison mới có thể đọc thông báo bởi vì chỉ có mình cô có khoá riêng cùng cặp để giải mã thông báo. Ngược lại, Allison có thể gửi một thông báo bí mật cho Herb, bằng cách mã hoá thông báo với khoá công khai của Herb. Khi nhận được thông báo này, Herb sử dụng khoá riêng cùng cặp 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 về từ máy chủ thư tín (mail server) và được giải mã, nó sẽ có dạng văn bản rõ trên máy của người nhận và hoàn toàn có thể đọc được.

Mã hoá đối xứng (Mã hoá khoá riêng) chỉ sử dụng một khoá số, chẳng hạn như 45683942078, để mã hoá và giải mã dữ liệu. Do sử dụng chung một khoá bí mật, cả người gửi lẫn người nhận thông báo đều phải biết khoá này. 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_N^2 khoá bí mật, chẳng hạn với 12 người muốn truyền thông với nhau, chúng ta cần 66 khoá bí mật.



Hình 2.2 (a) Mã bầm, (b) Mã hoá khoá riêng, (c) Mã hoá khoá công khai.

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 để mã hoá các thông tin nhạy cảm hoặc thông tin thương mại và nó được sử dụng rộng rãi nhất. Tuy nhiên, kích cỡ khoá 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 hơn là không thể.

Hệ mật khoá công khai có một số thuận lợi so với hệ mật khoá 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 hệ mật khoá đối xứng tương ứng. 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, hệ mật 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. Có nghĩa là, 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. Hệ mật 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 hệ mật 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 hệ mật khoá đối xứng bằng hệ mật khoá công khai. Chúng bổ sung lẫn nhau. Hệ mật khoá công khai được sử dụng để trao đổi khoá bí mật 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. Thông thường, các máy chủ thương mại an toàn dần 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 dần 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 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 yếu khác nhau, một số thuật toán đã cũ và không còn phù hợp với việc sử dụng và các đơn vị xử lý trung tâm tốc độ cao hiện nay. Kiểu thứ 3 được gọi là Digest (Hash). Các thuật toán Digest không mã hoá các thông tin. Thay vào đó, chúng tính toán độ dài cố định cho một thông báo, thường là 128 bit, đây chính là chữ ký của thông báo (hay tóm lược nội dung 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.

Giao thức Tầng Socket an toàn (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.

SSL và S-HTTP có các mục tiêu khác nhau. SSL đảm bảo kết nối giữa hai máy tính, S-HTTP gửi các thông báo an toàn, nhưng với cả hai, việc mã hoá các thông báo gửi đi và giải mã các thông

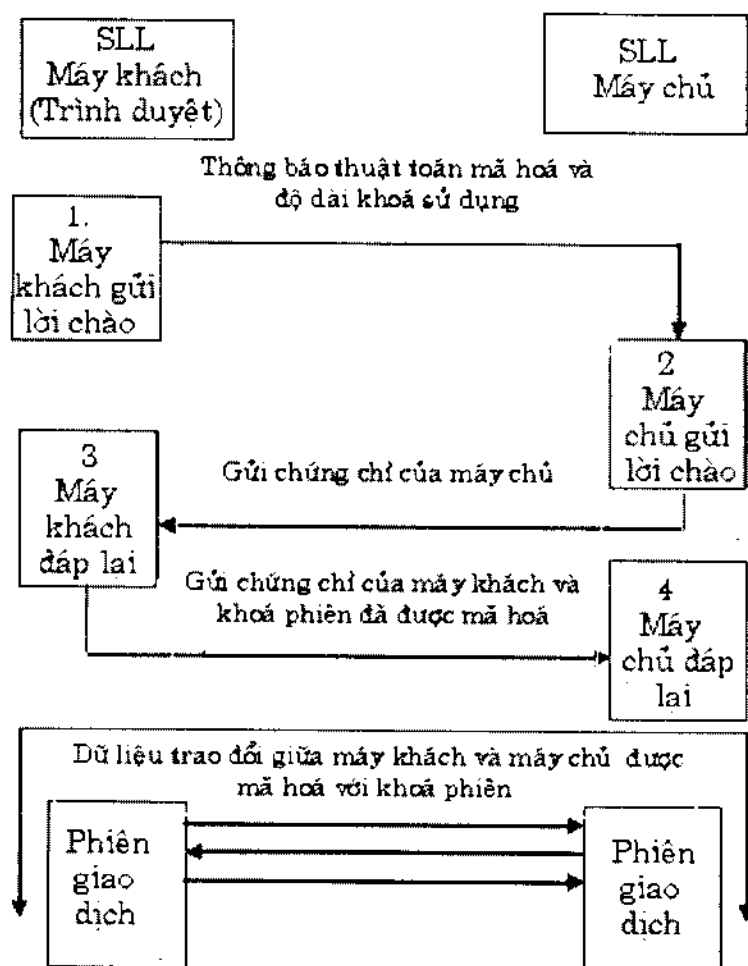
báo nhận được diễn ra tự động và trong suốt với người sử dụng. SSL làm việc ở tầng vận tải, còn S-HTTP làm việc ở tầng ứng dụng.

SSL cung cấp một thủ tục bắt tay an toàn (thoả thuận ban đầu, còn được gọi là thủ tục *handshake*), 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 phải luôn nhận diện được máy kia. Các máy khách và máy chủ nên có chứng chỉ hợp lệ khi tiến hành trao đổi thông tin. Sau khi nhận diện, 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 thông tin nhưng 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 sung thêm cho HTTP. Ví dụ, SSL có thể đảm bảo các phiên FTP, cho phép đưa lên hoặc tải xuống 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 chủ 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 chỉ báo 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 *https://www.amazon.com*, lập tức bạn thiết lập được một liên kết an toàn với Amazon.com.

SSL có hai độ dài là 40 bit và 128 bit. Đây chính là độ dài của khoá phiên được sinh ra cho mỗi giao dịch có mã hoá. Thuật toán

mã hoá sử dụng khoá phiên để tạo ra bản mã (từ 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 bit. 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.



Hình 2.3 Thiết lập một phiên SSL

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 và mã hoá mọi cuộc truyền thông giữa 2 máy tính. Khi trình duyệt của một máy khách đến một Web site của một máy chủ tin cậy, hai máy tiến hành trao đổi 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: "Hãy 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.

Máy khách và máy chủ thoả thuận rằng mọi trao đổi phải được giữ bí mật, vì những thông tin được truyền đi trên Internet bao gồm số thẻ tín dụng, số hoá đơn và các mã kiểm tra. Để đảm bảo bí mật, SSL sử dụng mã hoá khoá công khai (mã hoá phi đối xứng) và mã hoá khoá riêng (mã hoá đối xứng). Mã hoá khoá công khai dễ sử dụng nhưng chậm hơn rất nhiều so với mã hoá đối xứng. Đó chính là lý do tại sao SSL sử dụng mã hoá đối xứng cho hầu hết các cuộc truyền thông an toàn của mình. Máy khách và máy chủ trao đổi khoá phiên 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 phiên cho cả hai. Sau đó, trình duyệt mã hoá khoá phiên 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 phiên được mã hoá, trình duyệt gửi nó cho máy chủ. Ngược lại, máy chủ sử dụng khoá riêng của mình để giải mã và tìm ra khoá phiên. Tất cả các thông báo giữa máy khách và máy chủ được mã hoá với 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 tin cậy) lại bắt đầu tương tự. Tuỳ thuộc vào những gì đã thoả thuận, máy khách và máy chủ có thể sử dụng mã 40 bit hoặc 128 bit. Thuật toán mã

hoá có thể là DES, hoặc RAS.

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 sử dụng khoá phiên 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 truyền siêu văn bản an toàn (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/dáp 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 bí mật (khóa đối xứng), trong khi đó máy chủ có thể yêu cầu xác thực máy khách bằng cách sử dụng các kỹ thuật mật mã khóa 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 "Yêu cầu" (*Required*), "Tuỳ chọn" (*Optional*) hoặc "Từ chối" (*Refused*). Khi một thành viên quy định rằng đặc tính an toàn riêng là "Yêu cầu", 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 tư lự 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 đã sử dụng chữ ký số.

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 phần đầu (*header*) của gói đặc biệt. Header định nghĩa kiểu kỹ thuật an toàn, cụ thể là mã hoá đối xứng, 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 tùy 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.

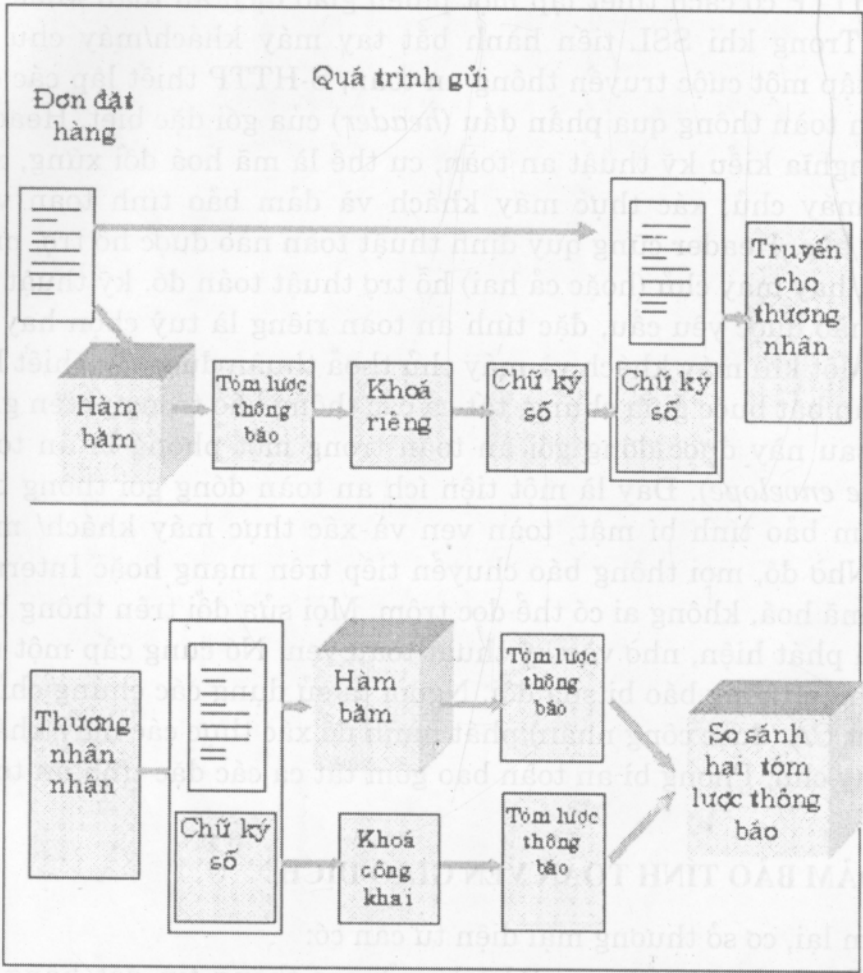
2.6 ĐẢM BẢO TÍNH TOÀN VỆ GIAO DỊCH

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

- Trình duyệt của máy khách: gửi các thông tin 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 thông tin 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.



Hình 2.4 *Quá trình gửi và nhận một thông báo*

Cần kết hợp các kỹ thuật để tạo ra thông báo có khả năng chống trộm 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: tạo ra tóm lược thông báo (xác định duy nhất thông báo) mà không thể chuyển ngược lại thông báo ban đầu, thuật toán và các tham số của hàm băm được công khai và các va chạm 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 nhân 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 thương nhân. Thương nhân 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 nhân 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 với khoá riêng của mình.

Chữ ký số chính là tóm lược thông báo được mã hoá. Đơn đặt hàng có đi kèm chữ ký số đảm bảo xác thực người gửi và thông báo không bị sửa đổi. Một chữ ký cung cấp tính toàn vẹn thông báo và xác thực người gửi như thế nào? Khi tóm lược thông báo được mã hoá bằng cách sử dụng các kỹ thuật khoá công khai, có nghĩa là chỉ chỉ có người gửi có khoá riêng để mã hoá tóm lược thông báo. Khi thương nhân giải mã chữ ký số bằng khoá công khai của người gửi, 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 cả về nội dung (thông báo không bị sửa đổi trên đường

truyền) và nguồn gốc (xác thực người gửi) thông báo. Điều này giải quyết vấn đề làm giả. Nếu cần, cả hai thành viên có thể thoả thuận giữ bí mật giao dịch, bổ sung thêm vào việc đảm bảo toàn vẹn và xác thực mà chữ ký số đã cung cấp. Đơn giản, chỉ cần mã hoá toàn bộ chữ ký số và thông báo với khoá công khai của người nhận, nhằm đảm bảo tính bí mật thông báo. Việc kết hợp sử dụng mã hoá khoá công khai và chữ ký số đảm bảo an toàn cho các cuộc giao dịch trên Internet. Hình 2.4 minh hoạ một thông báo và chữ ký số 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 việc sử dụng nhiều 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 có thể 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.

Mã hoá hoặc các chữ ký số có thể bảo vệ các gói thông tin, tránh bị trộm cắp hoặc sửa đổi. 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 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.

2.7 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 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 được phép 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 kiểm tra chữ ký số (có trong chứng chỉ) bằng cách sử dụng khoá công khai của người phát hành chứng chỉ, 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 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 sung, 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 thu tín.

Nhiều hệ thống máy chủ Web lưu giữ tên người sử dụng và mật khẩu trong một tệp. 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 (ACL). ACL là một danh sách hoặc cơ sở dữ liệu, các tài nguyên, tên của người có thể truy nhập vào các tệp hoặc các tài nguyên khác. Mỗi tệp có một danh sách kiểm soát truy nhập riêng. Bất cứ khi nào máy khách yêu cầu máy chủ Web truy nhập vào một tệp hoặc một tài liệu (có định trước cấu hình yêu cầu kiểm tra truy nhập), máy chủ Web sẽ kiểm tra ACL của 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. 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 dọa). 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 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:

- *Bức tường lửa lọc gói (Packet filter firewall)* 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.

- *Bức tường lửa máy chủ cổng nối (Gateway server firewall)* được sử dụng để lọc các luồng thông tin, tùy thuộc vào ứng dụng mà chúng yêu cầu. Nó 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. Nó cung cấp một điểm trung tâm, tất cả các yêu cầu được phân loại, ghi lại và phân tích tại điểm này.

- *Bức tường lửa máy chủ uỷ quyền (Proxy server firewall)* 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).

2.8 TÓM TẮT

Trong chương này, chúng ta đã xem xét 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. Ba 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 để đảm bảo bí mật thông tin, có hai loại mã hoá được trình bày ở trên là mã hoá khoá công khai (mã hoá phi đối xứng) và mã hoá khoá riêng (mã hoá đối xứng). Mã hoá khoá công khai giải quyết được vấn đề phân phối khoá, nhưng thời gian xử lý của nó chậm hơn rất nhiều so với mã hoá khoá riêng. Mã hoá khoá riêng được sử dụng trong hầu hết các phiên giao dịch, 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 đảm bảo tính toàn vẹn thông báo và xác thực người dùng. Một thành viên thứ ba tin cậy (CA) phát hành 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 tin an toàn trên Internet. Cuối cùng là máy chủ thương mại, cũng giống với máy khách, nó cần 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 III

MỘT SỐ KỸ THUẬT AN TOÀN CHO THƯƠNG MẠI ĐIỆN TỬ

3.1 MÃ HOÁ ĐỐI XỨNG

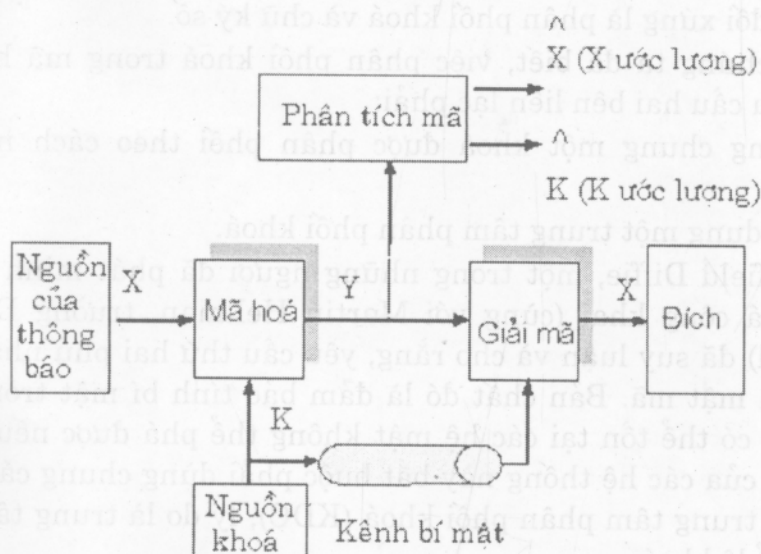
Trong mã hoá đối xứng, bản rõ (dạng văn bản ban đầu có thể hiểu được) được chuyển thành bản mã (dạng văn bản vô nghĩa khó hiểu). Quá trình mã hoá sử dụng một thuật toán và một khoá. Khoá là một giá trị không phụ thuộc vào bản rõ. Đầu ra của thuật toán phụ thuộc vào khoá xác định (đây chính là khoá đang 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 được biến đổi trở lại dạng bản rõ ban đầu nhờ một thuật toán giải mã, thuật toán này sử dụng cùng một khoá như đã được sử dụng khi mã hoá.

Độ an toàn của mã hoá đối xứng 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 chip thuật toán mã giá thành thấp. Các chip 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.

Hãy quan sát kỹ các yếu tố cơ bản của lược đồ mã hoá đối xứng trong hình 3.1. Nguồn A tạo ra một thông báo ở dạng rõ, $X = \{X_1, X_2, \dots, X_M\}$. 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 $K = \{K_1, K_2, \dots, K_l\}$ được sinh ra. 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.



Hình 3.1 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 $Y = \{Y_1, Y_2, \dots, Y_N\}$. Chúng ta có thể viết như sau:

$$Y = E_K(X)$$

Khi người nhận hợp pháp nhận được bản mã 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 MÃ HOÁ KHOÁ CÔNG KHAI

3.2.1 Các nguyên lý của các hệ mật khoá công khai

Mã hoá khoá công khai giải quyết hai vấn đề khó khăn trong mã hoá đối xứng là phân phối khoá và chữ ký số.

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

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 mật 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.

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.

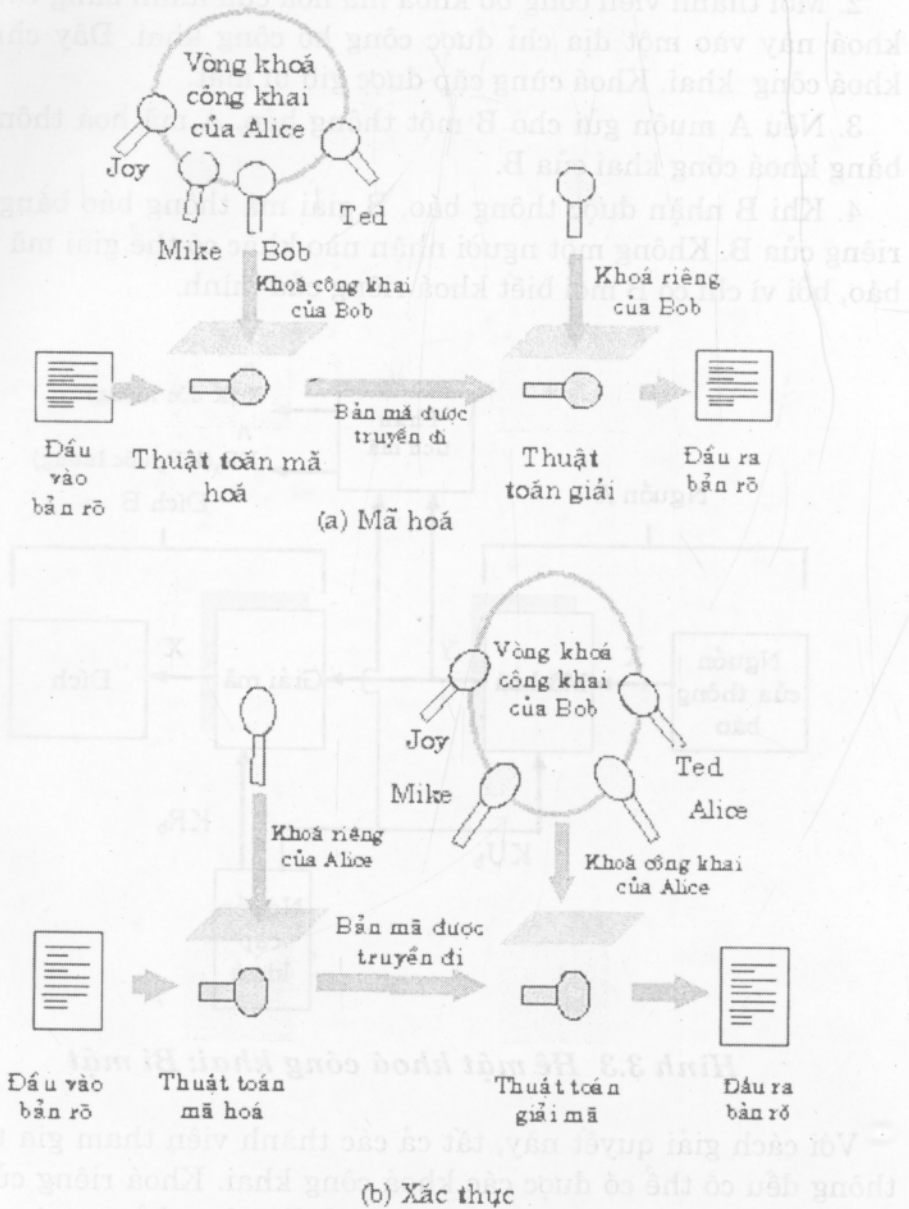
Các hệ mật khoá công khai

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 3.2 Mã hoá khoá công khai

Hình 3.2 minh hoạ quá trình mã hoá khoá công khai. Các bước

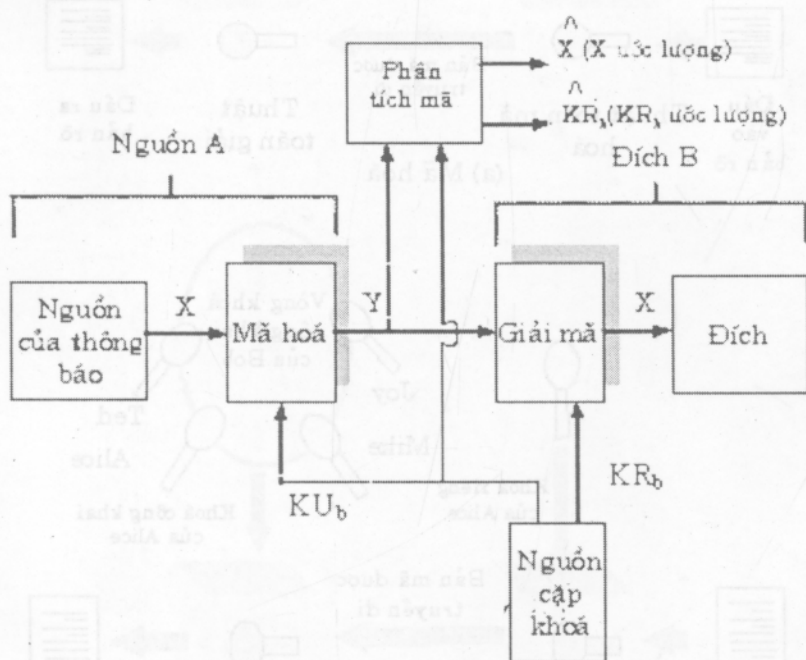
cơ bản gồm:

1. Mỗi thành viên sinh ra một cặp khóa, cặp khóa 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 khóa này vào một địa chỉ được công bố công khai. Đây chính là khóa công khai. Khóa cùng cặp được giữ bí mật.

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

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



Hình 3.3 Hệ mật 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 khóa công khai. Khóa riêng của mỗi thành viên được giữ bí mật. Quá trình liên lạc chỉ an toàn chừng nào khóa riêng còn được giữ bí mật. Mỗi thành viên có thể thay đổi các khóa riêng của mình 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 đặc điểm quan trọng của mã hoá khoá công khai và mã hoá đối xứng. Để phân biệt chúng, 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.

Chúng ta xem xét chi tiết các yếu tố cần thiết trong lược đồ mã hoá khoá công khai (hình 3.3).

Nguồn A đưa ra một thông báo rõ và bản rõ của thông báo là $X = [X_1, X_2, \dots, X_M]$. Các phần tử X_i ($i = 1 \div M$) của X là các chữ cái trong bảng chữ cái hữu hạn nào đó. 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.

Bảng 3.1 Mã hoá khoá công khai và mã đối xứng

Mã hoá đối xứng	Mã hoá khoá công khai
<i>Các yêu cầu khi sử dụng</i> 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.	<i>Các yêu cầu khi sử dụng</i> 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.
<i>Các yêu cầu an toàn</i> 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.	<i>Các yêu cầu an toàn</i> 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.

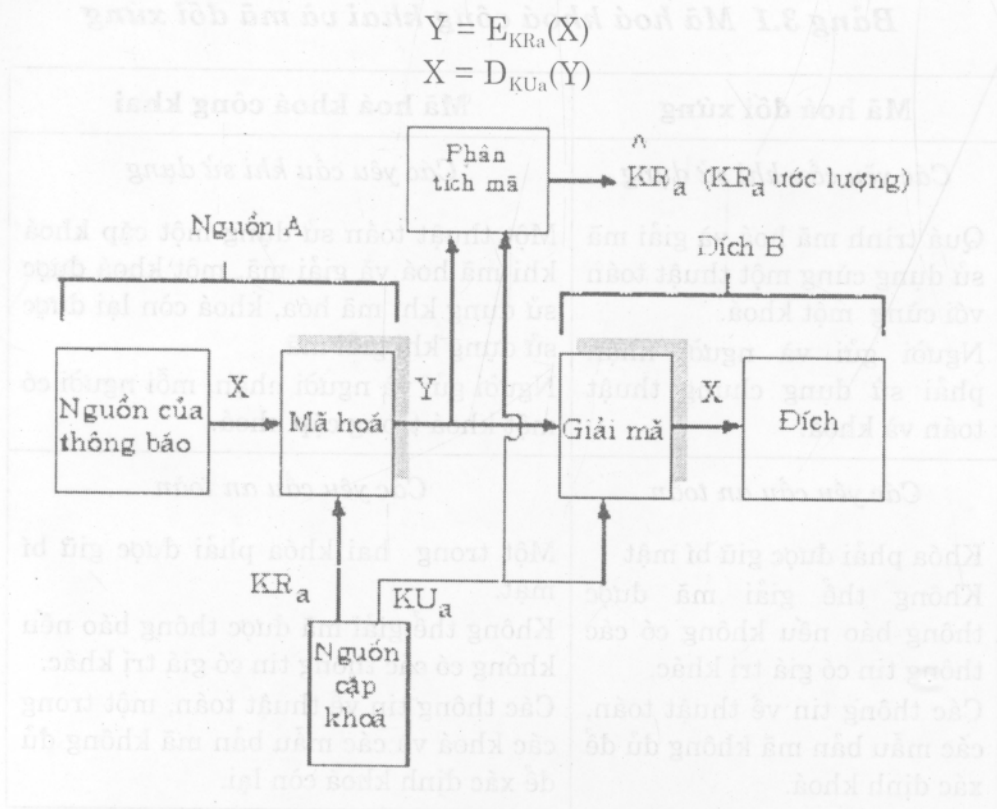
Với đầu vào là thông báo X và khoá mã hoá KU_b , A tạo ra một

bản mã $Y = [Y_1, Y_2, \dots, Y_N]$ với $Y = E_{K_{Ub}}(X)$.

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

Đối phương (có thể có được Y và K_{Ub} nhưng không có K_{Rb} hoặc X) phải tìm cách khôi phục lại X và/hoặc K_{Rb} . Giả sử rằng, anh ta có các thông tin về thuật toán mã hoá (E) và giải mã (D), anh ta 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 K_{Rb} bằng cách sinh ra một K_{Rb} ước lượng.

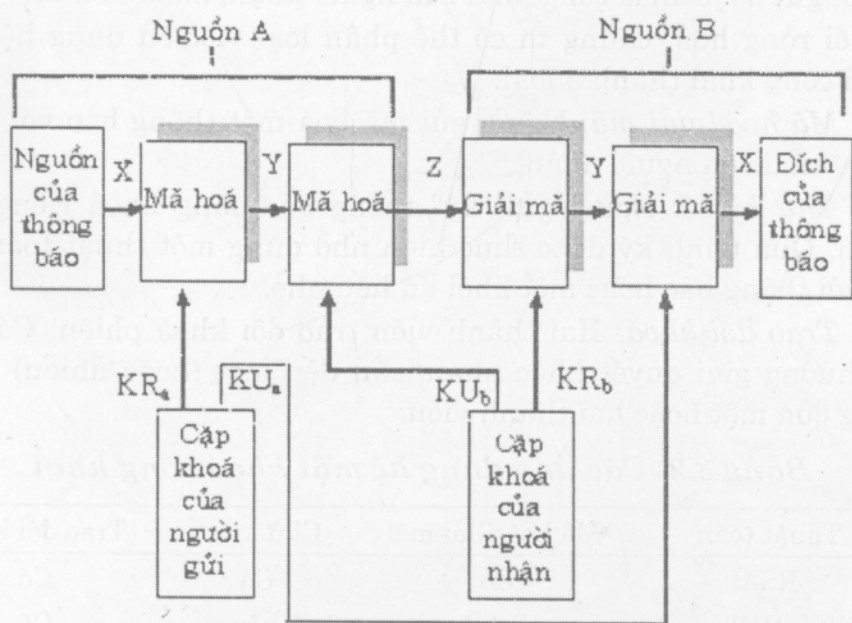
Chúng ta đã biết, một trong hai khoá trong cặp khoá có thể được sử dụng để mã hoá, khoá còn lại được sử dụng để giải mã. Điều này cho phép thực hiện một lược đồ mã hơi khác một chút. Lược đồ được minh hoạ trong hình 3.3 cung cấp tính bí mật. Hình 3.2b và 3.4 minh hoạ việc sử dụng mã hoá khoá công khai cho xác thực:



Hình 3.4 Hệ mật khoá công khai: Xác thực

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, 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.



Hình 3.5 Hệ mật khoá công khai: Bí mật và xác thực

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

$$Z = E_{K_{Ub}} [E_{K_{Ra}}(X)]$$

$$X = D_{K_{Ua}} [D_{K_{Rb}}(Z)]$$

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 mật khoá công khai

Trước tiên, chúng ta cần làm rõ một khía cạnh của các hệ mật 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 mật khoá công khai.

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

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

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

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

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

Bảng 3.2 Các ứng dụng hệ mật khoá công khai

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

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.

Các yêu cầu đối với hệ mật khoá công khai

Hệ mật được minh hoạ trong hình 3.3, 3.5 phụ thuộc vào một thuật toán 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. Người nhận 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 của người nhận, mã hoá thông báo M và tạo ra một bản mã tương ứng:

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

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

$$M = D_{KR_b}(C) = D_{KR_b}[E_{KU_b}(M)]$$

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 sung 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:

$$M = E_{KU_b}[D_{KR_b}(M)]$$

Ở đây có một vài yêu cầu khắt khe (đã kiểm nghiệm trong thực tế). Ví dụ, các yêu cầu cần đáp ứng hàm của 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.

$$Y = f(X) \text{ dễ dàng}$$

$$X = f^{-1}(Y) \text{ không thể}$$

Chúng ta tiếp tục với định nghĩa hàm của 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 của sập một chiều là họ các hàm nghịch đảo f_k , sao cho:

$$Y = f_k(X) \text{ dễ dàng, nếu biết } k \text{ và } X$$

$X = f^{-1}_k(Y)$ 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 của 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:

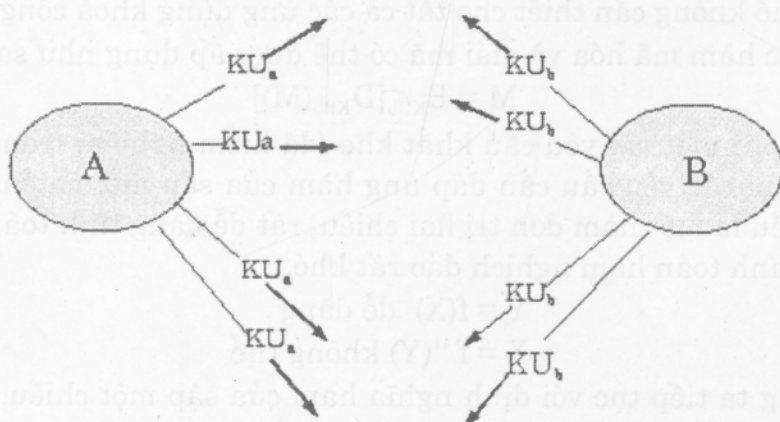
- Phân phối các khoá công khai.
- Sử dụng mã hoá khoá công khai để phân phối các khoá bí mật.

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
- Trung tâm quản lý khoá công khai
- Các chứng chỉ khoá công khai



Hình 3.6 Phân phối khoá công khai không kiểm soát

Khai báo công khai các khoá công khai

Xuất phát điểm của mã hoá khoá công khai là khoá công khai

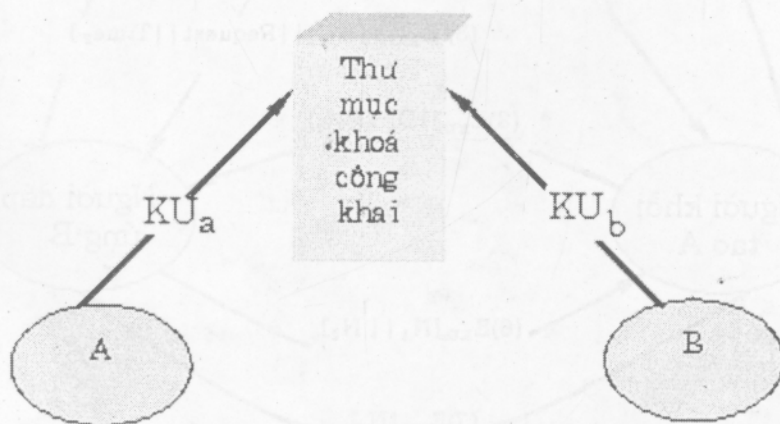
được công bố công khai. Do vậy, nếu có một thuật toán được chấp nhận rộng rãi, chẳng hạn như RSA, bất kỳ thành viên nào cũng có thể gửi khoá công khai của mình cho thành viên khác hoặc quảng bá cho cộng đồng lớn (hình 3.6).

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.

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 3.7).



Hình 3.7 Công bố khoá công khai

Một lược đồ như vậy gồm các yếu tố sau:

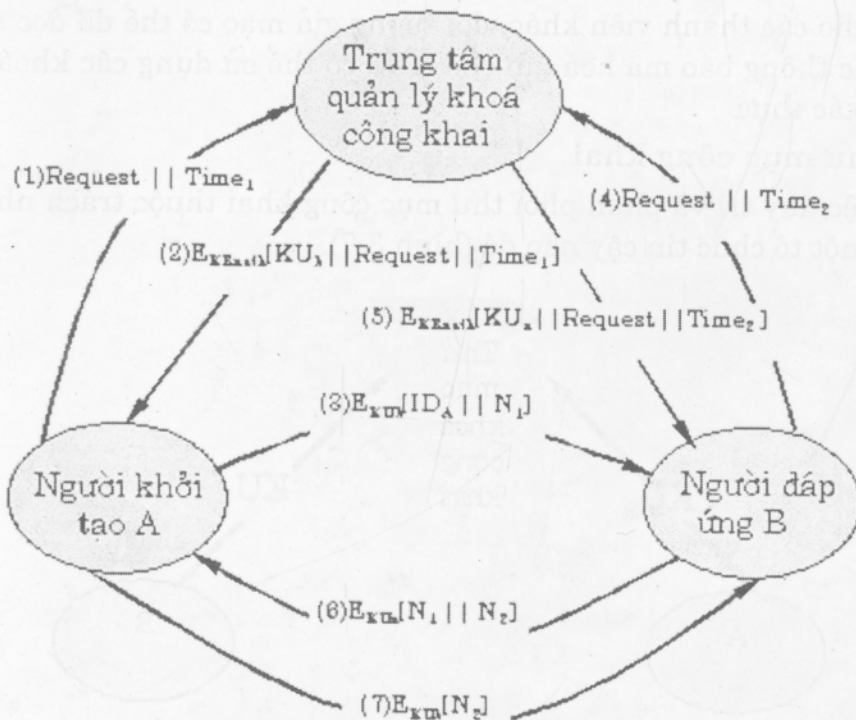
1. Cơ quan quản lý duy trì một thư mục, mỗi thành viên có một entry {tên, khoá công khai} trong thư mục.

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

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

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

5. 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.



Hình 3.8 *Lược đồ phân phối khoá công khai*

Trung tâm 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 3.8).

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

Quá trình trao đổi thông tin bí mật xảy ra như sau:

1. 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.

2. 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.

3. 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 giá trị (được gọi là nonce) N_1 được sử dụng để nhận dạng giao dịch này.

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

5. 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 sung thêm (tuỳ chọn):

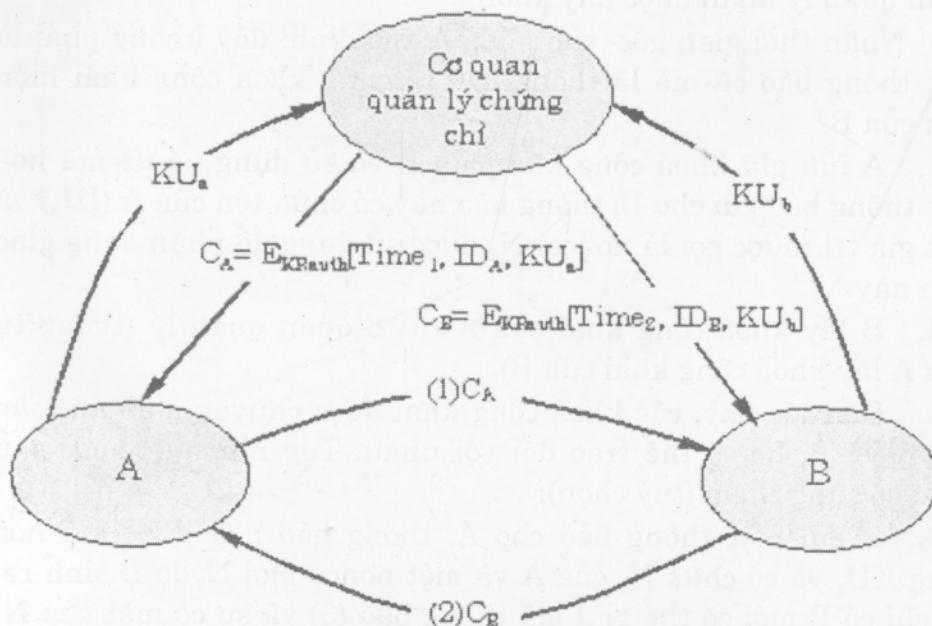
6. B gửi một thông báo cho A, thông báo này được mã hoá bằng KU_a và có chứa N_1 của A và một nonce mới N_2 do B sinh ra. Do chỉ có B mới có thể giải mã thông báo (3) và sự có mặt của N_1 trong thông báo (6) đảm bảo với A rằng B chính là người A đang liên lạc.

7. 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 3.8 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. 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.



Hình 3.9 Trao đổi các chứng chỉ khoá công khai

Chúng ta có thể đưa vào lược đồ này các yêu cầu 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.
4. Và một yêu cầu được bổ sung thêm như sau:

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

Hình 3.9 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:

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

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:

$$DKU_{auth}[C_A] = D_{KU_{auth}}[E_{KR_{auth}}[T, ID_A, KU_a]] = (T, ID_A, KU_a)$$

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.

Nhân 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.

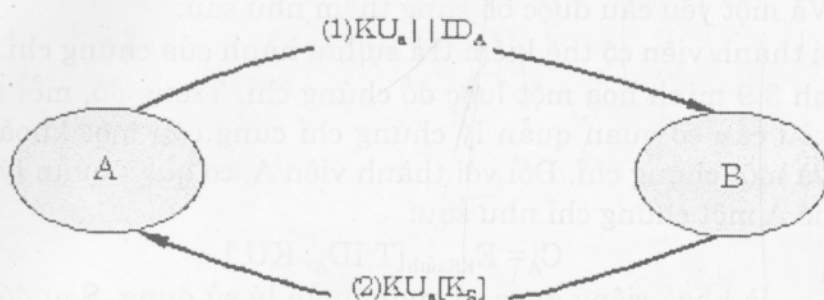
Việc làm lộ khoá riêng được so sánh với việc mất một thẻ tín dụng. Người chủ sở hữu huỷ bỏ số thẻ tín dụng, nhưng vẫn có thể xảy ra rủi ro cho đến khi tất cả những người liên lạc nhận thức được- thẻ tín dụng cũ không được sử dụng nữa. Nhân thời gian chỉ ra thời hạn kết thúc.

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

Mã hoá 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 3.10).



Hình 3.10 Sử dụng mã hoá khoá công khai để thiết lập một khoá phiên

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

1. 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).
2. B tạo ra khoá bí mật (K_s) và truyền cho A. Khoá được mã bằng khoá công khai của A.
3. A tính toán $D_{KR_a}[E_{KU_a}[K_s]]$ để khôi phục lại khoá bí mật. Chỉ A mới có thể giải mã thông báo. Chỉ A và B biết được K_s .
4. 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 hoá 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:

1. 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).

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

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

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

5. E truyền $E_{KU_a}[K_s]$ 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 3.11) 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.

Các bước tiếp theo xảy ra như sau:

1. 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).

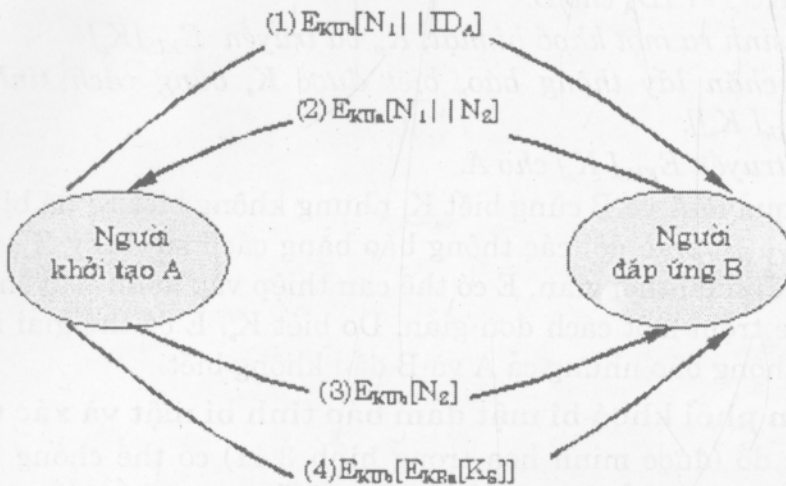
2. B gửi thông báo (2) cho A. Thông báo được mã hoá bằng KU_a . Nó có chứa N_1 của A và một nonce mới N_2 do B sinh ra. Do chỉ có B mới có thể giải mã thông báo (1), sự xuất hiện của N_1 trong thông báo (2) đảm bảo rằng A đang liên lạc với B.

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

4. A chọn một khoá bí mật K_s và gửi thông báo (3) $M = E_{KU_B}[E_{KR_A}[K_s]]$ 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.

5. B tính toán $D_{K_{Ub}}[D_{K_{Rb}}[M]]$ 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 3.8. Kết quả mà lược đồ này mang lại là đảm bảo tính tin cậy và xác thực trong trao đổi khoá bí mật.



Hình 3.11 Sử dụng mã hoá khoá công khai để trao đổi khoá bí mật

Một lược đồ kết hợp

Có cách khác sử dụng mã hoá khoá công khai để phân phối khoá bí mật là sử dụng lược đồ kết hợp. Lược đồ này duy trì một trung tâm phân phối khoá, viết tắt là KDC. Trung tâm này có chung một khoá chủ với từng người sử dụng và phân phối các khoá phiên. Các khoá phiên 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 sử dụng mã hoá khoá công khai có thể làm giảm hiệu năng của toàn bộ hệ thống, do thời gian tính toán mã hoá và giải mã rất lớn. Mã hoá khoá công khai có thể

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 BẮM

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:

1. *Khám phá (Disclosure)*: các nội dung của thông báo.

2. *Phân tích lưu lượng thông tin (Traffic analysis)*: Phát hiện lưu lượng 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.

3. *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.

4. *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.

5. *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.

6. *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 có thể bị làm trễ hoặc chuyển tiếp nhiều lần.

7. *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 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 3.12 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.

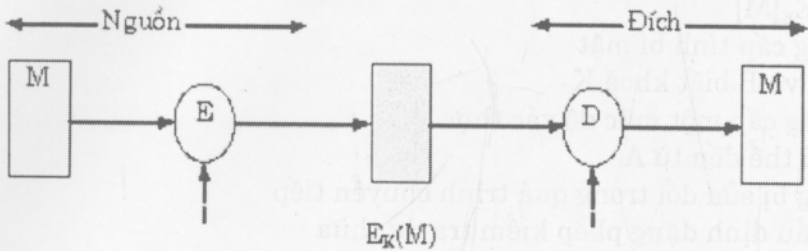
Trong mã hoá đối xứng, thông báo đi từ nguồn A đến đích B được mã hoá, bằng cách sử dụng một khoá bí mật K giữa A và B.

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.

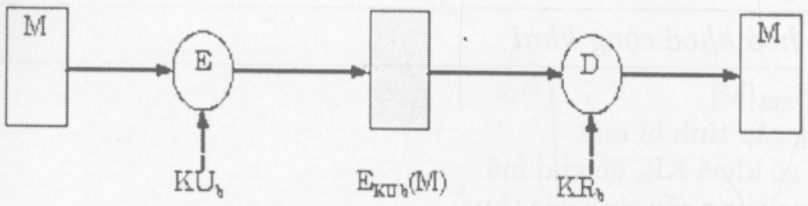
Mã hoá đối xứng cũng cung cấp tính xác thực. Tuy nhiên, điều này cũng cần được xem xét cẩn thận. Chúng ta quan sát những gì xảy ra ở đích B. Biết trước hàm giải mã D và khoá bí mật K, với một đầu vào X bất kỳ, chúng ta có đầu ra như sau: $Y = D_K(X)$. Nếu X là bản mã của thông báo gốc M thì đầu ra Y 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

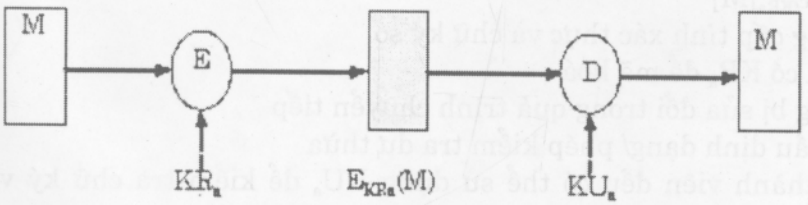
đích B để mã hoá thông báo M. Do B có khoá riêng tương ứng (KR_b) nên chỉ B mới có thể giải mã thông báo. Lược đồ này không cung cấp tính xác thực, bởi vì bất kỳ người nào cũng có thể sử dụng khoá công khai của B để mã hoá thông báo, tự nhận mình là A.



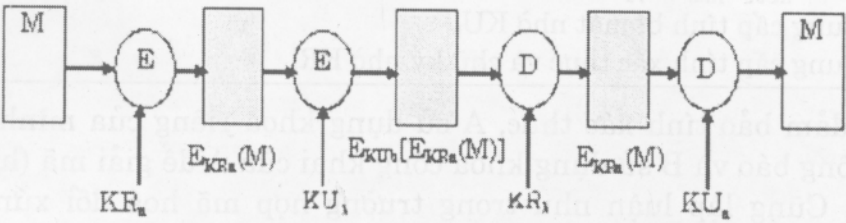
(a) Mã hoá đối xứng: bí mật và xác thực



(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 3.12 Các dạng sử dụng mã hoá thông báo cơ bản

Bảng 3.3 *Mối quan hệ mật thiết giữa tính bí mật và xác thực trong mã hoá thông báo**(a) Mã hoá đối xứng* $A \rightarrow B: E_K[M]$

- ◆ Cung cấp tính bí mật
- Chỉ A và B biết 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 $A \rightarrow B: E_{KU_b}[M]$

- ◆ 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

 $A \rightarrow B: E_{KR_a}[M]$

- ◆ 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 và xem thông báo

 $A \rightarrow B: E_{KU_b}[E_{KR_a}(M)]$

- ◆ Cung cấp tính bí mật nhờ KU_b
- ◆ Cung cấp tính xác thực và chữ ký nhờ KR_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 3.12c). 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.

Giả sử có một cấu trúc như vậy thì lược đồ trong hình 3.12c 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

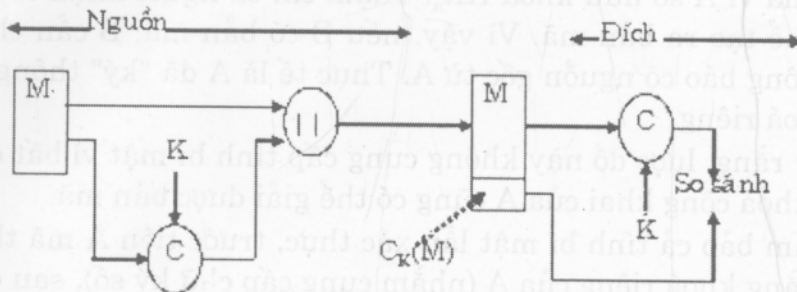
Một kỹ thuật xác thực (mang tính lựa chọn) như sau: sử dụng một khoá bí mật để tạo ra một khối dữ liệu nhỏ có kích thước cố định (được gọi là MAC, đây là các chữ cái đầu của *Message Authentication Code*, hay mã xác thực thông báo). MAC được gắn với thông báo.

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 3.13a). 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:

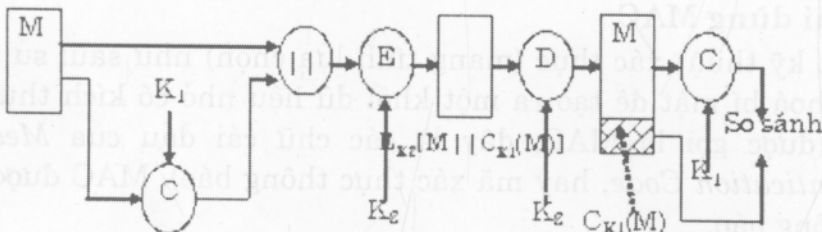
1. Người nhận được đảm bảo thông báo không bị sửa đổi. Nếu đối tượng tấn công sửa đổi thông báo nhưng không sửa đổi MAC, thì giá trị MAC mới (do người nhận tính toán) sẽ không trùng khớp với MAC đi kèm với thông báo. Do giả thiết đối tượng tấn công không biết khoá bí mật nên không thể sửa đổi MAC sao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

phù hợp với mọi sửa đổi trên thông báo.

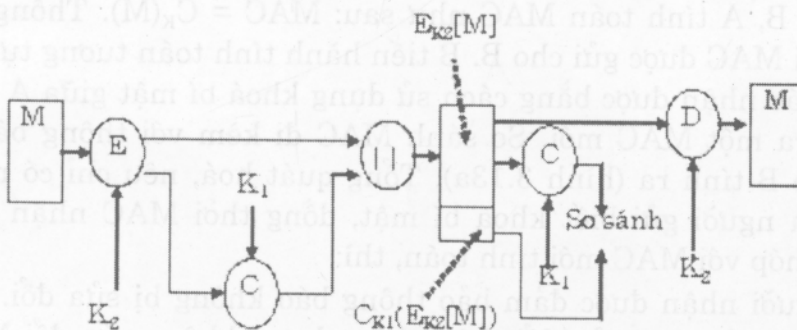
2. Người nhận được đảm bảo rằng thông báo có nguồn gốc từ người gửi hợp pháp. Do không ai khác (ngoài người gửi và người nhận chủ định) biết khoá bí mật, nên không ai có thể chuẩn bị thông báo với một MAC hợp lệ.



(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 3.13 Các dạng sử dụng MAC cơ bản

3. 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 khi tính toán MAC (minh hoạ trong hình 3.13b,c). Trong những trường hợp này, người nhận và người gửi cần có hai khoá.

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 rõ 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.

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 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 sung thêm ba lý do cơ bản như sau:

3. 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 (giao thức quản lý mạng đơn giản) 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.

4. 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.

5. 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.

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

Bảng 3.4 *Mối quan hệ mật thiết giữa tính bí mật và xác thực của các giải pháp trong hình 3.13*

(a) $A \rightarrow B: M \parallel C_K(M)$ ◆ Cung cấp tính xác thực - Chỉ A và B biết khoá K
(b) $A \rightarrow B: E_{K_2}[M \parallel C_{K_1}(M)]$ ◆ Cung cấp tính xác thực - Chỉ A và B biết khoá K_1 ◆ Cung cấp tính bí mật - Chỉ A và B biết khoá K_2
(c) $A \rightarrow B: E_{K_2}[M] \parallel C_{K_1}(E_{K_2}(M))$ ◆ Cung cấp tính xác thực - Sử dụng K_1 ◆ Cung cấp tính bí mật - Sử dụng K_2

Hàm băm (Hash Function)

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:

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.

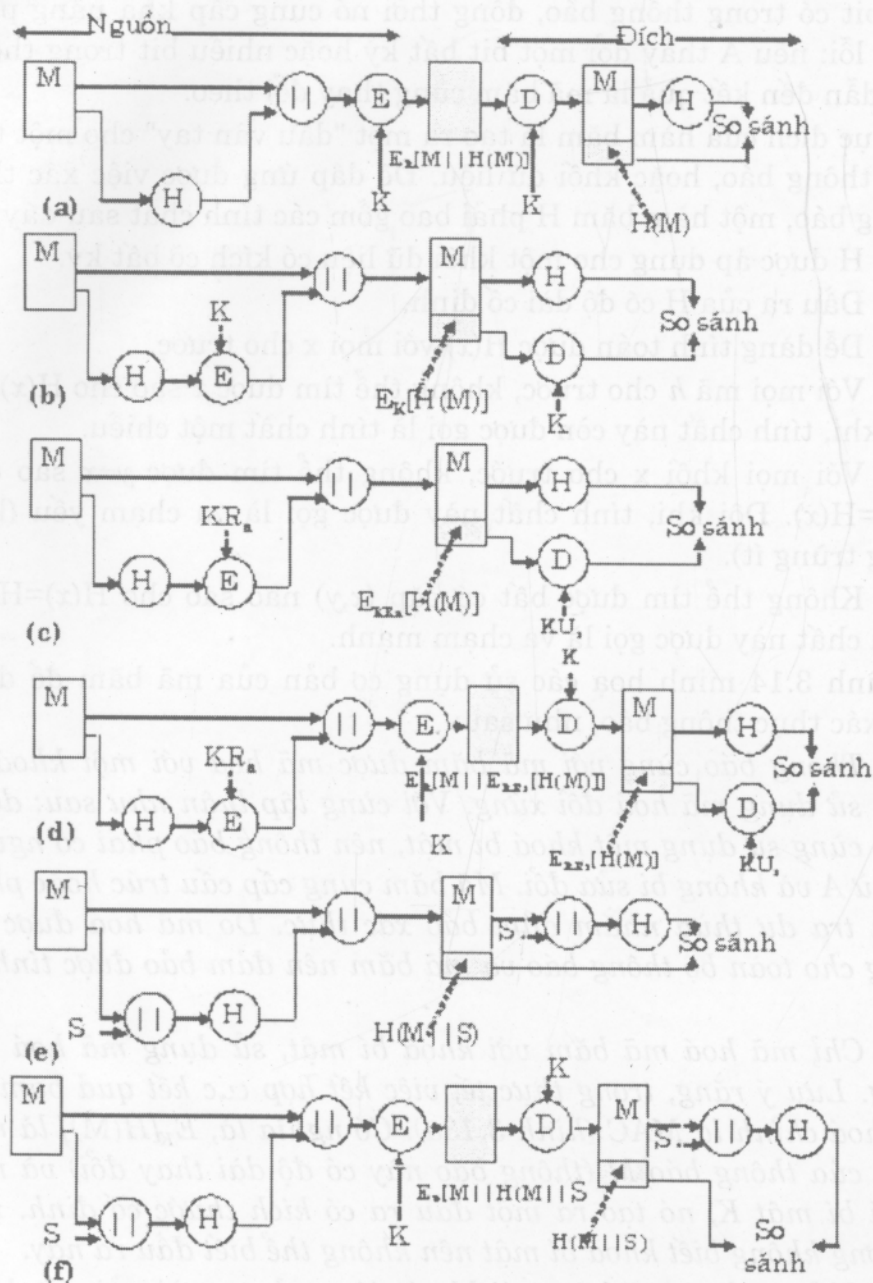
Hình 3.14 minh họa các sử dụng cơ bản của mã băm để đảm bảo xác thực thông báo, như sau:

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 3.13a). 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.



Hình 3.14 Các dạng sử dụng cơ bản của hàm băm

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 gán 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.

Bảng 3.5 *Mối quan hệ mật thiết giữa xác thực và bí mật trong các giải pháp được minh hoạ trong hình 3.14*

(a) $A \rightarrow B: E_K[M \parallel H(M)]$ ♦ Cung cấp tính bí mật - Chỉ A và B biết khoá K ♦ Cung cấp xác thực - H(M) được bảo vệ	(d) $A \rightarrow B: E_K[M \parallel E_{KRa}[H(M)]]$ ♦ Cung cấp xác thực và chữ ký số ♦ Cung cấp tính bí mật - Chỉ A và B biết khoá K
(b) $A \rightarrow B: M \parallel E_K[H(M)]$ ♦ Cung cấp xác thực - H(M) được bảo vệ	(e) $A \rightarrow B: M \parallel H(M \parallel S)$ ♦ Cung cấp xác thực - Chỉ A và B biết S
(c) $A \rightarrow B: M \parallel E_{KRa}[H(M)]$ ♦ Cung cấp xác thực và chữ ký số - H(M) được bảo vệ - Chỉ A có thể tạo ra $E_{KRa}[H(M)]$	(f) $A \rightarrow B: E_K[M \parallel H(M \parallel S)]$ ♦ Cung cấp xác thực - Chỉ A và B biết S ♦ Cung cấp tính bí mật - Chỉ A và B biết khoá K

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 được cấp bằng sáng chế và phải đăng ký.
- Một số thuật toán bị Mỹ kiểm soát xuất khẩu.

3.4 CHỮ KÝ SỐ

2.4.1 Các yêu cầu

Xác thực thông báo sẽ bảo vệ hai thành viên đối với một thành viên thứ 3. 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:

1. 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.

2. 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 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 bằng khoá riêng của người gửi (hình 3.12c), hoặc mã hoá mã băm của thông báo bằng khoá riêng của người gửi (hình 3.14c).

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 3.12d và 3.14d. 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 (hay 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 3.6 trình bày một số ví dụ về chữ ký số của thành viên thứ ba.

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

<i>Mã hoá đối xứng, thành viên thứ ba xem thông báo</i>
$X \rightarrow A: M \parallel E_{K_{XA}}[ID_X \parallel H(M)]$
$A \rightarrow Y: E_{K_{AY}}[ID_X \parallel M \parallel E_{K_{XA}}[ID_X \parallel H(M)] \parallel T]$
<i>Mã hoá đối xứng, thành viên thứ ba không xem thông báo</i>
$X \rightarrow A: ID_X \parallel E_{K_{XY}}[M] \parallel E_{K_{XA}}[ID_X \parallel H(E_{K_{XY}}[M])]$
$A \rightarrow Y: E_{K_{AY}}[ID_X \parallel E_{K_{XY}}[M] \parallel E_{K_{XA}}[ID_X \parallel H(E_{K_{XY}}[M])]] \parallel T]$
<i>Mã hoá khoá công khai, thành viên thứ ba không xem thông báo</i>
$X \rightarrow A: ID_X \parallel E_{KR_X}[ID_X \parallel E_{KU_Y}(E_{KR_X}[M])]$
$A \rightarrow Y: E_{KR_A}[ID_X \parallel E_{KU_Y}(E_{KR_X}[M])] \parallel T]$

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:

$$E_{K_{ay}} [ID_X || M || E_{K_{xa}} [ID_X || H(M)]]$$

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 $E_{K_{xa}}[ID_X || H(M)]$) giả.
- Y phải tin cậy A chỉ gửi $E_{K_{ay}}[ID_X || M || E_{K_{xa}}[ID_X || H(M)]] || T$ 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_{xy} , 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_{xy} . 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.

3.4.2 Chuẩn chữ ký số

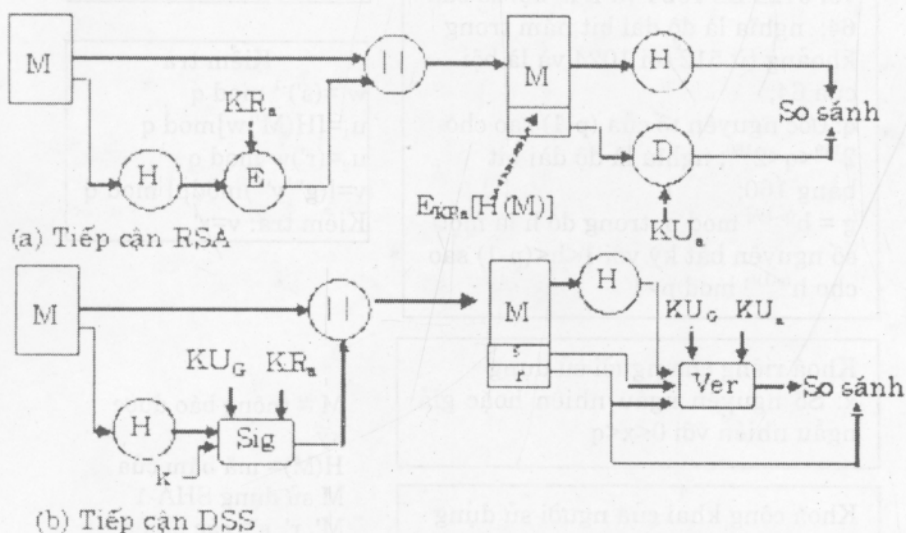
Chuẩn chữ ký DSS

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 3.15 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.



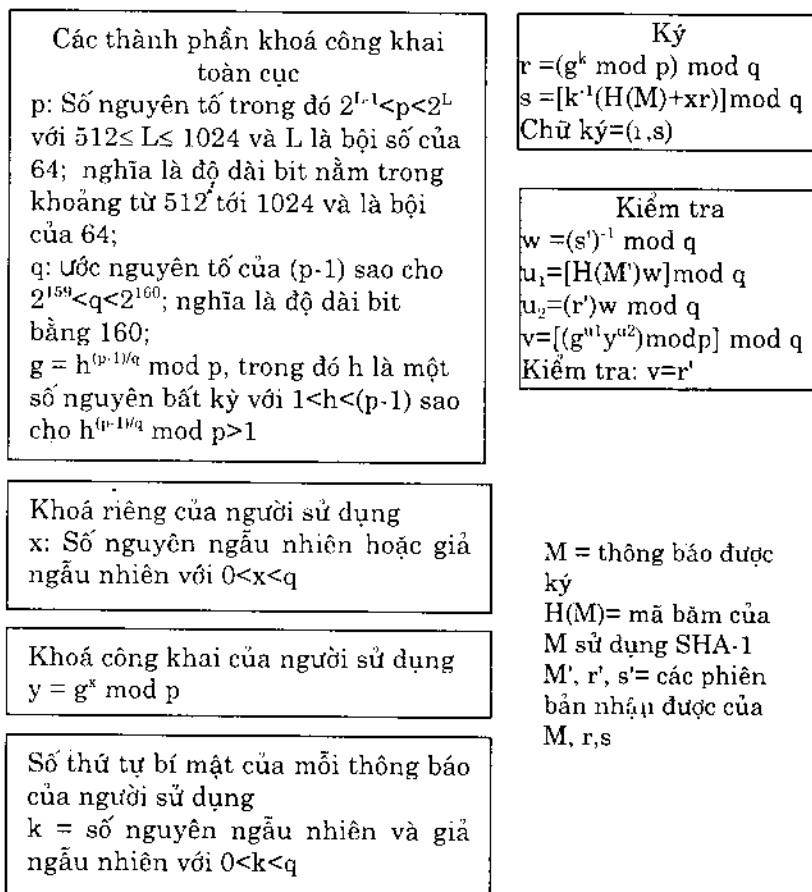
Hình 3.15 Hai tiếp cận chữ ký số

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_s) 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



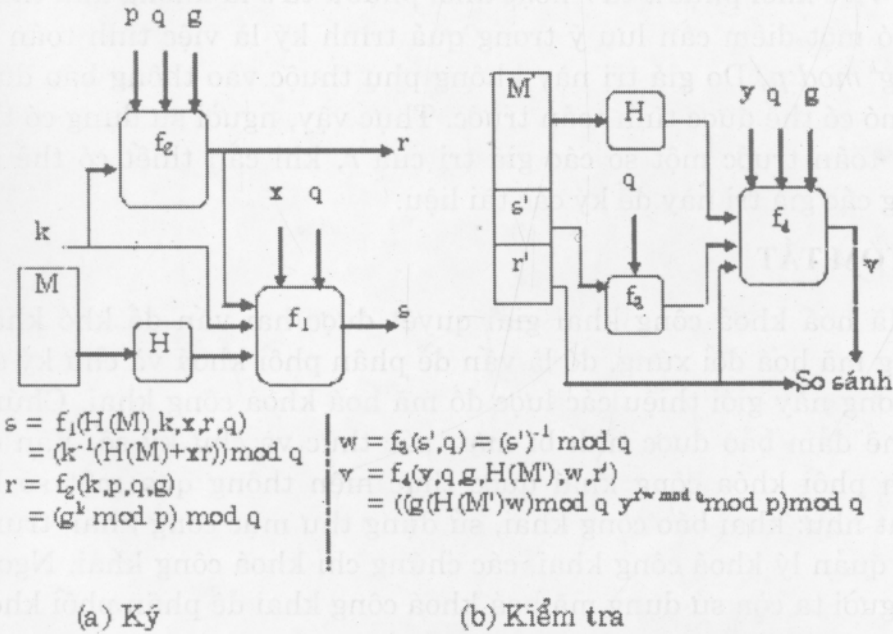
Hình 3.16 Thuật toán ký số (DSA)

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

Hình 3.16 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: $y = g^x \bmod p$.

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 3.17 Quá trình ký và kiểm tra 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 3.17 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: $s = (k'(H(M) + xr)) \bmod q$ trong đó k' 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 $g^h \bmod p$. 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.

3.5 TÓM TẮT

Mã hoá khoá công khai giải quyết được hai vấn đề khó khăn trong mã hoá đối xứng, đó là vấn đề phân phối khoá và chữ ký số. Chương này giới thiệu các lược đồ mã hoá khoá công khai. Chúng có thể đảm bảo được tính bí mật, xác thực và chữ ký số. Vấn đề phân phối khoá công khai được thực hiện thông qua một số kỹ thuật như: khai báo công khai, sử dụng thư mục công khai, trung tâm quản lý khoá công khai, các chứng chỉ khoá công khai. Ngoài ra người ta còn sử dụng mã hoá khoá công khai để phân phối khoá bí mật.

Xuất phát từ yêu cầu xác thực thông báo, hay đúng hơn đây là một thủ tục nhằm kiểm tra xem các thông báo nhận được có nguồn gốc từ một nguồn tin cậy, hợp lệ và có bị sửa đổi khi đi trên đường truyền hay không. Có thể nhóm chúng thành 3 loại: mã hoá

thông báo, mã xác thực thông báo (MAC) và hàm băm. Hàm băm được sử dụng trong quá trình tạo và kiểm tra chữ ký số.

Ngoài ra, chương này còn được giới thiệu về chữ ký số, chức năng của chữ ký số như xác thực, hỗ trợ chống chối bỏ; các loại chữ ký số như chữ ký số trực tiếp hoặc chữ ký số của thành viên thứ 3; thuật toán chữ ký số và chuẩn chữ ký số DSS.

CHƯƠNG IV

CHỨNG CHỈ ĐIỆN TỬ

Chứng chỉ được định nghĩa là một “tài liệu có chứa một công bố được chứng thực, như là sự đúng đắn của một điều gì đó”. Trong lĩnh vực điện tử, 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 công 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, khoá công khai được gắn kết chặt chẽ với một cá nhân, một thiết bị, hoặc một thực thể riêng biệt. Chứng chỉ khoá công khai được một cơ quan chứng thực (có thể là một người hay một thực thể, được gọi tắt là CA) ký. CA chứng thực nhận dạng và khoá công khai (hoặc các thuộc tính khác) của chủ thể chứng chỉ. Chủ thể chứng chỉ là một người, thiết bị, hoặc thực thể khác, nói chung là đối tượng nắm giữ khoá riêng tương ứng với khoá công khai được chứng thực có trong chứng chỉ. 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 rộng.

Trong chương này, chúng ta tập trung vào các chứng chỉ khoá công khai, cách sử dụng chúng, các chuẩn liên quan, một số vấn đề liên quan đến luật và việc sử dụng các chứng chỉ cho các mục đích khác nhau.

4.1 GIỚI THIỆU VỀ CÁC CHỨNG CHỈ KHOÁ CÔNG KHAI

Khi người khởi tạo (người gửi) thông báo muốn sử dụng mã hoá khoá công khai để mã hoá một thông báo 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.

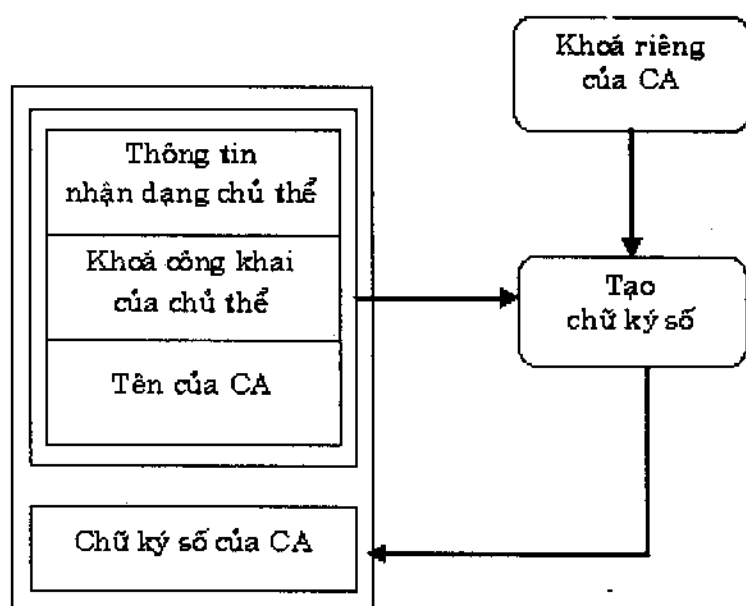
Khi khoá công khai được gửi đến cho một người dùng thì không cần thiết phải giữ bí mật khoá công khai này. Tuy nhiên, người sử dụng khoá công khai phải đảm bảo chắc chắn rằng khoá công khai được sử dụng đúng là của người nhận thông báo chủ định hoặc người ký. Nếu một đối tượng có thể dùng một khoá công khai khác thay thế cho khoá công khai hợp lệ, các nội dung của thông báo mã hoá có thể bị lộ, đối tượng này có thể biết được nội dung của các thông báo và có thể làm giả chữ ký số. Nói cách khác, các biện pháp bảo vệ (xuất phát từ các kỹ thuật này) sẽ bị lộ nếu một đối tượng có thể thay thế các khoá công khai không được chứng 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 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 ở phân tán. Các chứng chỉ khoá công khai giúp cho việc phân phối khoá công khai trở nên có hệ thống.

Hệ thống chứng chỉ khoá công khai làm việc như sau: CA phát hành 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 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 kiểu thực thể hợp pháp nào đó, thì chủ thể thường được gọi là một thuê bao (*subscriber*) của CA. Các chứng chỉ được CA ký bằng khoá riêng của CA.

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 an toàn (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 thuê bao đó bằng cách lấy từ bản sao chứng chỉ của thuê bao. Chứng chỉ của thuê bao có thể được kiểm tra bằng cách kiểm tra chữ ký của CA có trên chứng chỉ. Người sử dụng các chứng chỉ theo cách này được gọi là thành viên tin cậy.



Hình 4.1 Chứng chỉ khoá công khai đơn giản

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 dịch vụ an toàn truyền thông truyền thống để đảm bảo bí mật, 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 đảm bảo tính xác thực và

toàn vẹn). Nếu một đối tượng truy nhập trái phép định làm giả một chứng chỉ được phát hành cho một người sử dụng khoá công khai, anh ta sẽ bị người này phát hiện vì có thể kiểm tra được chữ ký số của CA. 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 khoá công khai là một người sử dụng có thể có được một số lượng lớn các khoá công khai của các thành viên khác một cách 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

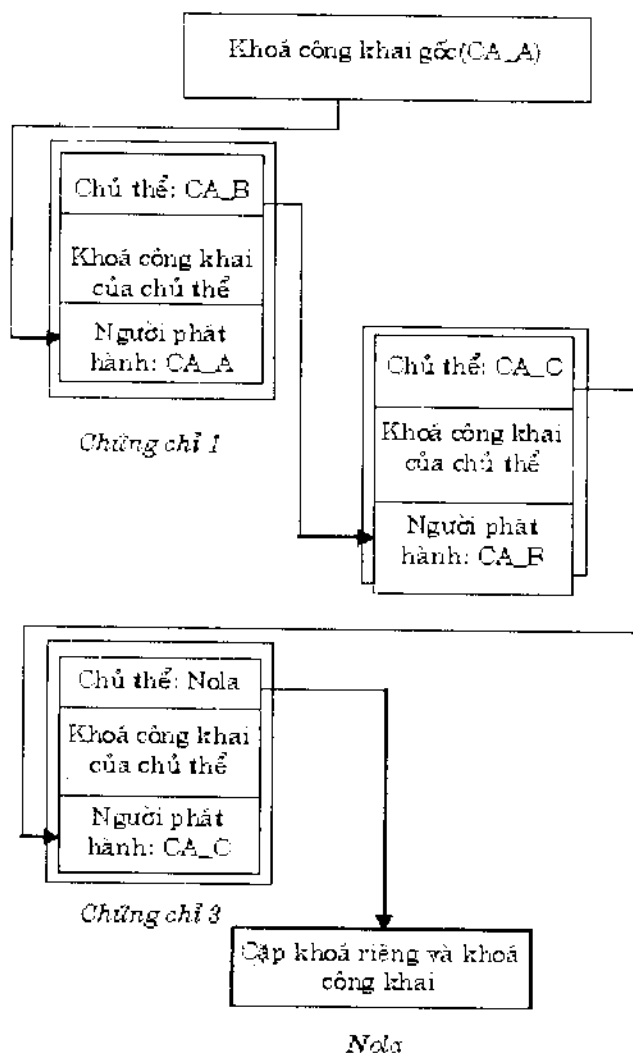
Nếu việc thiết lập một CA (có thể phát hành các chứng chỉ khoá công khai cho tất cả những người giữ các cặp khoá công khai và khoá riêng trên thế giới) là khả thi và tất cả những người sử dụng tin cậy vào các chứng chỉ do CA này phát hành thì chúng ta có thể giải quyết được vấn đề phân phối khoá công khai. Rất tiếc là điều này không thể thực hiện được. Đơn giản vì một CA không thể có đầy đủ thông tin và các mối quan hệ với tất cả 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 lưu giữ an toàn.

Vì vậy, một người sử dụng có thể áp dụng phương thức đệ quy chứng chỉ để có 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 như 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.

Người sử dụng khoá công khai



Hình 4.2 Đường dẫn chứng thực

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.

Mỗi cặp khoá có thời gian sử dụng bị giới hạn nhằm ngăn chặn các cơ hội phân tích mã và các tấn công gây tổn thất.

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. Người sử dụng khoá công khai không nên sử dụng một chứng chỉ đã hết hạn, trừ khi muốn xác nhận lại hoạt động trước đó; ví dụ, 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 thì CA có thể phát hành một chứng chỉ mới cho thuê bao này.

Hơn nữa, trong trường hợp khoá riêng bị lộ nhưng không bị phát hiện, thời hạn kết thúc của một chứng chỉ có thể bảo vệ người sử dụng, ngăn chặn việc tiếp tục sử dụng khoá công khai có trong một chứng chỉ được phát hành trước khi bị lộ. Còn có nhiều trường hợp, trong đó CA muốn huỷ bỏ một chứng chỉ trước khi thời hạn sử dụng của nó kết thúc. Ví dụ, trong trường hợp phát hiện hoặc nghi ngờ khoá riêng bị lộ. Thủ tục thu hồi được trình bày trong mục 4.6.

4.1.3. Các mối quan hệ mang tính pháp lý

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

(a) *Cộng đồng khép kín (Closed community)*: CA và các thuê bao của CA này là một thực thể hợp pháp. Ví dụ, giả thiết các thuê bao là các máy rút tiền tự động của một ngân hàng, chúng sinh chữ ký số cho các giao dịch tài chính và cơ quan chứng thực do

ngân hàng điều hành. Trong trường hợp này, mục đích của các chứng chỉ thuần túy là kỹ thuật, có nghĩa là cho phép các ứng dụng tài chính kiểm tra tính toàn vẹn của các giao dịch, thông qua một khoá công khai đã biết.

(b) *Cộng đồng mở (Open community)*: CA là một thực thể hợp pháp, độc lập với các thuê bao của mình. Chứng chỉ được các thực thể hợp pháp khác sử dụng. Ví dụ, nhà cung cấp dịch vụ chứng thực phát hành các chứng chỉ cho những người thuê dịch vụ. 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. Trong trường hợp này, CA thường được gọi là thành viên thứ 3 tin cậy.

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 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.

Chứng thực chỉ thực sự có hiệu quả nếu hai kiểu kiểm soát cơ bản sau được đưa ra thích hợp:

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

(b) *Bảo vệ khoá riêng (Private-key protection)*: Các kiểm soát phải được đưa ra để đảm bảo rằng chỉ có chủ thể - người được nhận dạng trong (a) có thể thực hiện việc kiểm soát sau đó đối với 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, treo và huỷ bỏ 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 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 ở một trong hai nơi (là hai lựa chọn cơ bản):

- ♦ *Hệ thống lưu giữ cặp khoá (Key-pair holder system)*: Cặp khoá được sinh ra trong cùng một hệ thống (trong cùng một thẻ bài phần cứng hoặc môđun 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 (Central system)*: 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 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 dự phòng hoặc lưu trữ trong một hệ thống trung tâm thì đây là một bước chuẩn bị thích hợp bởi vì hệ thống tương tự hoặc các hệ thống liên quan chặt chẽ thực hiện các chức năng sinh khoá và sao lưu dự phòng hoặc lưu trữ 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 dự phòng hoặc lưu trữ cặp khoá 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 mà chỉ 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 mô-đun phần cứng thường trú hoặc thẻ bài. Ví dụ như một thẻ thông minh hoặc thẻ PCMCIA.

(b) Hoặc lưu giữ trên một tệp 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 (Số hiệu nhận dạng cá nhân). Còn có các giải pháp xác thực cá nhân khác 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) có thể được sử dụng để bảo vệ một hoặc nhiều khoá riêng và/hoặc thông tin nhạy cảm trong cơ sở dữ liệu.

4.2.3 Cập nhật cặp khoá

Để 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. Tùy 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 sử dụng thông qua các ứng dụng, mọi người có thể cần đến chúng ngoài thể 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 ký số và mã hoá, tuân thủ các nguyên tắc quản lý vòng đời 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 và chữ ký số. Ví dụ, 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 được sử dụng cho các mục đích ký số phải được lưu giữ an toàn trong suốt thời gian tồn tại của nó, chỉ có đối tượng sở hữu được 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 - khoá được sinh ra, được sử dụng và huỷ bỏ 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) Khoá riêng dùng cho chữ ký số không cần phải sao lưu vì việc sao lưu này sẽ mâu thuẫn với yêu cầu (a). Trong thực tế, khoá riêng dành cho chữ ký số phải được huỷ bỏ 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) 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 sung thêm các yêu cầu quản lý khoá khác như sau:

(e) 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 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 một cách an toàn khi thời gian tồn tại của nó đã kết thúc. Theo (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 khoá công khai được sử dụng để mã hoá thường phải chịu nhiều kiểm soát xuất khẩu nghiêm ngặt hơn so với các 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 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.

♦ Các cặp khoá có thể có các chu kỳ sử dụng khác nhau. Cặp khoá có thể được cập nhật thường xuyên do các yêu cầu về chu kỳ sử dụng. 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.

♦ 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 mã. 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 hệ thống uỷ nhiệm khoá. Các khoá riêng dùng cho chữ ký số không nên bị chính phủ phát hiện theo cách này.

♦ Các yêu cầu trên nằm trong các thiết kế của các hệ thống gửi tin điện tử PEM (*Privacy Enhanced Mail*) và PGP (*Pretty Good Privacy*) 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 phát hành một chứng chỉ cho một thuê bao, thuê bao cần đăng ký với CA, xin cấp chứng chỉ một cách rõ ràng, cung cấp các thông tin cần thiết đối với một chứng chỉ, ví dụ khoá công khai và thông tin cho các trường hợp xác định khác có trong một 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 đó (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 tùy chọn của CA, một bản sao của chứng chỉ có thể được CA lưu giữ.
7. CA ghi lại các chi tiết của quá trình tạo chứng chỉ vào nhật ký kiểm toán.

4.3.3 Xác thực chủ thể

Trước khi phát hành một chứng chỉ, CA hoặc thực thể được CA uỷ quyền cần xác nhận đặc điểm nhận dạng của người, thiết bị

hoặc thực thể có khoá công khai được chứng thực.

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

- ♦ *Sự hiện diện cá nhân (Personal presence)*: Sự xuất hiện của một người trước một thực thể tin cậy được công nhận rộng rãi rất quan trọng đối với xác nhận nhận dạng. Cho phép CA hoặc người được CA uỷ quyền có được thông tin, hoặc các đặc điểm điển hình của người xin cấp chứng chỉ. Một khi xác nhận 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 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 (Identification document)*: CA hoặc người được CA uỷ quyền 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 hộ chiếu 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. 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. CA và những người được CA uỷ quyền có thể nhận biết một số 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, 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 tổ chức trung gian phân tán, họ sẽ liên lạc trực tiếp với thuê bao cần thiết. Những tổ chức 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 bài cá nhân cho những người được uỷ quyền nắm giữ chúng và khôi phục lại các thẻ bài đã quá hạn do những người này gửi đến.*

4.3.5 Cập nhật chứng chỉ

Mọi chứng chỉ đều có thời hạn kết thúc, vấn đề quản lý chứng chỉ thuộc trách nhiệm của CA. 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 huỷ bỏ và cập nhật các chứng chỉ thường đi đôi với việc huỷ bỏ và cập nhật các cặp khoá.

Đôi khi, việc cập nhật chứng chỉ được thực hiện như một quá trình trong suốt đời 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 việc cập nhật một chứng chỉ kéo theo một thay đổi nào đó, ví dụ 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 nên gửi xác nhận chấp nhận một chứng chỉ mới một cách rõ ràng.

4.4 Phân phối chứng chỉ

Để mã hoá dữ liệu gửi cho một thành viên từ xa, hoặc để một thành viên từ xa có thể kiểm tra một chữ ký số, người sử dụng cần có bản sao chứng chỉ, từ đó có được khoá công khai của thành viên ở xa, các chứng chỉ 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 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 lưu giữ.

4.4.2 Phân phối thông qua dịch vụ thư mục

Khi sử dụng mã hoá 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 từ các bản sao của chứng chỉ khoá công khai được yêu cầu lưu giữ cục bộ. Nhưng 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 lưu giữ (có thể lưu giữ các chứng chỉ) là đặc biệt thích hợp.

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 minh Viễn thông Quốc tế (ITU) và Tổ chức tiêu chuẩn hoá Quốc tế (IOS). Các chuẩn thư mục được ITU thiết kế là X.500. Chuẩn 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 với 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.

Ngay từ đầu người ta đã 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. Do 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 nhanh, tương thích với mô hình thư mục X.500. LDAP đơn giản hơn nhiều và bổ sung 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.

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/IEC/ITU.

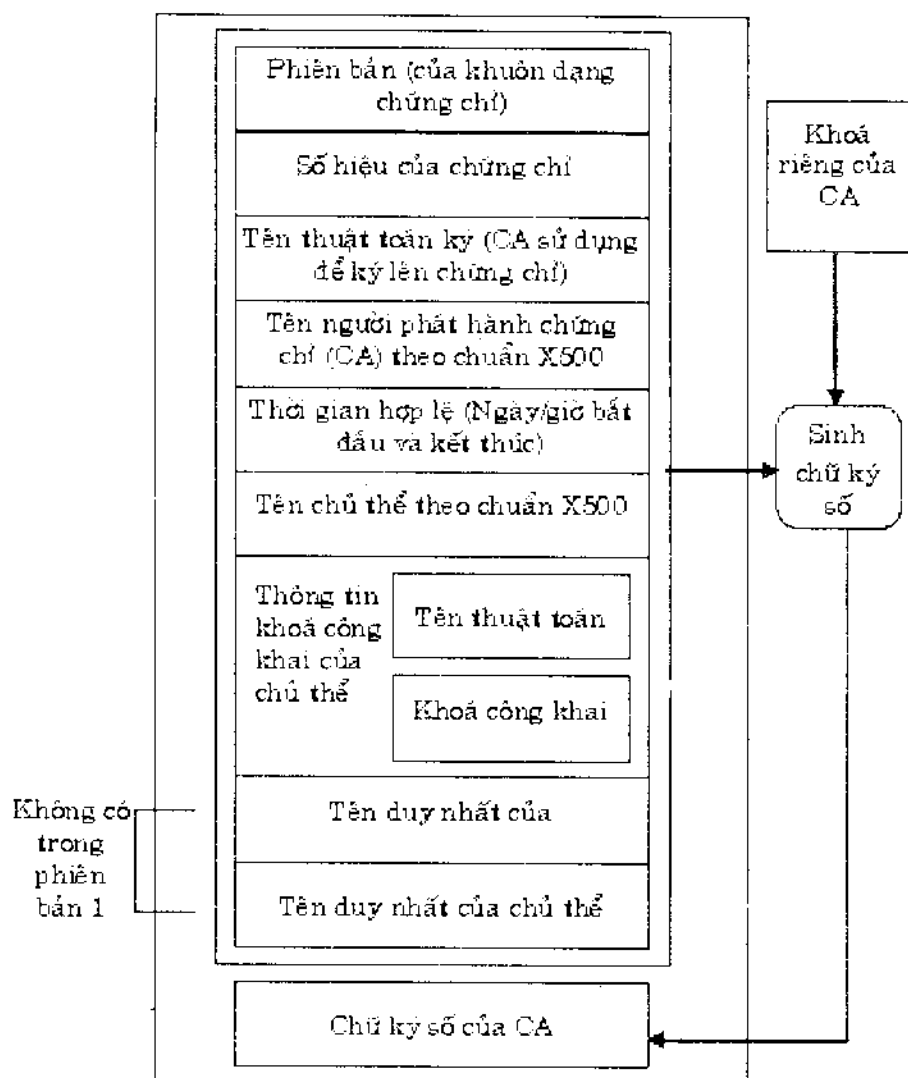
4.5.1 Khuôn dạng chứng chỉ cơ bản

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 sung 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").



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

(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 của người phát hành (Issuer unique identifier)*: Là một chuỗi bit tùy 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").

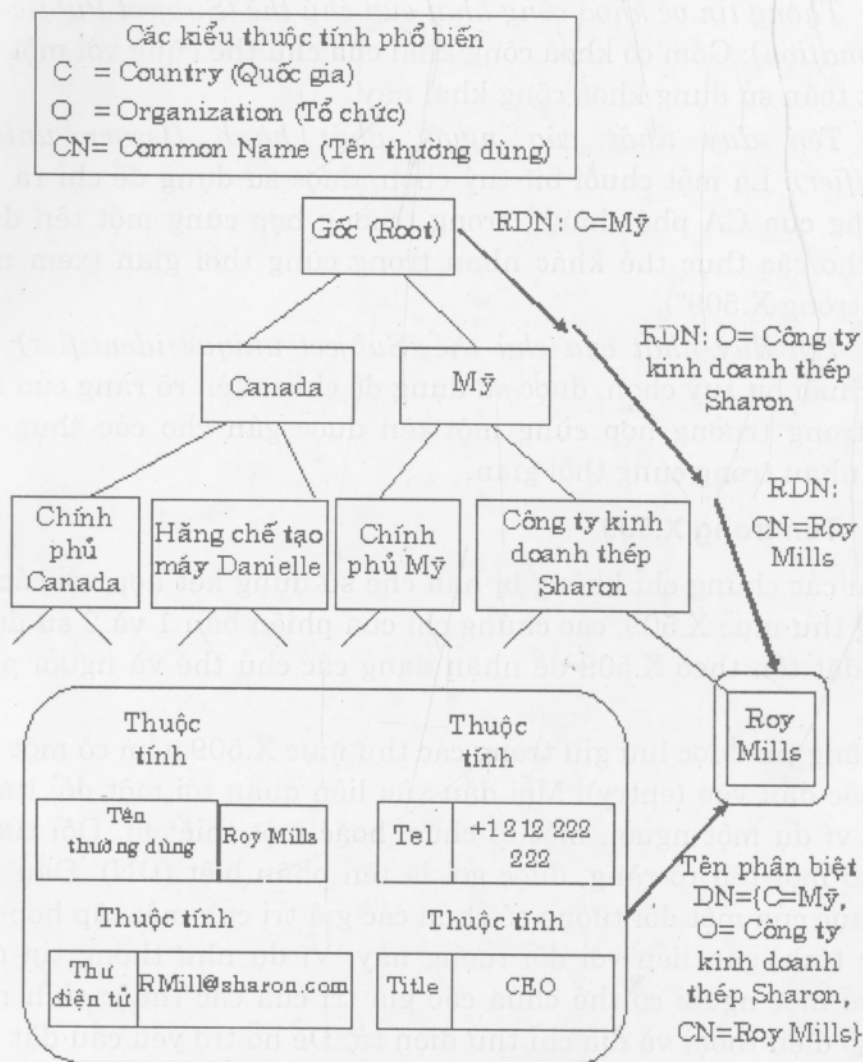
(i) *Tên duy nhất của chủ thể (Subject unique identifier)*: Là một chuỗi bit tùy chọn, được sử dụng để chỉ ra tên rõ ràng của chủ thể, trong trường hợp cùng một tên được gán cho các thực thể khác nhau trong cùng thời gian.

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.

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 điện tử. Để hỗ trợ yêu cầu đặt tên rõ ràng, tất cả các đầu vào của X.509 được tổ chức hợp lý theo 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 mức trên gần nó nhất (ở trên cây) cùng với tên phân biệt liên quan (RDN), nó phân biệt đầu vào phụ thuộc với các mức dưới trực tiếp khác của cùng một thực thể mức trên.



Hình 4.4 Ví dụ về cấu trúc tên X.500

RDN biểu diễn một (hoặc nhiều) giá trị 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 thuộc tính được cung cấp duy nhất). Ví dụ, một người có thể có RDN như sau *Common Name = Roy Mills*.

Hình 4.4 trình bày một ví dụ về cấu trúc tên X.500. Mức gốc gồm có nhiều đỉnh, mỗi đỉnh liên kết với một quốc gia. Mức tiếp theo (ở dưới mức các quốc gia) có các đỉnh liên kết với các tổ chức của quốc gia 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 họa trong hình 4.4.

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 sung. 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 thường dùng (CN), 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 cho người làm công của Sharon có thể như sau: {*Common Name = 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:

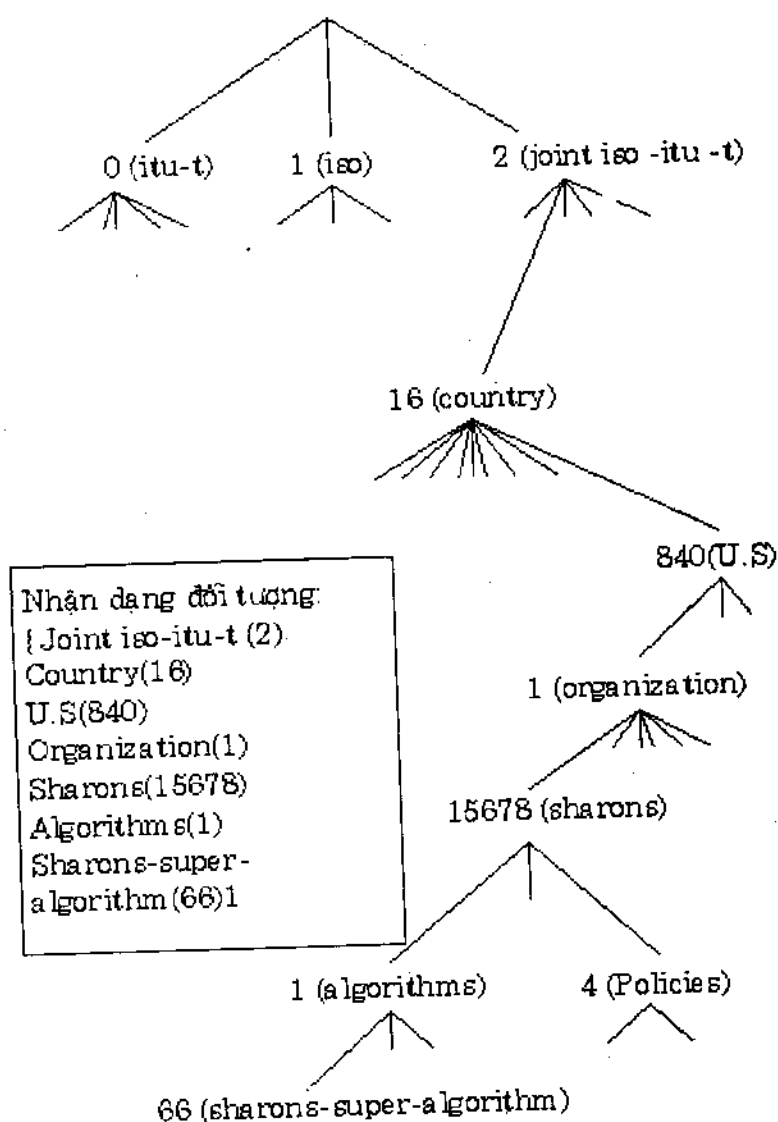
- 0 (dành cho ITU)
- 1 (dành cho ISO)
- 2 (dành cho cả ITU và ISO)

Theo ISO, mức thứ hai lấy các giá trị như sau: 0 (dành cho các chuẩn của ISO), 1 (dành cho các quốc gia 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 (Country) được sử dụng cho các cơ quan đăng ký quốc gia.

Với Country = {2 16} là đặc biệt quan trọng. Tại mức kê dưới, các mã quốc gia (có 3 số) được sử dụng để nhận dạng từng quốc gia cụ thể. Mỗi quốc gia chỉ định một tổ chức làm cơ quan đăng ký quốc gia của mình. Ví dụ, mã quốc gia của Mỹ là 840. Mỹ chọn ANSI (Viện chuẩn Quốc gia Mỹ) làm cơ quan đăng ký quốc gia. 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 tùy 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 Ví dụ về tên đối tượng

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)}.

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
<i>/iso(1) identified-organization(3) oiw(14) secsig (3) algorithm(2) 29/</i>	<i>Chữ ký số : RSA với SHA-1</i>	<i>Các thoả thuận tại hội thảo khoa học của các nhà thực thi môi trường hệ thống mở NIST</i>
<i>/iso(1) member-body(2) us (840) x9-57(10040) x9algorithm (4) dsa-with-sha1/</i>	<i>Chữ ký số : DSA với SHA-1</i>	<i>ANSI X9.57</i>
<i>/joint-iso-ccitt(2) country(16) us(840) organization(1) us-government (101) dod(2) infosec(1) algorithms (1) 2/</i>	<i>Chữ ký số : DSA với SHA-1</i>	<i>Chương trình MISSI của Bộ Quốc phòng Mỹ</i>
<i>/iso(1) member-body(2) us (840) rsadsi(113549) pkcs(1) pkcs-1(1) md5WithRSAEncryption (4)/</i>	<i>Chữ ký số : RSA với MD5</i>	<i>Công ty bảo mật RSA. PKCS#1</i>

4.5.4 Khuôn dạng chứng chỉ X.509 mở rộng (v.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 sung 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 chỉ 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 tùy 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 sung thêm các trường vào khuôn dạng của chứng chỉ. Các tổ chức chuẩn (như ISO/IEC, ITU và ANSI 19) chấp nhận bổ sung 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 sung 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 xuất hiện khi trường mở rộng là thiết yếu (*critical*) hoặc không thiết yếu (*non-critical*). Nếu cờ chỉ báo 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. Nếu cờ chỉ báo là "thiết yếu" thì một hệ thống sẽ không an toàn nếu sử dụng bất kỳ phần nào 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 chỉ 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 thủy 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 chỉ báo 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 sử dụng các 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 sung 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 chỉ báo 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.

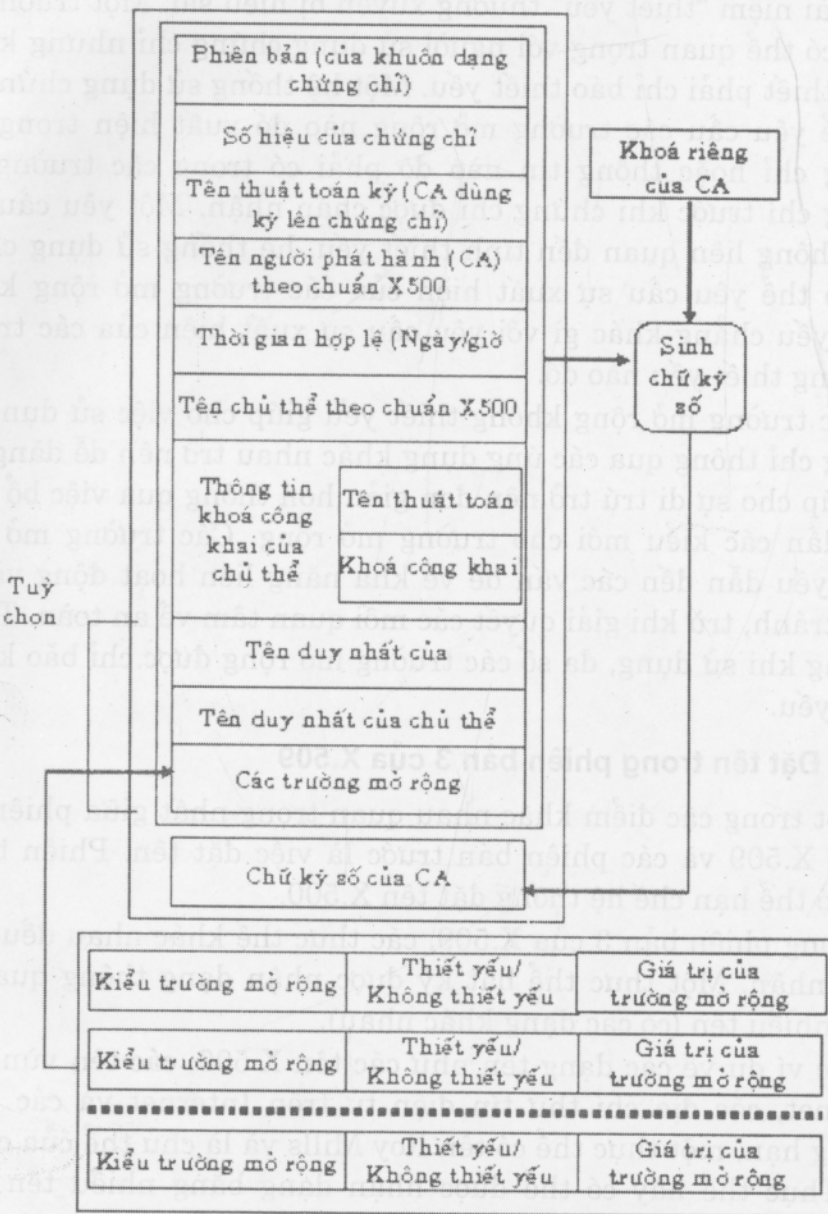
Trong phiên bản 3 của X.509, các thực thể khác nhau đều được chấp nhận. Một thực thể bất kỳ được nhận dạng thông qua một hoặc nhiều tên (có các dạng khác nhau).

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. Chẳng hạn, một thực thể có tên Roy Mills và 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=Mỹ, Organization=Sharon's Steelcorp, Inc., Common Name=Roy Mills};
- ♦ Tên X.500: {Country=Mỹ, Organization=Sharon's

Steelcorp,Inc., Title=CEO};

♦ Địa chỉ thư tín điện tử: RMills@sharons.com.



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

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:

- (a) Địa chỉ thư điện tử;
- (b) Tên miền của Internet;
- (c) Địa chỉ thư điện tử X.400;
- (d) Tên thư mục X.500;
- (e) Tên thành viên EDI (gồm có tên của cơ quan gán tên, cộng với tên thành viên được cơ quan này gán cho);
- (f) Tên xác định duy nhất Web (trong đó URL là một kiểu phụ);
- (g) Địa chỉ IP trên Internet (tạo thành một tên đối tượng, được trình bày chi tiết trong mục "Đăng ký đối tượng");
- (h) Tên được đăng ký (theo dạng tên bất kỳ – dạng tên được đăng ký như là một đối tượng (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 sung 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 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) *Tên khoá của CA phát hành (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 dạng bằng cách:

- ♦ Thông qua một tên khoá rõ ràng;
- ♦ Thông qua một con trỏ trỏ tới một chứng chỉ khác, trong đó khoá của người phát hành chứng chỉ này được một CA khác chứng thực; hoặc
- ♦ Thông qua tên khoá rõ ràng và một con trỏ chứng chỉ.

Trường này giúp cho các hệ thống 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) *Tên khoá của chủ thể (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) *Sử dụng khoá (Key Usage)*: Trường này được sử dụng để chỉ ra mục đích sử dụng khoá, chẳng hạn cho chữ ký số, hoặc thiết lập khoá mã. Trường này có hai biến thể, "thiết yếu" và "không thiết

yếu". Khi trường chỉ báo "thiết yếu", CA quy định chỉ được sử dụng chứng chỉ và khoá vào các mục đích đã được xác định. Nếu người sử dụng dùng chứng chỉ vào các mục đích khác thì coi như đã vi phạm chính sách của CA và không nên tin tưởng vào chứng chỉ này. Khi trường chỉ báo "không thiết yếu", 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 nhiều khoá và chứng chỉ khác nhau, chúng được sử dụng cho các mục đích chữ ký số và thiết lập khoá mã, 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 đích 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) *Khoảng thời gian sử dụng khoá riêng (Private-key Usage Period)*: chỉ ra thời hạn sử dụng một khoá riêng cho mục đích ký số (khoá riêng này cùng cặp 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) *Các chính sách chứng chỉ (Certificate policies)*: chỉ ra các chính sách hoặc các hoạt động liên quan đến chứng chỉ.

(f) *Ánh xạ chính sách (Policy Mapping)*: (chỉ được sử dụng khi chủ thể của chứng chỉ là một CA) cho phép người phát hành xác định một hoặc nhiều chính sách (dành cho chứng chỉ của người phát hành này) có thể được quan tâm ngang bằng với các chính sách khác được sử dụng trong miền của CA.

Các trường mở rộng của nhóm (2) chỉ ra các tên lựa chọn dành cho các chủ thể và người phát hành chứng chỉ. Chúng cũng có thể cho biết thêm các thông tin thuộc tính của chủ thể, 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) *Tên lựa chọn của chủ thể (Subject Alternative Name)*: Trường này chỉ ra 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) *Tên lựa chọn của người phát hành (Issuer Alternative Name)*: Trường này chỉ ra một hoặc nhiều tên lựa chọn dành cho người phát hành chứng chỉ. Các dạng tên dành cho người phát hành cũng giống như các dạng tên dành cho trường Tên lựa chọn của chủ thể. 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) *Các thuộc tính thư mục của chủ thể (Subject Directory Attributes)*: Trường này chuyển thêm các giá trị thuộc tính X.500 mà chủ thể mong muốn (ngoài thông tin nhận dạng có trong các trường tên), chẳng hạn như vị trí của chủ thể trong một tổ chức, số điện thoại hoặc địa chỉ thư.

Các trường mở rộng của nhóm (3) có thể giúp cho các tổ chức khác nhau liên kết các cơ sở hạ tầng của họ với nhau. Khi 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 kiểu đường dẫn chứng thực xuất phát từ chứng chỉ này. Các trường mở rộng này gồm:

(a) *Các ràng buộc cơ bản (Basic Constraints)*: Trường này chỉ ra chủ thể của chứng chỉ 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, có thể định rõ 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) *Các ràng buộc đối với tên (Name Constraints)*: Trường này giới hạn không gian tên có thể chấp nhận trong các chứng chỉ có trong một đường dẫn chứng thực.

(c) *Các ràng buộc đối với chính sách (Policy constraints)*:

Trường này xác định một tập hợp các ràng buộc cho việc nhận dạng chính sách chứng chỉ và tham chiếu đến chính sách một cách tường minh.

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 (Bảng ký hiệu cú pháp trừu tượng số 1), nó được phát triển như một phần của chương trình chuẩn hoá OSI (Kết nối các hệ thống mở). 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 thuận tiện và thiếu công cụ chất lượng cao mà chi phí 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 khoảng 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 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 huỷ bỏ chứng chỉ. Do có thể bị huỷ bỏ 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 CA.

Thuê bao có quyền yêu cầu thu hồi các chứng chỉ của mình. Lý do thu hồi có rất nhiều, chẳng hạn do vi phạm nghiêm trọng những điều khoản bắt buộc trong quy định hoạt động chứng thực (CPS) do CA đưa ra, hoặc do lộ khoá riêng,...

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 thuộc trách nhiệm của cơ quan này.

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

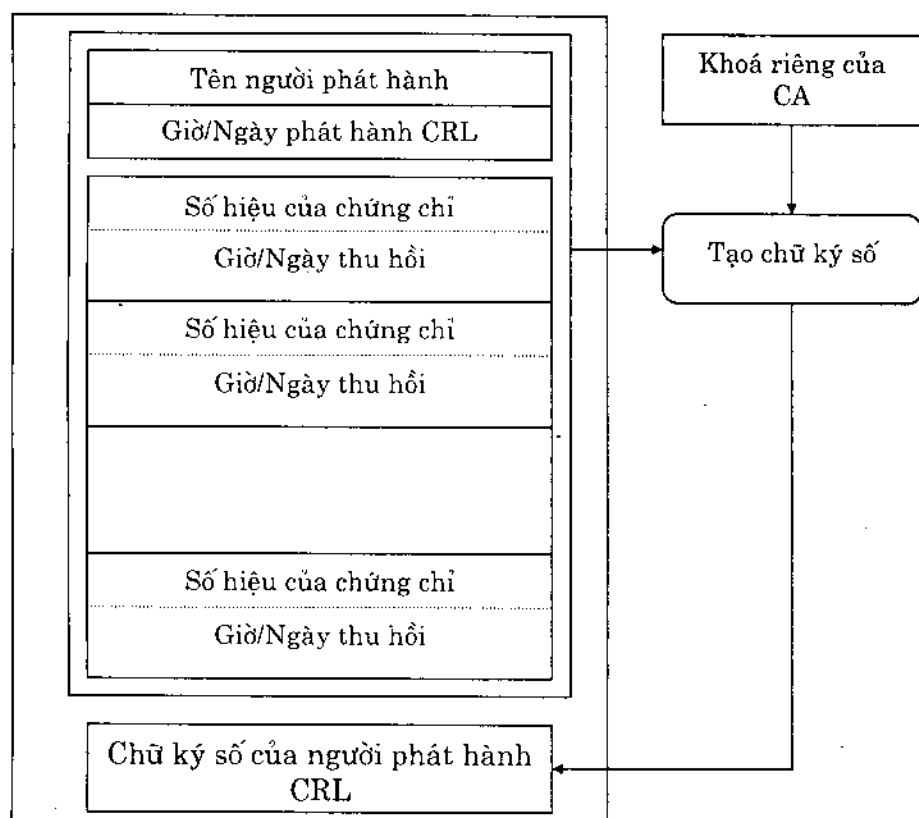
Sau khi quyết định thu hồi một chứng chỉ, CA cần thông báo cho những người sử dụng chứng chỉ biết sự thu hồi này. Giải pháp thông báo thông dụng nhất là CA phát hành định kỳ một cấu trúc dữ liệu được gọi là danh sách các chứng chỉ bị thu hồi. Khái niệm CRL được trình bày trong chuẩn X.509. CRL là một danh sách các chứng chỉ bị thu hồi được gán nhãn thời gian, danh sách này được CA ký và công bố. CRL có thể phân tán, ví dụ gửi nó đến một địa chỉ Web xác định hoặc thông qua đầu vào thư mục X.500 của CA. Mỗi chứng chỉ bị thu hồi được CRL nhận dạng thông qua số hiệu của nó vì 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 hệ thống sử dụng một chứng chỉ, nó phải kiểm tra chữ ký số có trong chứng chỉ, khoảng thời gian hợp lệ của chứng chỉ, một CRL phù hợp gần nhất để biết được rằng số hiệu của chứng chỉ không nằm 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.

CA phát hành các CRL định 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 sung 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 này là các CRL có thể được phân phối cùng một cách thức như đã dùng để phân phối chứng chỉ khoá công khai, nghĩa là thông qua truyền thông và các hệ thống máy chủ không cần bảo vệ một khi CRL đã được ký. Vì vậy, cách thức này trở nên kinh tế hơn khi cài đặt và thực hiện do 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 thu hồi

Một hạn chế của giải pháp này là thời gian định kỳ, nó hạn chế khoảng thời gian phát hành CRL. Chẳng hạn, có thể xảy ra trường hợp 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, sau 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 thông báo thu hồi. Tuy

nhien, 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 CRL không định kỳ từ một máy chủ không tin cậy và thay thế vào đó là một CRL đã được phát hành trước đó, mà 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 “phát hành các CRL định kỳ” là hệ thống sử dụng chứng chỉ có thể tìm kiếm các CRL từ một thư mục khi cần. Giải pháp này còn được gọi là giải pháp “kéo” (*pull*).

Một giải pháp phân phối lựa chọn khác là giải pháp “đẩy” (*push*), trong đó CA quảng bá CRL cho các hệ thống sử dụng chứng chỉ. 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, bởi vì các đối tượng tấn công có thể chặn và xoá bỏ các thông báo thu hồi. Thuận lợi chính của giải pháp “đẩy” chính là các thu hồi thiết yếu hơn (ví dụ do lộ khoá hoặc do lỗi của CA) có thể được thông báo 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 là 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 thu hồi nào cần được thông báo cho các hệ thống sử dụng chứng chỉ nào (trong một môi trường của cơ sở hạ tầng lớn tùy 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 (Khởi sinh an toàn hệ thống thông tin đa mức) của Bộ Quốc phòng Mỹ cung cấp một cơ sở hạ tầng khoá công khai dành cho DMS (Hệ thống gửi tin của 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 tình trạng thu hồi. Tuy nhiên, có thêm một giải pháp kiểu quảng bá, được sử dụng để thông báo

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. Các CA thông báo về các khoá bị lộ trên mạng 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, MISSI đang di trú việc sử dụng đặc tính mới của X.509, đặc tính này được gọi là các CRL gián tiếp (*indirect CRL*) 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. Nó không thể hỗ trợ tất cả các yêu cầu trong nước và tất nhiên nó không phải là một cơ sở hạ tầng mang tính toàn cầu và thương mại mở.

4.6.4 Sự thu hồi ngay lập tức

Một mối quan tâm thường xuyên đối với giải pháp "phát hành các CRL định kỳ" là các hệ thống sử dụng chứng chỉ không thể chấp nhận việc làm chậm trễ các thông báo thu hồi vì lý do thời gian định kỳ. Tùy thuộc vào môi trường ứng dụng, sẽ có nhiều thiệt hại nếu khoá bị lộ trong một ngày. Thực tế, thông tin về một chứng chỉ bị thu hồi có giá trị thiết thực 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 cần được quan tâm.

Với việc kiểm tra tình trạng 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 hiện thời của chứng chỉ. Nó phải được tiến hành an toàn, đảm bảo được tính đúng lúc và xác thực 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 tình trạng 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. Để nhận thấy rằng, một máy chủ như vậy cần tạo ra chữ ký số cho mỗi cuộc giao dịch và các 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 tình trạng 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 kho 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 khi chứng chỉ bị huỷ bỏ; 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 chen 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 huỷ bỏ. Hơn nữa, việc phân phối các chứng chỉ không cần các giao thức đặc biệt, thông thường cũng 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 tùy chọn, được sử dụng để bảo vệ đáp ứng giao dịch. Có thể sử dụng cách này để có 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 tùy 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 tình trạng thu hồi trong thời gian thực.

(c) *Chu kỳ phát hành các 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, kịp thời thông báo 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 'nghỉ ngừng 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 tùy 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.

4.6.5 Dòng thời gian xử lý thu hồi

Để hiểu được một số các liên kết giữa các CRL và các vấn đề pháp lý 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:

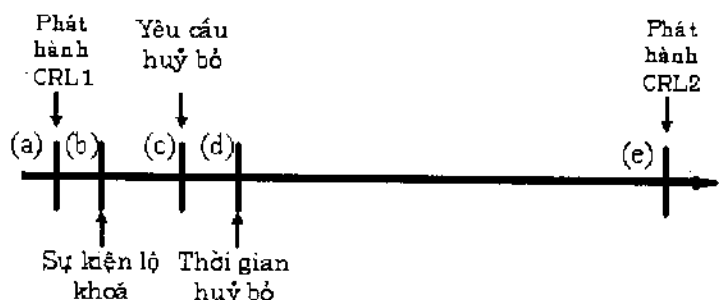
(a) *Phát hành CRL1*: Một CRL được phát hành trước khi có yêu cầu huỷ bỏ.

(b) *Sự kiện lộ khoá*: Sự kiện xảy ra dẫn đến huỷ bỏ chứng chỉ, ví dụ có thông báo 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 huỷ bỏ*: Yêu cầu huỷ bỏ được gửi tới 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 huỷ bỏ*: CA chính thức chấp nhận huỷ bỏ.

(e) *Phát hành CRL2*: CRL (có chứa chứng chỉ bị huỷ bỏ) được phát hành và công bố.



Hình 4.8 Dòng thời gian huỷ bỏ

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 riêng 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 thay đổi tại các thời điểm khác nhau (các điểm này đã được chỉ rõ trong dòng thời gian). Ví dụ, huỷ bỏ do 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 thông báo huỷ bỏ 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 huỷ bỏ chính thức được gửi đi nhưng người sử dụng chứng chỉ có thể không có cách nào biết được sự huỷ bỏ 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). Khi phát hành các CRL định kỳ, người sử dụng chứng chỉ sẽ không biết có thông báo huỷ bỏ mới cho đến khi CRL2 được phát hành. Do có thông báo thu hồi trực tiếp, nên người sử dụng chứng chỉ có thể biết được thông báo huỷ bỏ 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 có sử dụng khoá.

♦ *Giai đoạn sau (e)*: Lúc này, CA đã hoàn thành trách nhiệm của mình trong việc thông báo huỷ bỏ. Do người sử dụng chứng chỉ có thể sử dụng một chứng chỉ đã bị huỷ bỏ trong giai đoạn này, nên cần gán 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.

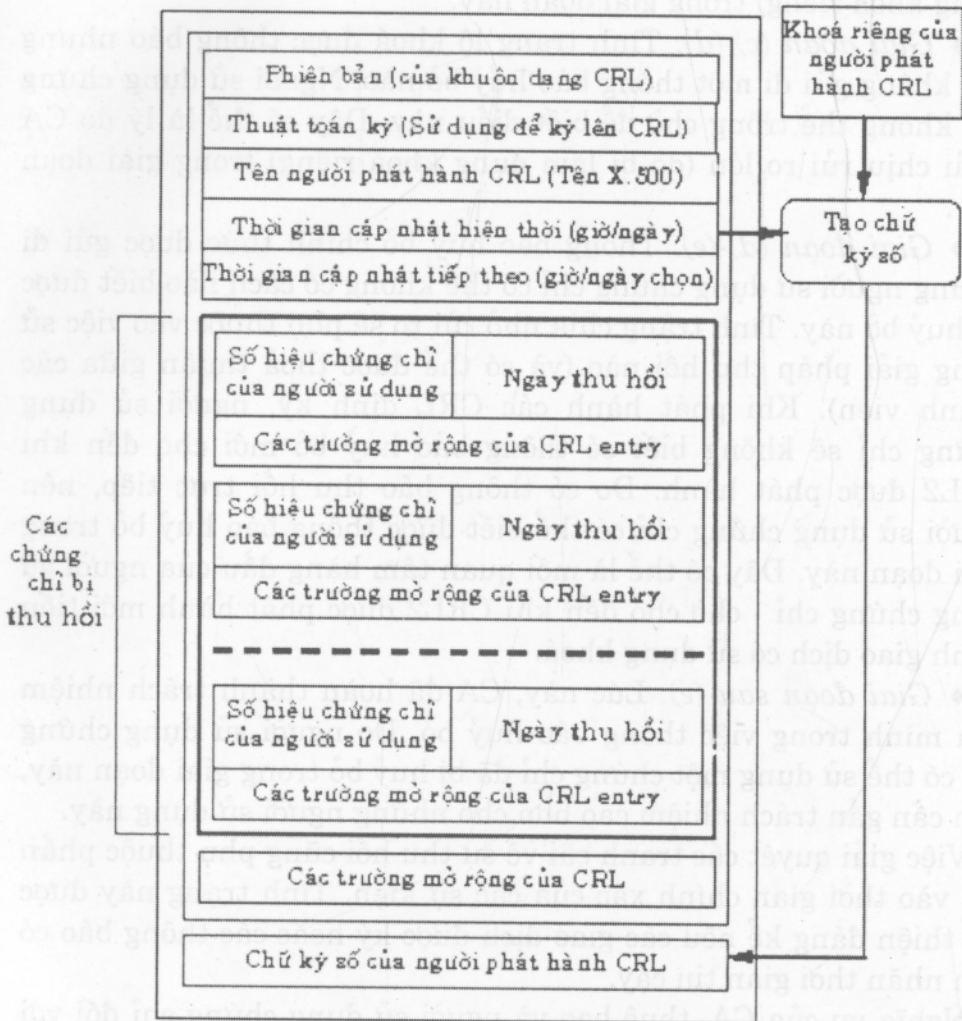
Nghĩa vụ của CA, thuê bao và người sử dụng chứng chỉ đối với sự kiện thu hồi, việc chia nhỏ trách nhiệm pháp lý, ngăn chặn tình trạng lộ khoá, tập trung vào việc thiết lập các hoạt động của CA và thoả thuận giữa các thành viên, đưa ra các quy tắc rõ ràng nhằm kiểm soát các sự kiện thu hồi.

4.7 CRL THEO X.509

Bổ sung thêm vào khuôn dạng chứng chỉ chuẩn 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



Hình 4.9 Khuôn dạng CRL của X.509

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 tùy chọn, có thể được bỏ qua nếu tất cả những người sử dụng của CRL biết được chu kỳ phát hành. Tuy nhiên, khuyến nghị không nên bỏ qua trường này.

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

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

(h) *Các trường mở rộng của CRL entry (CRL Entry Extensions)*: Đây là các trường bổ sung, 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 sung, 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.

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 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 đã phát hành trước đó; 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 thu hồi chứng chỉ.

♦ *Ngày hết hiệu lực (Invalidity Date)*: trường mở rộng của CRL entry. Trường này chỉ ra ngày huỷ bỏ khoá do lộ.

Trường mở rộng Mã lý do có các giá trị được định nghĩa như sau:

♦ *Lộ khoá (Key Compromise)*: Chứng chỉ của một thực thể cuối bị huỷ bỏ vì lý do lộ khoá hoặc nghi ngờ lộ khoá.

♦ *Lộ khoá của CA (CA Compromise)*: Chứng chỉ của một CA bị huỷ bỏ vì lý do lộ khoá hoặc nghi ngờ lộ khoá.

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

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

Trường mở rộng Mã lý do có hai giá trị đặc biệt:

♦ *"Loại bỏ khỏi CRL" (Remove from CRL)* được trình bày trong mục Delta-CRL.

♦ *"Treo chứng chỉ" (Certificate Hold)* được trình bày trong mục "Treo chứng chỉ".

Cả hai trường mở rộng của chứng chỉ là Tên khoá của CA phát hành (*Authority Key Identifier*) và Tên lựa chọn của người phát

hành (*Issuer Alternative Name*) (đã được trình bày trong mục 4.5) cũng có thể được sử dụng làm trường mở rộng của CRL. Chúng 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 một CRL và xử lý nó (như kiểm tra 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.

Một entry được đưa vào CRL khi có thông báo thu hồi. Số lượng thông báo thu hồi không thể đoán trước được nhưng 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 giữ 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 người sử dụng cuối, một CRL cho các CA khác và cả hai đều được chứng thực. CRL sau thường rất ngắn (có thể 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, URL hoặc 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 (tùy thuộc vào các lý do thu hồi khác nhau), với các thu hồi thông thường (ví dụ do thay đổi tên) có thể được xếp vào một CRL khác so với các thu hồi do lộ khoá. Tùy 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 điểm (hoặc nhiều điểm) phân tán các CRL. Để có thể kiểm tra tình trạng thu hồi, 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 với mọi lý do thu hồi, hoặc một CRL với một tập hữu hạn lý do thu hồi. Trường mở rộng này không cần chỉ báo "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.

- ♦ *Các điểm phân tán phát hành (Issuing Distribution Points)*: là một trường mở rộng của CRL, nó chỉ ra tên của điểm phân tán CRL cụ thể này, đồng thời chỉ ra nếu CRL 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 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, một đối tượng tấn công có thể lấy một CRL rỗng từ điểm A thay thế cho một CRL không rỗng ở điểm B, do 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 thông tin về các chứng chỉ bị thu hồi.

Việc sử dụng các Delta-CRL phụ thuộc vào một trường mở rộng của CRL là trường Chỉ báo Delta-CRL (*Delta-CRL Indicator*), nó nhận dạng 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 Mã lý do (*Reason code*). Giá trị "Loại bỏ khỏi CRL" (*Remove from CRL*) cho biết cần loại bỏ một đầu vào 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 Các điểm phân tán CRL (*CRL Distribution Points*). Trường mở rộng Các điểm phân tán CRL là trường tùy chọn, được sử dụng để nhận dạng người phát hành CRL khi người phát hành CRL này khác với 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 ủy quyền.

Trong một CRL gián tiếp, một chỉ báo đặc biệt được thiết lập trong trường mở rộng Các điểm phân tán phát hành (*Issuing Distribution Points*). Nó cho biết người sử dụng chứng chỉ cần kiểm tra người phát hành chứng chỉ đối với mọi đầu vào có trong CRL. Người sử dụng không thể tin tưởng rằng, người phát hành CRL phát hành tất cả các đầu vào (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 sung thêm và được định nghĩa như sau:

Người phát hành chứng chỉ (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 đầu vào đầu tiên của một CRL gián tiếp, đối với đầu vào này, người phát hành chứng chỉ mặc định là người phát hành CRL. Trên các đầu vào 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 đầu vào trước đó. Các quy tắc ngầm định là 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 mình 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 đáp ứng yêu cầu này, uỷ ban ANSI 19 đưa ra một cơ chế treo chứng chỉ. Tình trạng treo được thông báo qua một giá trị đặc biệt, "Treo chứng chỉ" (*Certificate Hold*), giá trị này nằm trong trường Mã lý do. Ở đây có thêm một trường mở rộng của CRL entry liên quan đến việc treo chứng chỉ 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 CẬP 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 thời gian hợp lệ, nó phản ánh khoảng thời gian tồn tại của 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) Danh sách các chứng chỉ bị thu hồi sẽ được CA công bố.

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 tùy 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 trường hợp sau:

(a) *Sự phê chuẩn mang tính thời điểm (Historic validation)*: 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 (Real-time validation)*: 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 gắn 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 chứa 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 phiên bản 3 của X.509 có sử dụng một trường mở rộng, được gọi là "Khoảng thời gian sử dụng khoá riêng" (*Private-key Usage Period*).

Ngoài ra, trường này có thể làm tăng tính 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 (của 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 Khoảng thời gian sử dụng khoá riêng (*Private-key Usage Period*) chỉ cho phép sử dụng khoá riêng trong năm đầu tiên. Tuy 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 chúng 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 khoá dùng để ký của CA chỉ là một trong các trường hợp về các cặp khoá dùng cho mục đích ký số. Tuy nhiên, chữ ký của chúng chỉ có khả năng làm cầu nối giữa hai trường hợp 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 trong thời gian thực" cũng rất cần thiết. Những người sử dụng chúng chỉ thường yêu cầu và có quyền nhận được các thông tin thu hồi mới nhất đối với tất cả các chứng chỉ đang thực sự được sử dụng của CA. Vì vậy, việc sử dụng trường Khoảng thời gian sử dụng khoá riêng (*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 kết một khoá công khai với một người, một thiết bị hoặc một thực thể bằng cách đưa tên hoặc các thông tin nhận dạng 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 hay không.

Việc phân tán các thông tin uỷ quyền cũng có thể thực hiện thông qua việc sử dụng 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 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 mang các thông tin uỷ quyền; ví dụ, trường Các ràng buộc cơ bản (*Basic Constraints*) uỷ quyền cho thực thể cụ thể hoạt động như CA. Rõ ràng là các chứng chỉ đều chứa thông tin uỷ quyền của chủ thể, ví dụ, các thuộc tính trong trường Các thuộc tính thư mục của chủ thể (*Subject Directory Attributes*) hoặc các trường mở rộng phi chuẩn 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 người được 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 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 dạng này có thể là tên hoặc tham chiếu đến chứng chỉ khoá công khai (kết hợp cả tên người phát hành và số hiệu chứng chỉ X.509).

(c) *Người phát hành (Issuer)*: Tên của bộ phận hay cơ quan 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 của chứng chỉ này. Số hiệu này được cơ quan phát hành chứng chỉ 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 quá trình chứng thực. Các thông tin này có thể được chủ thể, cơ quan phát hành chứng chỉ thuộc tính hoặc thành viên thứ ba cung cấp, tùy thuộc vào kiểu thuộc tính đặc thù.

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

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

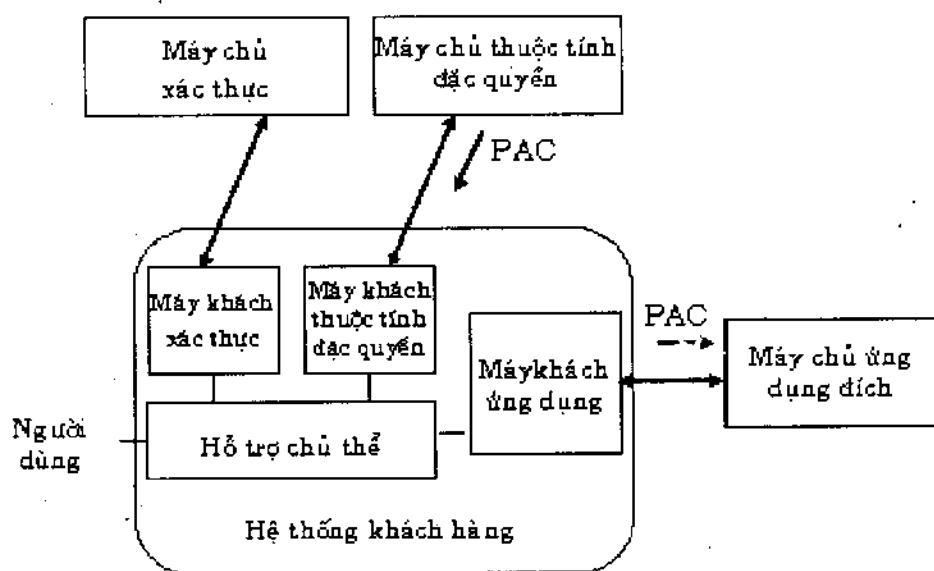
Các chứng chỉ thuộc tính tạo thành một cơ chế mục đích chung, có nhiều sử dụng. Việc phân tán các thông tin uỷ quyền được chứng thực là một trong các sử dụng này. Để hỗ trợ việc sử dụng các chứng chỉ thuộc tính, ANSI 19 đang phát triển một chuẩn, trong đó định nghĩa một tập hợp các thuộc tính liên quan 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.

Các chứng chỉ thuộc tính chiếm một mảng rất quan trọng trong 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 khách truy nhập vào các hệ thống máy chủ có hỗ trợ nhiều ứng dụng cần thiết. Các tổ chức khác nhau điều hành các hệ thống máy chủ này. Cấu hình được minh họa trong hình 4.10. Quá trình xác thực sử dụng cơ chế xác thực máy khách-máy chủ, chẳng hạn như cơ chế Kerberos. Cơ chế này như sau: 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.



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

PAC là một cấu trúc dữ liệu, cấu trúc này được một máy chủ tin cậy sinh ra trong miền 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.

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, ngoại trừ người giữ hợp lệ.

Trong các môi trường này, các thiết kế ban đầu đều sử dụng mã hoá đối xứng. Trong các phát triển mới đây, mã hoá 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 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 Danielle có thể gán tên cho tất cả những người làm công của công ty, chẳng hạn 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 vấn đề 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 công 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 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 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 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 chủ định hoặc người ký hay không. 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 xác 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 có được các khoá công khai của một số lớn các thành viên khác một cách đáng tin cậy, xuất phát từ thông tin về khoá công khai của một CA.

Hệ thống chứng chỉ khoá công khai phụ thuộc vào khoá riêng tương ứng với khoá công khai được chứng thực có trong chứng chỉ, chủ thể của chứng chỉ được sử dụng khoá này. 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 phối cho những người dùng cuối thông qua các dịch vụ thư mục, các máy chủ hoặc kho lưu giữ, hoặc gắn vào tài liệu 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, đưa ra nhiều đặc tính mới và tùy 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, chứng chỉ cần bị huỷ bỏ. Giải pháp thông báo thu hồi phổ biến nhất là 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 thu hồi khác cũng có thể được sử dụng, ví dụ truyền thông 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 hiện thời của chứng chỉ, chẳng hạn thu hồi tạm thời (treo) hoặc thu hồi vĩnh viễn (huỷ bỏ).

Việc phân tán các thông tin uỷ quyền là một yêu cầu khác với yêu cầu gắn kết một khoá công khai với một nhận dạng nào đó, nhưng chứng chỉ có thể đáp ứng được yêu cầu này. Một cơ quan được công nhận có thể phát hành một chứng chỉ, công bố rằng một người 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 chứng chỉ X.509 có trong phiên bản 3, chứng chỉ thuộc tính (được ANSI định nghĩa), 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 sở hạ tầng khoá công khai đơn giản (SPKI):

CHƯƠNG V

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 (Giao dịch điện tử an toàn) của MasterCard/Visa (được sử dụng trong thanh toán sử dụng thẻ ngân hàng trên Internet) và MISSI (Khởi sinh an toàn hệ thống thông tin đa mức) 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 (Scalability)*: 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 (Support for multiple applications)*: 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 tệp.

(c) *Khả năng liên vận hành của các cơ sở hạ tầng được quản trị tách biệt (Interoperability of separately administered infrastructure)*: 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 (Support for multiple policies)*: Các đường dẫn chứng thực thích hợp với một ứng dụng, không nhất thiết phải thích hợp với ứng dụng khác. (Ví dụ, chúng 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 (Simply risk management)*: 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) *Các chuẩn (Standards)*: 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

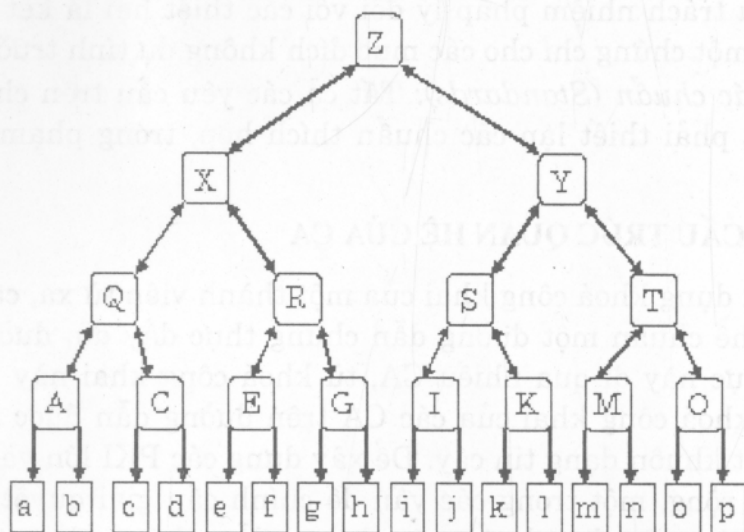
Khi sử dụng khoá công khai của một thành viên từ xa, cần phải tìm và phê chuẩn một đường dẫn chứng thực đầy đủ, đường dẫn chứng thực này đi qua nhiều CA, từ khoá công khai này tới một CA gốc, khoá công khai của các CA trên đường dẫn được lưu giữ trong một khuôn dạng tin cậy. Để xây dựng các PKI lớn và 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.

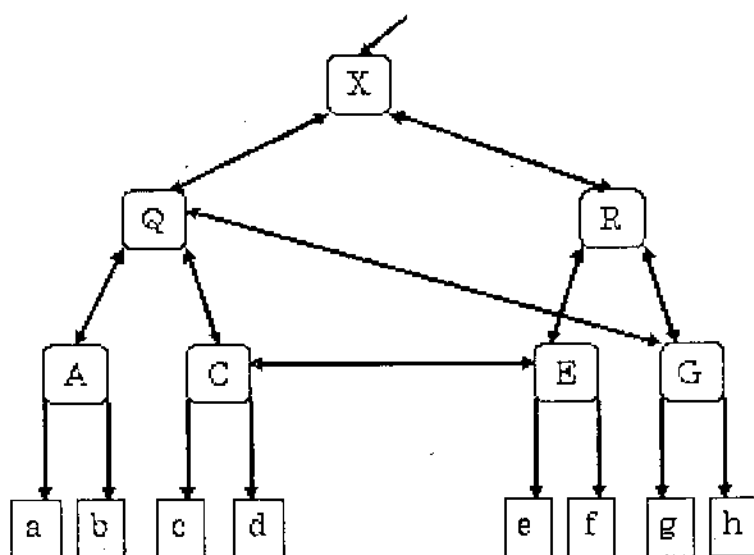
Một vấn đề xuất hiện trong cấu trúc phân cấp này là nhiều đường dẫn chứng thực mong muốn được đi qua các CA ở mức cao hơn, đặc biệt là CA mức cao nhất, đó là Z . Vì vậy, tất cả các thành viên trong cơ sở hạ tầng cần tin cậy Z . Nếu một đối tượng tấn công có được khoá riêng của Z thì đối tượng tấn công 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.

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 sung

Cấu trúc phân cấp mang lại cho chúng ta một cách thích hợp để 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 sung 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 sung. 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 sung

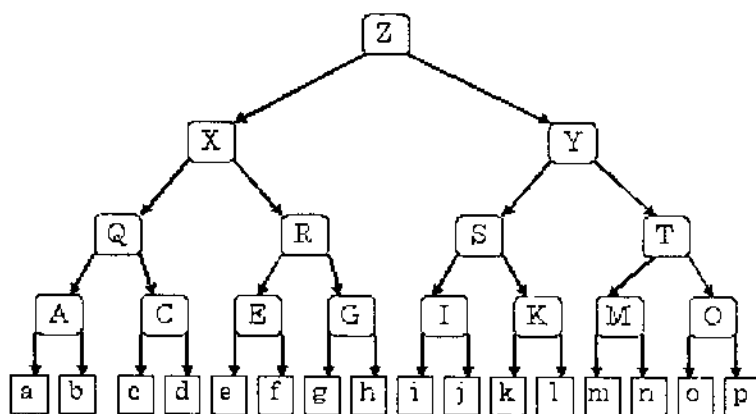
Các liên kết bổ sung kiểu như vậy không phải là một phần của cấu trúc phân cấp cơ bản, đôi khi chúng được gọi là các chứng chỉ chéo. Liên kết giữa *C* và *E* có nghĩa là ở đây hiện có một đường

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 sung 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 sung và khuyến khích sự ngầm định này.

5.2.3 Cấu trúc phân cấp trên - xuống

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, dùng trong gửi tin quân sự an toàn. Cấu trúc này được gọi là cấu trúc phân cấp trên - xuống, được minh hoạ trong hình 5.3.



Hình 5.3 Cấu trúc phân cấp trên xuống

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).

Cấu trúc này có một số ưu thế quan trọng bao gồm:

- ♦ 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.

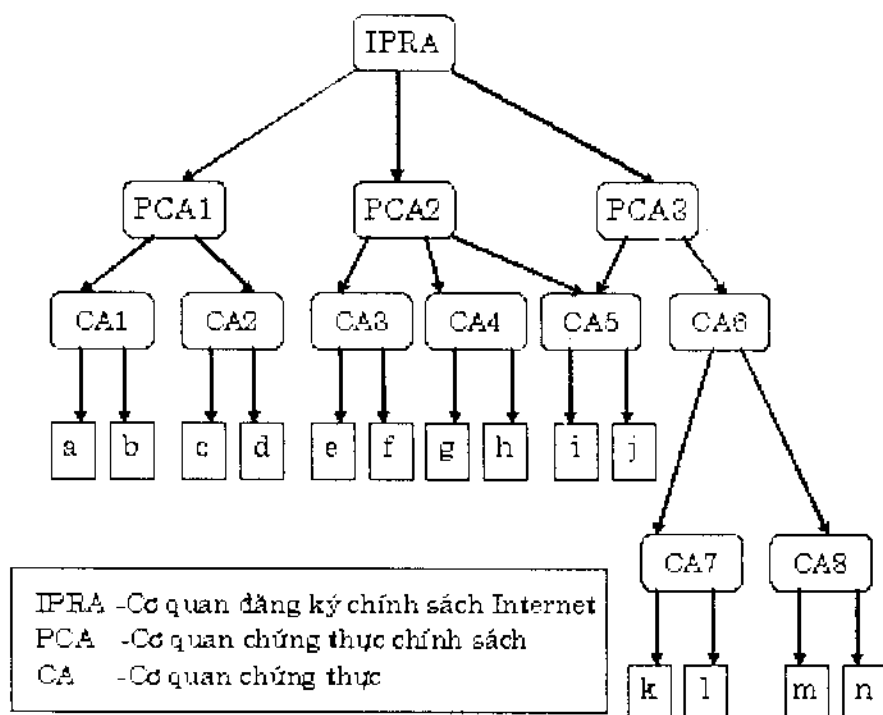
5.2.4 Cơ sở hạ tầng PEM

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 trên - xuống 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 đề quan trọng.

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 (Viện công nghệ Massachusetts) điều hành dưới sự bảo trợ của Hiệp hội Internet (Internet Society). Nó phân phối khoá công khai gốc một cách rộng rãi và chứng thực các cơ quan chứng thực chính sách.



Hình 5.4 Cơ sở hạ tầng PEM

(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. 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, hoặc các vùng địa lý riêng.

Ở đây có một biến thể của cấu trúc phân cấp trên - xuống. 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 có thể kết hợp với các CA mức thấp hơn:

(a) *CA của 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 kết hợp 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.

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* cho 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

lôgic, các hệ thống sử dụng chúng chỉ sẽ tự động phát hiện sự không hợp lệ và loại bỏ chúng 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 sung hai đặc tính quan trọng cho cấu trúc phân cấp trên - xuống 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 lỗi, bị thoả hiệp (làm lộ khoá) hoặc thiếu tinh thần trách nhiệm.

5.2.5 Các cây phân cấp

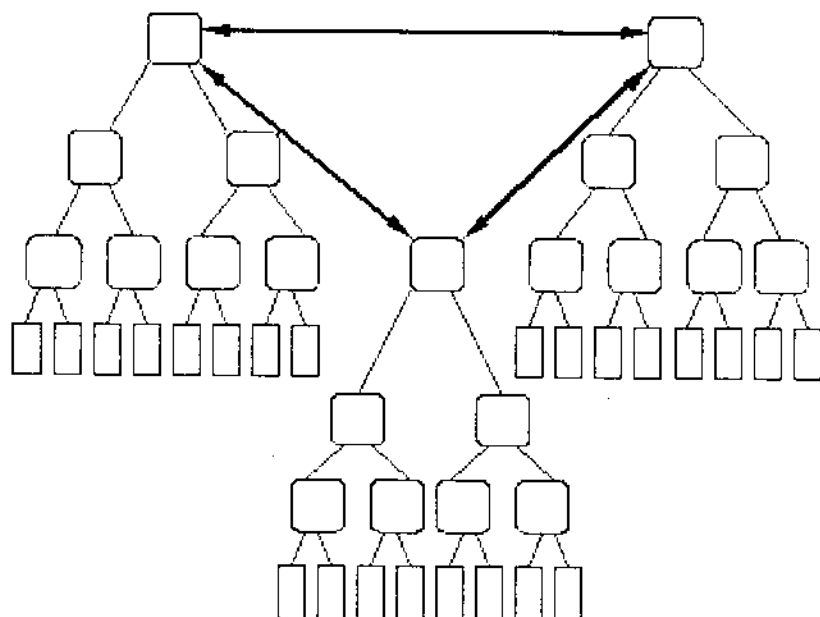
Có một vấn đề chính trong các cấu trúc phân cấp là một thành viên nào đó trong hệ thống phân cấp có thể không chấp nhận một cơ quan có thể được tin cậy cho tất cả các mục đích định trước. Ví dụ, chúng ta xem xét các cấu trúc phân cấp trong chính phủ của một nước, hệ thống phân cấp có thể hợp lý hoàn 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.



Hình 5.5 Các cây phân cấp

Liên kết một số lượng nhỏ các cấu trúc phân cấp trên - xuống 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, tùy 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.

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 tùy 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. Một người sử dụng PGP cần lưu giữ một tập hợp các khoá công khai của những người sử dụng khác trong một tệp, tệp này được lưu giữ cục bộ và được gọi tên là một "vòng khoá" (*key ring*). Việc lưu giữ các khoá như vậy cho biết:

- ♦ Trong bất cứ trường hợp nào, người dùng cũng quan tâm đến tính hợp lệ của khoá;

- ♦ Mức độ tin cậy của người dùng dành cho khoá này với mục đích chứng thực các khoá công khai của những người sử dụng khác.

Khi một người sử dụng xác định được khoá là hợp lệ thì lưu nó vào "vòng khoá" của mình, 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, người dùng 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*: Nếu báo khoá theo cách này, lập tức PGP sẽ hỏi người dùng mỗi khi PGP cần sử dụng khoá này để kiểm tra việc chứng thực trên khoá khác rằng người dùng có tin cậy khoá được sử dụng cho mục đích này hay không.

- ♦ *Không*: PGP sẽ không sử dụng chứng chỉ phụ thuộc vào khoá được sử dụng cho mục đích kiểm tra này.

- ♦ *Thông thường*: Người dùng báo sự tin cậy của mình là "bên lề" (*marginal*). 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 có thể tìm ra hai chứng chỉ bên lề khác nhau dành cho một khoá công khai, phần mềm PGP sẽ xem khoá công khai 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*: PGP sẽ tự động chấp nhận và sử dụng một chứng chỉ được kiểm tra bằng khoá công khai này.

Sơ sánh với các cấu trúc CA không mềm dẻo (đã trình bày trong các mục trước), 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 thư tín điện tử cá nhân khi truyền trên Internet. 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, có thể xảy ra 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 bắt 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. Chẳng hạn 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.

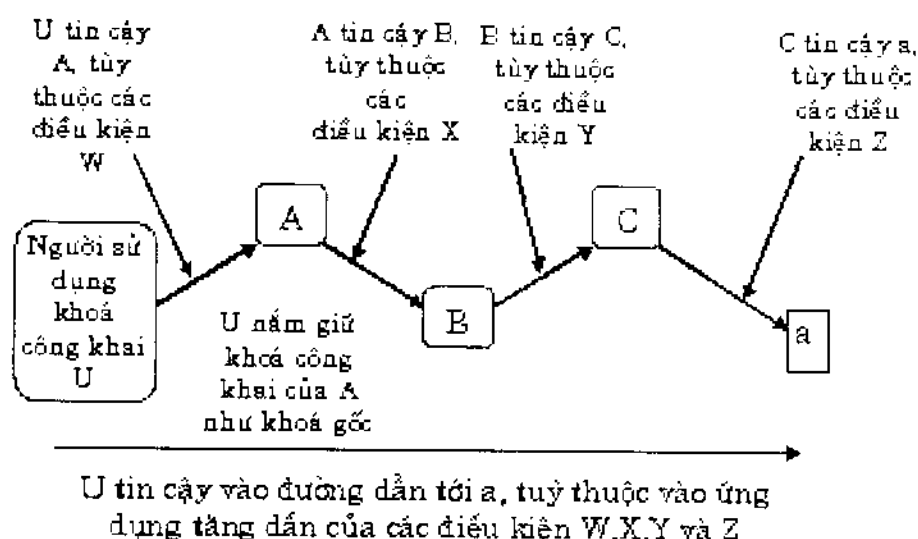
Để trung thành với các giới hạn tin cậy trên, hệ thống sử dụng chứng chỉ có thể chứng thực các giới hạn này một cách tự động, như là một phần của quá trình phê chuẩn đường dẫn chứng thực.

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 cậy 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

dầu tiên, người sử dụng khoá công khai gắn các điều kiện tin cậy của mình đối với CA (có nghĩa là *U* tin cậy *A*). Đối với các giai đoạn còn lại cũng làm tương tự như vậy, 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 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 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.



Hình 5.6 Mô hình tin cậy ràng buộc tăng dần

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.

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 của mô hình tin cậy ràng buộc tăng dần. Tuy nhiên, cấu trúc này còn có một số hạn chế như sau:

- ♦ Hệ thống phân cấp trên - xuống 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 miền 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, miền của người sử dụng là miền 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.

- ♦ 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 dụ, giả thiết công ty thép Sharon có một văn phòng chính tại Mỹ và một văn phòng chi nhánh tại Anh. Các tên tự 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 công ty này 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.

- ♦ 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 Internet, 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 độ tin cậy của CA. Việc làm lộ khoá riêng của CA có thể gây ra những hậu quả nghiêm 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 cho phép một khoá công khai được nhiều người chứng thực. Điều này tạo ra các chứng chỉ bên lề (*marginal certificate*). Các chứng chỉ này 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, thì cũng sẽ không an toàn. 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 phát hành một chứng chỉ, CA công bố với người sử dụng rằng khoá công khai có trong chứng chỉ dành cho một thực thể cụ thể (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 chỉ phí thấp hơn chiếm ưu thế. Vì vậy, các chứng chỉ được phát hành tùy thuộc vào các chính sách và các thủ tục khác nhau và có thể phù hợp với các mục đích khác nhau.

CA công bố các hoạt động và thủ tục chứng thực trong một tài liệu có tên là CPS (Các quy định hoạt động chứng thực).

X.509 có một số đặc tính tùy 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 được phát hành phù hợp với một chính sách riêng; hoặc nhiều 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

và / hoặc lớp các ứng dụng có các yêu cầu an toàn chung.

Ví dụ, một chính sách chứng chỉ 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 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 việc 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 USD. 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 Các chính sách chứng chỉ (Certificate Policies)

Trong phiên bản 3 của chứng chỉ X.509, trường mở rộng Các chính sách chứng chỉ (*Certificate Policies*) được sử dụng 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 chỉ rõ một hệ thống sử dụng chứng chỉ phải xử lý trường mở rộng Các chính sách chứng chỉ (*Certificate Policies*) như thế nào.

Trường mở rộng này có hai biến, một trong hai biến được chỉ báo là "thiết yếu", biến còn lại được chỉ báo "không thiết yếu". Chúng ta cần tìm hiểu sự khác nhau giữa hai trường hợp vì nó rất quan trọng. Trường chỉ báo "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 phân 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 chỉ báo "không thiết yếu" được thiết kế và 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 USD, 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 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 Các chính sách chứng chỉ (*Certificate Policies*) được chỉ báo "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 USD, 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?

Bất chấp có chỉ báo "không thiết yếu" hay "thiết yếu", trường mở rộng Các chính sách chứng chỉ (*Certificate Policies*) có dự phòng cho việc chuyển thêm thông tin liên quan đến chính sách chứng chỉ (cùng với tên chính sách chứng chỉ) trong trường *qualifier*. Chuẩn không quy định trường *qualifier* phải được sử dụng cho mục đích nào. 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 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* sẽ trở nên hữu ích khi đạt được các thoả thuận về 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 (Policy Mapping)

X.509 định nghĩa trường mở rộng Ánh xạ chính sách (*Policy Mapping*), dùng khi một chứng chỉ được sử dụng để liên kết hai miền 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 xác định nào đó trong miền của CA được quan tâm ngang bằng với các chính sách xác định khác có trong miền khác.

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 miền 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 Ánh xạ chính sách (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 Ánh xạ chính sách (*Policy Mapping*) thường được chỉ báo "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.

5.3.4 Mở rộng Các ràng buộc chính sách (Policy Constraints)

Nó gồm có hai trường chỉ báo tùy chọn, được dùng với mục đích riêng, như sau:

(a) *Chỉ báo yêu cầu chính sách tường minh (Require Explicit Policy indicator)*: CA yêu cầu thông báo tên chính sách được chấp nhận phải xuất hiện trong tất cả các chứng chỉ trên đường dẫn chứng thực và tên này phải rõ ràng. Tùy chọn này hữu ích trong một số trường hợp như sau: trong miền 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 xuất hiện 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 chứng 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 yêu cầu chính sách tường minh (*Require Explicit Policy*).

(b) *Chỉ báo ngăn cấm ánh xạ chính sách (Inhibit Policy Mapping indicator)*: 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 (Community and applicability restrictions)*: 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 (Identification and authentication policy)*: 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 (Key Management policy)*: 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 (Operational policy)*: 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 (Local security policy)*: 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 (Legal provisions)*: Đây là một công bố về các giới hạn trách nhiệm pháp lý (CA xác nhận công bố này), chẳng hạn, sử dụng các chứng chỉ theo một chính sách riêng, 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 tùy 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 tùy 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, bao gồm các địa chỉ thư điện tử trên Internet và các tên miền của Internet. IETF (Tổ công tác kỹ thuật Internet) và PKIX (Nhóm nghiên cứu cơ sở hạ tầng khoá công khai) xác 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

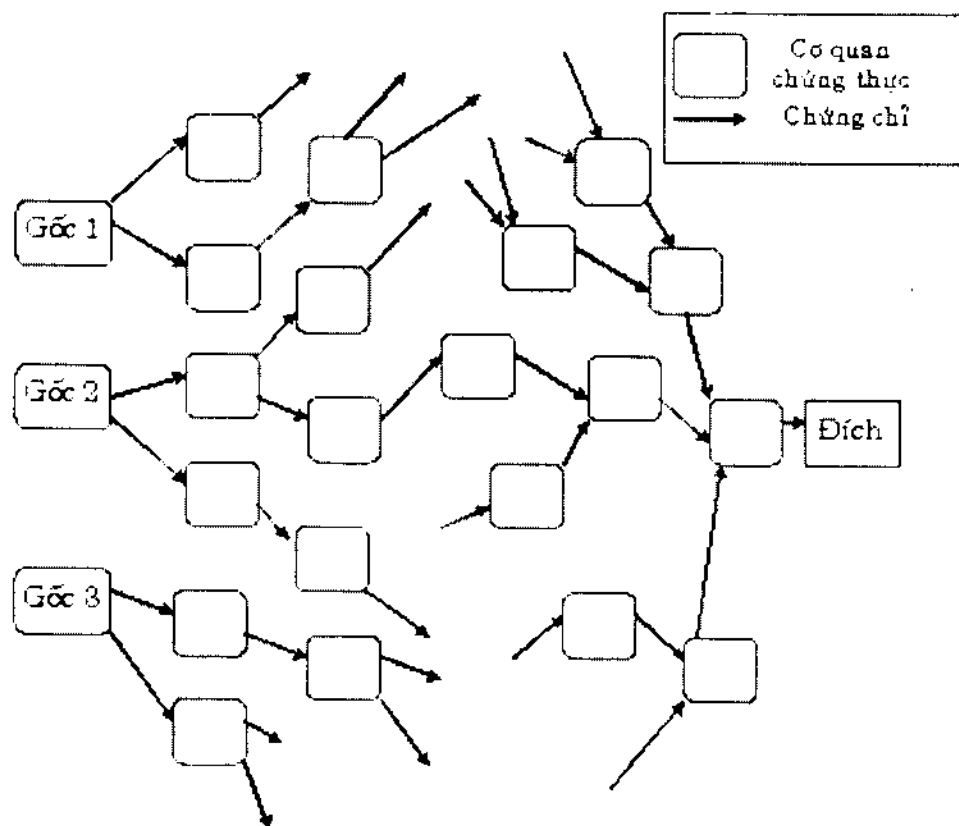
Hai vấn đề quan trọng cần được quan tâm nhiều nhất trong thiết lập các hệ thống khoá công khai trên phạm vi lớn là làm thế nào để tìm được một đường dẫn chứng thực thích hợp và khi tìm được rồi thì phê chuẩn nó như thế nào. Các chức năng này phải được thiết lập trong tất cả các hệ thống sử dụng chứng 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, tùy thuộc vào cấu trúc quan hệ của các CA và vào các thông tin bổ sung 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*). Điều này được minh hoạ trong hình 5.7.



Hình 5.7 Vấn đề tìm đường dẫn chứng thực tổng quát

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 này, 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 bước 1 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).

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 trên - xuống 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 tình trạng của 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 đối với 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 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 sung có thể giải quyết hiệu quả một số tình trạng pháp lý không rõ ràng. Thêm vào đó, các khối xương 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, luật chữ ký số phải quy định được: các truyền thông điện tử và các bản ghi được ký số là hợp pháp và có hiệu lực như các tài liệu được ký truyền thống. Luật chữ ký số 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 khác cũng đã ban hành luật chữ ký số, ví dụ như Đức, Đan mạch và Ý.

5.7.1 Công nghệ

Một số 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 xuất 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.

Một số luật khác 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 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, việc ban hành luật này 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

(a) 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.

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 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 sung 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 lưu giữ được tổ chức lại

5.7.3 Các văn bản và chữ ký

Yêu cầu tối thiểu đối với 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 trong luật của Utah là các nguyên tắc điển hình:

Mục 401. Thỏa mãn các yêu cầu chữ ký. (1) Với 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 (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. (1) Một thông báo hợp lệ và có hiệu lực như khi nó được thảo thành văn bản (trên giấy) nếu nó:

- (a) Chứa toàn bộ chữ ký;
- (b) Chữ ký số này được kiểm tra bằng cách sử dụng 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 công nghệ 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.

Luật chữ ký số (ví dụ 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 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 có nên yêu cầu cấp phép trong phạm vi quyền hạn, hoặc đơn giản

chỉ cung cấp đặc quyền giữa các nước 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 hỗ trợ 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. 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. 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 sẻ 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. 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 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 bị lỗi hoặc bị làm giả một khi CA đã 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, chẳng hạn như:

(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 nguyên tắc 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 họa 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 (MISSI), 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 tổ chức đại diện (chẳng hạn như Visa và MasterCard).

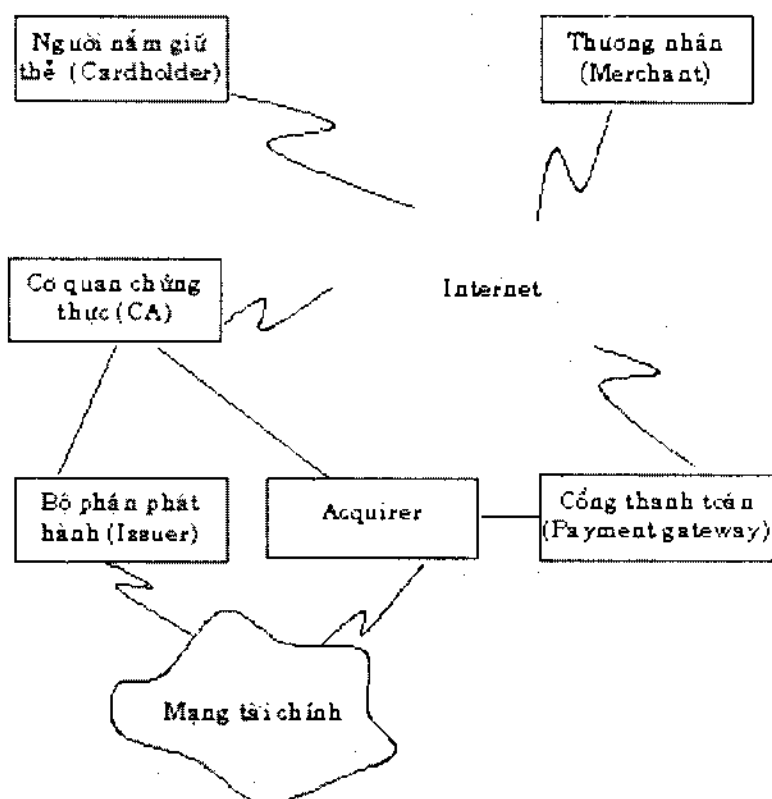
(b) *Người nắm giữ thẻ (Cardholder):* là người nắm giữ thẻ ngân hàng hợp pháp, anh ta đã đăng ký với bộ phận phát hành tương ứng để tiến hành thương mại điện tử.

(c) *Thương nhân (Merchant)*: là người bán hàng, hoặc tổ chức có hàng hoá, dịch vụ hoặc thông tin bán cho người nắm giữ thẻ.

(d) *Cơ quan Acquirer*: là một cơ quan tài chính hỗ trợ các thương nhân 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 nhân. Hệ thống được điều hành bởi một Acquirer hoặc một thành viên khác (hỗ trợ các Acquirer); Thông thường, cổng thanh toán cần có giao diện với Acquirer để hỗ trợ xác thực và giành được các giao dịch.

(f) *Các cơ quan chứng thực (Certification authorities)*: là một thành phần của cơ sở hạ tầng, chứng thực khoá công khai của người nắm giữ thẻ, thương nhân, và/hoặc Acquirer, hoặc các cổng.



Hình 5.8 Các thành phần trong môi trường SET

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 nhân, anh ta gửi cho thương nhân một chỉ dẫn thanh toán. Thương nhân 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.

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 nhân (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 nhân 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 nhân hợp pháp và tiến hành các giao dịch gian lận;

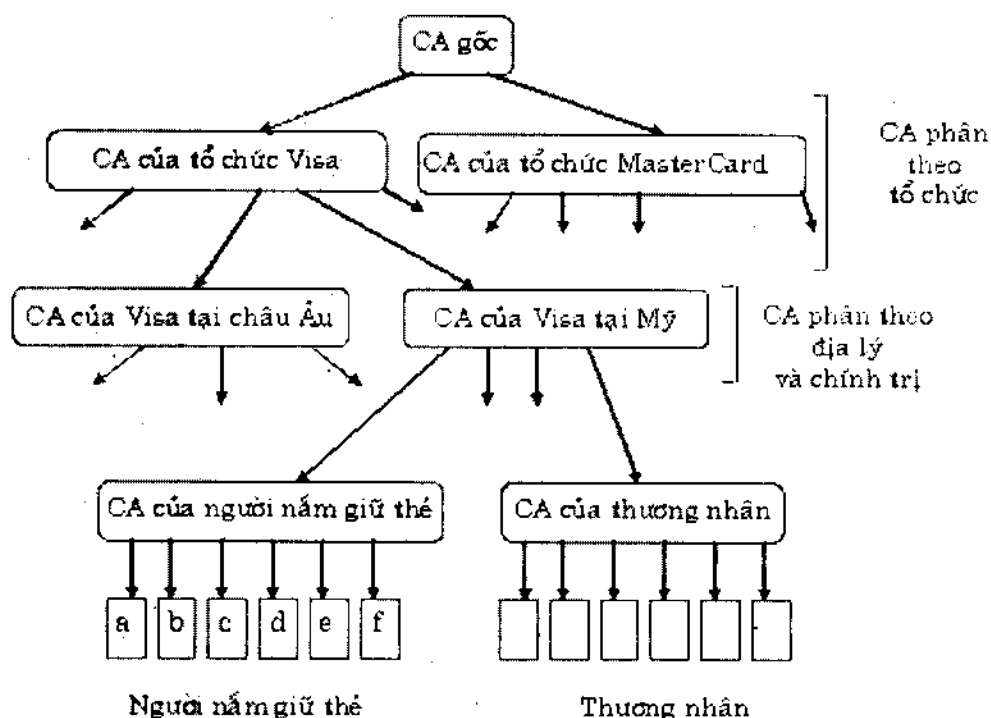
- ♦ Việc xác thực các Acquirer cho người nắm giữ thẻ và thương nhân nhằm bảo vệ, không cho phép bất kỳ người nào tự nhận mình là một Acquirer có khả năng giải mã các thông tin nhạy cảm có trong chỉ dẫn thanh toán;

- ♦ 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 trên - xuống, bao gồm các kiểu CA như sau:

(a) *CA gốc (Root CA)*: Tất cả các đường dẫn chứng thực bắt đầu

với khoá công khai của CA gốc. CA này được cách ly an toàn, rất hiếm khi được truy nhập vào, nó phát hành các chứng chỉ cho các CA của tổ chức. 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.



Hình 5.9 Cơ sở hạ tầng khoá công khai SET

(b) *CA phân theo tổ chức (Brand CA)*: Các CA này được điều hành bởi chính các tổ chức khác nhau, ví dụ như Visa và MasterCard. Mỗi tổ chức có quyền tự trị rất lớn để có thể quản lý được các chứng chỉ mức thấp hơn.

(c) *CA phân theo địa lý và chính trị (Geo-political CA)*: Mức CA này (tuỳ chọn) cho phép một tổ chức 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) *CA của người nắm giữ thẻ (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. Tùy thuộc vào các quy tắc của tổ chức, 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) *CA của thương nhân (Merchant CA)*: Các CA phát hành các chứng chỉ cho các thương nhân, dựa vào sự chấp thuận của một Acquirer. Tùy thuộc vào các quy tắc của tổ chức, CA có thể được điều hành bởi một Acquirer hoặc một thành viên khác.

Hệ thống phân cấp trên - xuống 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 (Cơ quan an toàn Quốc gia) 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.

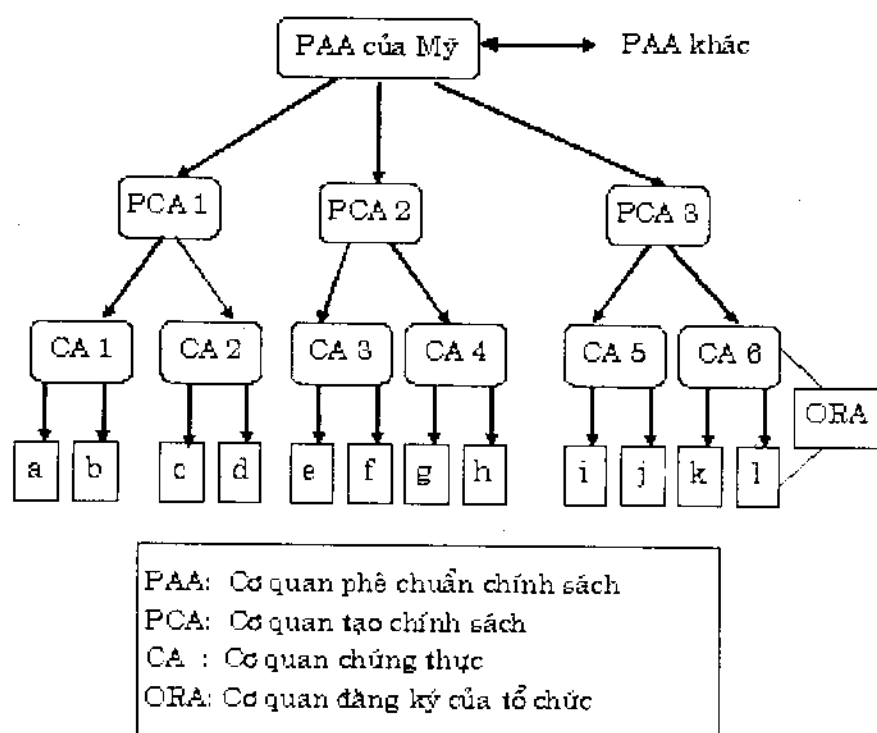
Một ứng dụng cho cơ sở hạ tầng này là DMS, hỗ trợ gửi tin trong quân sự, gửi đi các thông tin nhạy cảm nhưng chưa được xếp vào loại mật và các thông tin được phân loại ở mức thấp hơn. Tuy nhiên, cấu trúc MISSI không bị hạn chế.

Cơ sở hạ tầng MISSI có mối liên quan chặt chẽ với thiết kế Internet PEM, được minh hoạ trong hình 5.10.

Các thành phần ban đầu trong cơ sở hạ tầng này (một ví dụ khác của hệ thống phân cấp trên - xuống) 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 kế

dưới và cho phép chứng thực chéo các PAA khác trong các miền riêng lẻ hoàn toàn.



Hình 5.10 Cơ sở hạ tầng khoá công khai MISSI

(b) *Cơ quan tạo chính sách (PCA)*: Mỗi PCA là gốc quản trị dành cho miền chính sách an toàn riêng lẻ.

(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 miền chính sách. CA đăng ký các thực thể cuối và phát hành các chứng chỉ của mình.

(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 những thông tin đó cho CA.

Cơ sở hạ tầng MISSI là trường hợp có cấu trúc phân cấp trên -

xuống 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 CA gốc. Các liên kết chứng thực bổ sung giữa các nút có thể được thêm vào nhằm cải thiện hiệu năng. Cấu trúc phân cấp trên - xuống có điểm khác biệt là tất cả các đường dẫn chứng thực đều bắt đầu từ một CA gốc và tất cả những người sử dụng phải tin cậy CA này. Nếu mỗi 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 trên - xuống với các đặc tính bổ sung để liên kết các chính sách với các đường dẫn chứng thực và tuân theo các không gian tên của chủ thể. Với Web of trust, 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 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.

Chính sách chứng chỉ được sử dụng để chỉ ra cho người sử dụng biết chứng chỉ có được sử dụng 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 miền quản trị. Trường *qualifier* có thể chứa các thông tin bổ sung về chính sách, ví dụ một con 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 do 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 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 thực hiện 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 nhiều nước trên thế giới, 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/Master Card (dùng để hỗ trợ các thanh toán sử dụng thẻ ngân hàng) và PKI của Bộ Quốc phòng Mỹ, MISSI (dùng để hỗ trợ thư tín điện tử an toàn và các ứng dụng khác của chính phủ).

CHƯƠNG VI

QUY ĐỊNH HOẠT ĐỘNG CHỨNG THỰC

Trong an toàn thương mại điện tử, CA đóng một vai trò quan trọng. Các thành viên có thể sử dụng các chữ ký số và mã hoá một cách sự tin cậy nếu một CA tin cậy có thể đảm bảo tính xác thực và toàn vẹn của các khoá công khai. Tuy nhiên, CA chỉ có thể có hiệu lực khi các dịch vụ của nó được công nhận là thực tế, tin cậy và hợp pháp. Sự công nhận này phụ thuộc vào các hoạt động được CA đưa vào tài liệu có hiệu lực đối với mọi thành viên liên quan. Xuất phát từ mục đích này, ABA (American Bar Association) đã phát triển khái niệm "Quy định hoạt động chứng thực" (viết tắt là CPS). Trong chương này, chúng ta xem xét các hoạt động chứng thực, các CPS và các chủ đề điển hình thường được đưa vào một CPS. Chúng ta có thể bắt đầu với việc xem xét khái niệm CPS và các khái niệm khác, chẳng hạn như khái niệm "Chính sách chứng chỉ" của X.509, mối quan hệ giữa chúng như thế nào. Sau đó, chúng ta xem xét các vấn đề hoạt động khác mà một CA cần quan tâm và các vấn đề cần có trong một CPS.

6.1 KHÁI NIỆM

Quy định hoạt động chứng thực

Quy định hoạt động chứng thực (*Certification Practice Statement*, viết tắt là CPS) là các quy định mà cơ quan chứng thực tuân theo khi phát hành các chứng chỉ, với mỗi CA có một CPS cụ thể.

CPS thực sự có giá trị đối với từng CA, đặc biệt trong môi trường mở, các CA thương mại đóng vai trò là thành viên thứ ba tin cậy, đáp ứng yêu cầu của các tổ chức và cá nhân khác (đối tượng nắm giữ các khoá riêng, hoặc sử dụng các khoá công khai).

Trong môi trường thương mại điện tử, các rắc rối tiềm ẩn (xung

quanh mối quan hệ giữa các thực thể) tạo ra các vấn đề pháp lý phức tạp, chúng ta không thể coi nhẹ. Một CPS toàn diện bao gồm:

- Quyền và nghĩa vụ pháp lý của các thành viên cần được đưa ra rõ ràng và đầy đủ;
- Mô tả một cách có hệ thống các khía cạnh của môi trường hoạt động;
- Công nghệ và các hoạt động được chấp nhận hiện tại.

Một số thuật ngữ

Sau đây là một số thuật ngữ (được sử dụng trong các hướng dẫn về chữ ký số của ABA, hoặc các CPS thương mại) trong hoạt động chứng thực:

➤ Đăng ký chứng chỉ (*Enrollment*): Quá trình mà người xin cấp chứng chỉ thực hiện khi xin cấp một chứng chỉ.

➤ Cơ quan phát hành (*Issuing Authority*): Thuật ngữ này tương đương với thuật ngữ cơ quan chứng thực (*Certification Authority*) là thực thể phát hành các chứng chỉ.

➤ Thông tin của thuê bao chưa được kiểm tra (*Nonverified subscriber information*): là thông tin được người xin cấp chứng chỉ đệ trình (gửi) cho CA. Đó là những thông tin cần thiết đối với một chứng chỉ, nhưng sự đúng đắn của chúng chưa được CA xác nhận. CA không cung cấp sự đảm bảo nào khác đối với những thông tin này, ngoài sự đảm bảo rằng thông tin này được người xin cấp chứng chỉ đệ trình lên CA trong quá trình xin cấp chứng chỉ.

➤ Thời gian hoạt động của một chứng chỉ (*Operational period of a certificate*): Thời hạn này bắt đầu tính từ ngày, giờ chứng chỉ được phát hành. Thời hạn kết thúc được chỉ ra thông qua ngày, giờ chứng chỉ hết hiệu lực hoặc bị treo, hoặc huỷ bỏ.

➤ Thành viên tin cậy (*Replying party*): là một thành viên hoạt động với sự tin cậy vào chứng chỉ và khoá công khai của chủ thể chứng chỉ.

➤ Kho lưu giữ (*Repository*): là một cơ sở dữ liệu lưu giữ các chứng chỉ và thông tin liên quan khác, có thể truy nhập vào chúng một cách trực tuyến.

➤ Thuê bao (*Subscriber*): là chủ thể của một chứng chỉ, có khả năng và được phép sử dụng khoá riêng cùng cặp với khoá công khai có trong chứng chỉ.

6.2 BIỂU DIỄN MỘT CPS

Ngữ cảnh của CPS

Một CPS được viết ra nhằm phục vụ một cộng đồng riêng, chẳng hạn như một công ty tư nhân, một chính phủ, hoặc một cộng đồng mở. CPS cần chỉ rõ phạm vi và ý nghĩa pháp lý của nó. Ví dụ, một CPS thương mại có thể chỉ rõ *"CPS này được sử dụng để ràng buộc pháp lý và cung cấp thông tin cho tất cả các thành viên tạo, sử dụng và phê chuẩn các chứng chỉ trong ngữ cảnh của [một cộng đồng được dự kiến trước]."*

Các điều khoản cần thiết có trong một CPS phụ thuộc vào cộng đồng sẽ sử dụng nó (bao gồm mục đích, kích cỡ, độ phức tạp và các ứng dụng của nó). Một CPS được sử dụng trong một cộng đồng khép kín (chẳng hạn như một hãng hoặc Bộ nào đó của Chính phủ), thường tập trung vào các mối quan tâm khác nhau.

Khuôn dạng và cấu trúc

Ở đây không có khuôn dạng chuẩn, danh sách các chủ đề chuẩn, hoặc tổ chức chuẩn cho một CPS. Hơn nữa, vấn đề chính của một CPS là sự phức tạp tiềm ẩn cần được làm rõ. Do phải so sánh các điều khoản của các CPS khác nhau (ví dụ, khi các tổ chức khác nhau quan tâm đến khả năng liên kết các dịch vụ khoá công khai của họ với nhau), sẽ thật có ích nếu tìm ra một hướng tiếp cận chung khi xây dựng nội dung của một CPS. Do vậy, chúng ta sẽ có được nhiều thuận lợi khi việc chuẩn hoá ngày càng tiến triển tốt hơn.

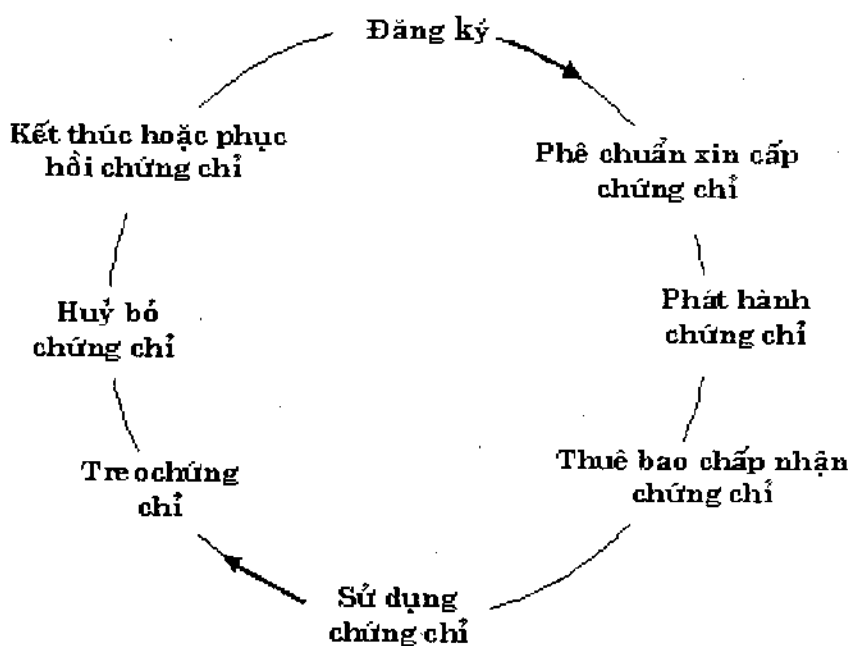
Một số đề xuất nhằm phát triển khung hoặc mẫu CPS đã được đưa ra. Các đề xuất này cung cấp tác giả của CPS với một khuôn mẫu chuẩn, trong đó đưa vào các điều khoản có thể áp dụng. Nếu tất cả các tác giả của CPS chấp thuận cùng một khuôn mẫu, hướng tiếp cận này sẽ mang lại nhiều thuận lợi, dễ dàng so sánh các CPS khác nhau và nhận ra sự giống và khác nhau giữa chúng. Điều này đặc biệt hữu ích khi các tổ chức cần phối hợp hoạt động, có nghĩa là, một tổ chức cần thừa nhận các hoạt động của các tổ chức liên quan khác. Ví dụ, nếu một tổ chức sử dụng "ánh xạ chính sách chứng chỉ X.509" (*X.509 certificate policy mapping*), phép ánh xạ này trở nên dễ dàng hơn nếu các chính sách chứng

chỉ được đưa ra theo cùng một khuôn mẫu.

Chính phủ Mỹ và Canada đã đưa ra một khung khá cụ thể cho lĩnh vực này, thúc đẩy bằng cách liên vận hành các cơ sở hạ tầng khoá công khai giữa hai nước với các quốc gia khác, với các cơ sở hạ tầng thương mại. Kết quả là đã đưa ra được một danh sách các chủ đề bao trùm lên toàn bộ CPS hoặc định nghĩa chính sách chứng chỉ.

Các tài liệu CPS được biểu diễn theo nhiều cách logic khác nhau. Chẳng hạn, theo các hướng dẫn của ABA, CPS trình bày chi tiết quyền hạn và nghĩa vụ của từng thành viên có trong đó (như CA, thuê bao và thành viên tin cậy). CPS có thể lựa chọn đưa ra quyền hạn và nghĩa vụ của các thành viên theo thứ tự mà họ xuất hiện trong chu kỳ tồn tại điển hình của một chứng chỉ.

Chúng ta tìm hiểu một hướng tiếp cận sau đây.



Hình 6.1 Chu kỳ tồn tại của chứng chỉ

Trước tiên, cơ quan chứng thực (CA) thiết lập và tiến hành các thủ tục. Sau đó, các hoạt động chung của CA (theo chu kỳ tồn tại

của chứng chỉ) như sau: xem xét đăng ký chứng chỉ (xin cấp), phê chuẩn xin cấp chứng chỉ, phát hành, chấp nhận và sử dụng chứng chỉ, treo chứng chỉ, huỷ bỏ chứng chỉ và kết thúc thời hạn tồn tại của chứng chỉ. Hình 6.1 minh hoạ chu kỳ tồn tại của chứng chỉ.

6.3 NỀN TẢNG CHO CÁC HOẠT ĐỘNG CHỨNG THỰC

Trước khi cung cấp dịch vụ, CA thương mại nên thiết lập các hoạt động pháp lý và kinh doanh tương ứng, tùy theo các yêu cầu dịch vụ của mình. Đồng thời, mô tả các biện pháp kiểm soát mà CA sẽ sử dụng để đảm bảo các hoạt động tin cậy. Ví dụ, những biện pháp kiểm soát này bao gồm: tạo và lưu giữ bí mật các khoá riêng của CA, lưu giữ bản ghi, tiến hành kiểm toán và quản lý nhân sự. Trong mục này giới thiệu các yêu cầu cơ bản dành cho một CA.

Các mức dịch vụ

Thông thường, CA nhận diện các mức dịch vụ tùy chọn khác nhau, trong phạm vi của các lớp chứng chỉ, chính sách chứng chỉ hoặc các khái niệm tương tự. Trong phạm vi của cơ sở hạ tầng mà CPS bao trùm lên, có thể có nhiều CA, mỗi CA hỗ trợ một hoặc nhiều mức dịch vụ. Các CA phát hành các chứng chỉ cho một mức dịch vụ nào đó, có thể phân biệt thông qua các dịch vụ giá trị gia tăng và các hoạt động phù hợp với các cộng đồng riêng.

Khuôn dạng chứng chỉ

Thông thường, một CA sẽ miêu tả khái lược của các chứng chỉ do CA phát hành và ý nghĩa của tất cả các trường có trong các chứng chỉ đó. Bằng cách sử dụng một khuôn dạng mục đích chung và được chuẩn hoá, chẳng hạn như khuôn dạng chứng chỉ X.509. Hiện nay, hầu hết các CA thương mại sử dụng khuôn dạng chứng chỉ X.509. Người ta có thể tìm ra các khuôn dạng chứng chỉ mới cho các ứng dụng thương mại.

Theo X.509, CA cần miêu tả các trường của chứng chỉ được sử dụng như thế nào, đặc biệt là các trường mở rộng trong phiên bản 3 của X.509. Các trường mở rộng có thể chuyển bất kỳ thông tin bổ sung nào liên quan tới khoá công khai được CA chứng thực, người phát hành chứng chỉ, thuê bao, các thành viên tin cậy và quá trình chứng thực. Ngoài ra, các trường mở rộng có thể được sử

dụng để cung cấp thông báo bổ sung, thông tin về các hoạt động của CA trong cộng đồng của người sử dụng. Tuy nhiên, chúng ta cần lưu ý khi sử dụng các trường mở rộng cho mục đích này, bởi vì không phải tất cả các ứng dụng của người dùng cuối (chẳng hạn như các trình duyệt Web) có khả năng đọc, hiển thị đúng đắn, hoặc thậm chí hoạt động dựa vào các trường mở rộng chuẩn của X.509.

Các trường mở rộng của chứng chỉ X.509 có ý nghĩa đặc biệt quan trọng đối với các hoạt động thực chứng, bao gồm:

- Chính sách chứng chỉ (*Certificate policies*): Trường này nhận diện một hoặc nhiều chính sách chứng chỉ do CA đưa ra và có hiệu lực đối với chứng chỉ này. Trường này có thể chỉ ra tên của một CPS, hoặc tên của một chính sách chứng chỉ được công nhận rộng rãi. Với trường hợp sau, ngầm định rằng chứng chỉ cũng có thể chứa một con trỏ trỏ tới CPS (nếu nó tồn tại), ví dụ trường *qualifier* của chính sách chứng chỉ. Trong bất kỳ trường hợp nào, định nghĩa chính sách chứng chỉ hoặc CPS nên chỉ rõ làm thế nào để làm sáng tỏ các trường *qualifier*.

- Các mở rộng thiết yếu khác (*Other critical extensions*, có thể được định nghĩa chuẩn hoặc riêng): Định nghĩa chính sách chứng chỉ hoặc CPS nên chỉ rõ làm thế nào để làm sáng tỏ các trường này, chỉ cần tham chiếu vào chuẩn X.509 có thể đáp ứng được điều này hay không.

Cấu trúc quan hệ của CA

Nói chung, hoạt động thực chứng phụ thuộc vào cấu trúc quan hệ giữa các CA trong một môi trường riêng. Ví dụ, cần phải chỉ rõ nếu một cấu trúc phân cấp được thực thi, hoặc các yêu cầu khi chấp nhận một CA mới vào cơ sở hạ tầng có cung cấp các dịch vụ thực chứng xác định, hay các thủ tục khi CA muốn chấm dứt mối quan hệ của mình với cơ sở hạ tầng này.

Tất cả các CA trong một cơ sở hạ tầng khoá công khai (PKI) phải tôn trọng một (hoặc nhiều) CPS. Do vậy, CPS thường có một điều khoản bắt buộc đối với tất cả các thành viên tuân theo CPS khi thực hiện các dịch vụ riêng của mình.

Đặt tên

Một số vấn đề liên quan tới phát triển cơ sở hạ tầng khoá công

khai (hoặc các ứng dụng được phân phối) vẫn không ngừng phát sinh. Thực tế, sự phức tạp và thận trọng của việc đặt tên đã tạo ra rất nhiều các vấn đề lớn cho Internet, ví dụ các vấn đề liên quan đến tính riêng tư và chúng ta có nên quản lý tất cả các tên hay không.

Các tên được sử dụng để nhận diện chủ thể chứng chỉ, chẳng hạn như số tài khoản, bí danh, hoặc chức danh của chủ thể, có ý nghĩa với cộng đồng của thuê bao. CA cần chỉ rõ ý nghĩa của các tên chủ thể (trong các chứng chỉ do CA phát hành), có thể thay đổi tùy theo lớp dịch vụ hoặc chính sách chứng chỉ.

Thông thường, trong thương mại điện tử mở, tên được sử dụng để nhận diện thuê bao tuân theo các quy định mà một hệ thống đặt tên được công nhận rộng rãi đặt ra, chẳng hạn như tên và địa chỉ cá nhân, địa chỉ thư điện tử, hoặc tên đăng ký của công ty. Các tên được một cơ quan gán cho. Tùy chọn, một tổ chức điều hành CA cũng có thể đóng vai trò như là một cơ quan gán tên. Nếu vậy, CPS nên mô tả các chính sách liên quan đến dịch vụ đăng ký tên. Lưu ý rằng, nếu CA phát hành không tự mình đóng vai trò là cơ quan gán tên, nó cần tin cậy vào các cơ quan gán tên bên ngoài, nhằm đảm bảo rằng các chứng chỉ được phát hành, cũng như các thông tin về tên có trong đó là hoàn toàn rõ ràng.

Công bố và lưu giữ

Việc công bố các chứng chỉ và thông tin liên quan là nghĩa vụ của các cơ quan chứng thực và người sử dụng chứng chỉ. Ví dụ:

- Việc công bố một chứng chỉ xác nhận rằng chủ thể của chứng chỉ đã chấp nhận nó.
- Việc công bố dữ liệu thu hồi (dành cho cộng đồng của cơ sở hạ tầng khoá công khai liên quan) xác nhận rằng các chứng chỉ đó không được tin cậy và thành viên tin cậy không nên tin tưởng vào các chứng chỉ này.
- Việc công bố một CPS nhằm ràng buộc CA và cộng đồng của cơ sở hạ tầng khoá công khai vào các hoạt động của nó.

CA duy trì một kho lưu giữ để công bố các thông tin có hiệu lực nào đó, chẳng hạn như các chứng chỉ, danh sách các chứng chỉ bị thu hồi (CRL), hoặc các thông tin khác về tình trạng treo hoặc hủy bỏ của chứng chỉ, CPS và các thông tin khác liên quan đến hoạt

động chứng thực. Kho lưu giữ thực sự cần thiết cho hoạt động của cơ sở hạ tầng khoá công khai trong một cộng đồng mở, là nơi tập trung tất cả các nguồn thông tin gắn liền với một CA. Việc phát triển kho lưu giữ lớn và dễ sử dụng không chỉ đáp ứng yêu cầu của khách hàng, mà còn có thể đảm bảo liên lạc tin cậy hơn với tất cả các thành viên.

Chứng thực liên vùng (inter-domain certification)

Trong các cơ sở hạ tầng khoá công khai mở và cấu trúc lớn, các CA (đại diện cho các miền chứng thực khác nhau, chẳng hạn như các tổ chức thương mại) có thể phát hành chứng chỉ cho các CA khác, để việc phối hợp hoạt động trở nên thuận tiện. Ngay từ giai đoạn bắt đầu của quá trình phát triển cơ sở hạ tầng khoá công khai, chứng thực liên vùng đã được đưa ra. Các hoạt động kiểm toán, an toàn và gắn liền với trách nhiệm pháp lý của các CA thương mại cũng được đưa ra trong giai đoạn này. Hơn nữa, hoạt động chứng thực cũng cần chỉ rõ khi nào hỗ trợ chứng thực liên vùng và nếu có thì tiến hành hướng tiếp cận nào để xác định các chức năng, các mức đảm bảo và tin cậy có thể so sánh được.

Quyền điều tra tình trạng lộ

Quyền cho phép các CA điều tra tình trạng lộ (và tình trạng thiếu các hoạt động tin cậy một cách có chủ định) là không thể thiếu được. Do vậy, CPS nên chỉ rõ quyền và sự linh động của các CA khi điều tra.

Tin cậy và an toàn

CA phải là một thành viên thứ ba tin cậy, sử dụng công nghệ và thủ tục nhằm cung cấp một mức độ an toàn và tin cậy hợp lý. Để miêu tả các yêu cầu này, các hướng dẫn của ABA đưa ra khái niệm "Hệ thống tin cậy". Hệ thống này bao gồm các thủ tục, phần cứng và phần mềm máy tính sao cho:

- An toàn hợp lý, tránh được tình trạng xâm phạm và lạm dụng;
- Cung cấp một mức sẵn sàng, hoạt động chính xác và tin cậy hợp lý;
- Thích hợp cho việc thực hiện các chức năng dự định dành cho chúng;

- Tôn trọng các nguyên tắc an toàn đã được chấp thuận.

Các yêu cầu về an toàn thông tin, vật lý và cá nhân dành cho các CA là thiết yếu đối với một hệ thống tin cậy. CPS nên đưa ra các vấn đề này một cách trực tiếp hoặc tham chiếu tới chúng. Tuy nhiên, cần thận trọng khi công khai chi tiết về các biện pháp đối phó bên trong. Thông thường, các biện pháp đối phó này và các thủ tục liên quan tới chúng được lưu trong tài liệu riêng, việc truy nhập vào các tài liệu này bị giới hạn.

Tất cả các truyền thông, đặc biệt là các truyền thông có ảnh hưởng đến an toàn của cơ sở hạ tầng khoá công khai, phải được bảo vệ bằng cách sử dụng các cơ chế an toàn ứng với các rủi ro đi kèm. Các phương tiện cũng phải được bảo vệ vật lý. CA cũng phải trình bày rõ ràng, chính xác và tuân theo các hoạt động quản lý cá nhân.

Một điều vô cùng quan trọng là CA phải tạo ra và bảo vệ khoá riêng của mình một cách an toàn, bằng cách sử dụng một hệ thống tin cậy và phải tiến hành các biện pháp phòng ngừa cần thiết, nhằm ngăn chặn mất mát, khám phá, sửa đổi hoặc sử dụng trái phép.

Tuy nhiên ở mức cao, CPS nên đưa ra (hoặc tham chiếu thích hợp) chính sách an toàn cục bộ và chính sách an toàn kỹ thuật. Chính sách an toàn cục bộ bao gồm các chủ đề sau:

- Các kiểm soát vật lý (*Physical controls*): Các biện pháp được thực hiện nhằm đảm bảo an toàn phương tiện (nơi thiết lập hệ thống CA), bao gồm sử dụng người canh giữ, các thiết bị giám sát, khoá và các thiết bị kiểm soát truy nhập (chẳng hạn như khoá thẻ bài và các thiết bị sinh trắc học).

- Các kiểm soát thủ tục (*Procedural controls*): Các biện pháp bao gồm nhận biết các *role* (tập đặc quyền) kiểm soát thông qua các kỹ thuật mật mã, nó có thể ảnh hưởng trực tiếp đến việc phát hành, sử dụng, treo, hoặc huỷ bỏ các chứng chỉ, hoặc đặc quyền truy nhập vào kho lưu giữ. Việc bảo vệ khoá riêng hoặc các giá trị bí mật khác (mà từ đó có thể thu được khoá riêng) nên bao gồm kiến thức tách rời (*split knowledge*) hoặc chia sẻ bí mật (*secret sharing*), nhờ đó các chia sẻ bí mật được phân phối cho một số cá nhân độc lập. Các điều khoản chia sẻ bí mật cần giải quyết rất

nhiều các vấn đề, trong đó có bảo vệ phần cứng, các biểu diễn của CA, sự chấp nhận chia sẻ bí mật của những người nắm giữ, người phát hành và người nắm giữ lưu giữ các bản ghi, trách nhiệm pháp lý của người nắm giữ và sự đảm bảo của người phát hành chia sẻ bí mật.

- Các kiểm soát cá nhân (*Personnel controls*): Bao gồm các biện pháp như kiểm tra cơ sở, đào tạo và đào tạo lại, luân chuyển, kiểm soát hoạt động bất hợp pháp và tiến hành các kiểm soát đặc biệt đối với hợp đồng cá nhân (chẳng hạn giám sát, kiểm toán và các điều khoản hợp đồng đặc biệt). Nói riêng, CA có trách nhiệm trong điều tra, nghiên cứu và giám sát người phục vụ tại các vị trí tin cậy.

- Các chính sách an toàn kỹ thuật bao gồm các chủ đề sau:

- Các chức năng và sự đảm bảo an toàn máy tính (*Computer security functions and assurance*): Các biện pháp (chẳng hạn như sử dụng các sản phẩm an toàn được chính phủ thông qua) tương thích với các tiêu chuẩn đã được công nhận về chức năng và sự đảm bảo an toàn.

- Các kiểm soát và sự đảm bảo chu kỳ hoạt động của hệ thống (*System life cycle controls and assurance*): Các biện pháp đưa ra là an toàn môi trường và điều kiện phát triển, an toàn phát triển cá nhân, an toàn quản lý cấu hình trong quá trình bảo hành sản phẩm và các hoạt động thiết kế phần mềm.

- Các kiểm soát an toàn mạng (*Network security controls*): Các biện pháp liên quan tới việc bảo vệ mạng, chẳng hạn như sử dụng các bức tường lửa.

- Các đảm bảo và kiểm soát thiết kế môđun mật mã (*Cryptographic module engineering controls and assurance*): Các biện pháp liên quan đến đặc tính của các môđun phần cứng hoặc phần mềm mật mã.

Trách nhiệm tài chính

Các CA phải được giải quyết và có đủ nguồn tài chính để duy trì các hoạt động và thực hiện nghĩa vụ của mình, hay kinh phí được sử dụng trong các trường hợp khắc phục sai sót như thế nào, chẳng hạn như trong trường hợp lộ khoá riêng của CA. Họ cũng phải có trách nhiệm với các rủi ro của thuê bao, người sử dụng

chứng chỉ, những người tin cậy vào các chứng chỉ do họ phát hành, hoặc các dịch vụ khác mà họ cung cấp khi đóng vai trò là thành viên tin cậy.

Các bản ghi

Cung cấp tài liệu hoạt động là điều không thể thiếu được đối với một CA tin cậy. CA phải có khả năng chứng minh được các hoạt động của mình là đúng đắn, chẳng hạn như hỗ trợ chống chối bỏ cho các giao dịch có sử dụng chứng chỉ do CA phát hành.

Với mỗi chứng chỉ, các bản ghi thường liên quan đến các hoạt động tạo, phát hành, sử dụng, treo, huỷ bỏ, kết thúc thời hạn tồn tại, tạo mới và xin cấp lại chứng chỉ. Các bản ghi này nên lưu thông tin liên quan tới quyền sở hữu của CA đối với:

- Tên chủ thể chứng chỉ (ngoại trừ chứng chỉ dành cho một lớp, trong đó chủ thể hoàn toàn không được xác thực và tên chủ thể không nằm trong đó);
- Nhận dạng của người yêu cầu treo hoặc huỷ bỏ chứng chỉ (ngoại trừ các điều khoản đặc biệt có thể áp dụng cho các chứng chỉ của một lớp, trong đó chủ thể hoàn toàn không được xác thực);
- Thông tin khác được biểu diễn trong chứng chỉ;
- Các tem thời gian;
- Các thông tin dự tính trước liên quan đến việc phát hành các chứng chỉ.

Các bản ghi có thể được lưu giữ ở dạng thông báo trên máy tính hoặc tài liệu trên giấy, tem thời gian của chúng do một thành viên thứ ba tin cậy và độc lập gán cho, hoặc sử dụng một cơ chế gán tem tin cậy, điều này làm tăng tính toàn vẹn của cơ sở hạ tầng khoá công khai, góp phần chống chối bỏ các thông báo đã được ký số.

Việc duy trì các bản ghi hoạt động chứng thực trong một khoảng thời gian định trước là điều bắt buộc, vì nhiều lý do sau đây:

- ▢ Hỗ trợ chống chối bỏ các thông báo đã được ký số;
- ▢ Bằng chứng chứng tỏ CA đã thực hiện đúng đắn, bác bỏ các thông tin về sự lạm dụng;
- ▢ Thỏa mãn các yêu cầu của dự luật và luật có thể áp dụng.

Kiểm toán

Việc kiểm toán đối với các CA là thực sự cần thiết, không chỉ đáp ứng được các yêu cầu bên ngoài, mà còn chứng minh được tính tin cậy của một CA. CA nên duy trì một vết kiểm toán (cho tất cả các sự kiện cần thiết, chẳng hạn như sinh khoá, cấp, phê chuẩn, treo và huỷ bỏ chứng chỉ).

Các CA thương mại tiến hành kiểm toán bằng cách sử dụng các công cụ kiểm toán độc quyền và có các chuẩn chung. CPS nên đưa ra nghĩa vụ kiểm toán của từng CA và các thực thể liên quan khác, chẳng hạn như cơ quan đăng ký địa phương. Thông qua việc kiểm toán này, chúng ta cũng có thể đánh giá được mức độ tuân thủ CPS, cũng như các hướng dẫn, thủ tục, các chuẩn, các thoả thuận có thể áp dụng.

Khôi phục sau thảm hoạ và lên kế hoạch ứng biến

Việc khôi phục sau thảm hoạ và lên kế hoạch ứng biến đặc biệt quan trọng đối với một CA, bởi vì CA có nghĩa vụ phải bảo vệ các khoá riêng của mình, đảm bảo tính sẵn sàng của các thông tin liên quan đến tình trạng chứng chỉ. Vì vậy, CPS nên chỉ rõ những gì CA cần tuân theo khi thực hiện, cung cấp tài liệu, kiểm tra việc lập kế hoạch ứng biến và khôi phục sau thảm hoạ.

Ngoài ra, chúng ta cũng cần tính đến trường hợp khoá riêng gốc bị lộ. Nếu khoá gốc của một cơ sở hạ tầng bị lộ, việc khôi phục bao gồm huỷ bỏ các chứng chỉ, tất cả các thành viên liên quan, không riêng gì thuê bao, thành viên tin cậy cần được thông báo về tình trạng này, một cặp khoá mới phải được thiết lập và khoá công khai gốc phải có hiệu lực đối với người sử dụng.

Thông tin bí mật

Tuỳ thuộc vào các thuộc tính của một chứng chỉ, CA sẽ nhận được các dữ liệu cá nhân hoặc bí mật từ những người xin cấp chứng chỉ, từ đó có thể phê chuẩn đặc điểm nhận dạng, quyền, hoặc các thuộc tính khác của người xin cấp, điều này thực sự cần thiết khi phát hành chứng chỉ theo một mô hình tin cậy. Căn cứ vào mức độ nhạy cảm của thông tin, CPS nên xác định rõ làm thế nào để duy trì tính bí mật của các thông tin riêng tư.

Ví dụ, một CPS có thể chỉ rõ các thông tin (có kiểu sau đây) sẽ được nhận và tạo ra một cách bí mật, không được phép khám phá

chúng, trừ khi CPS, chủ thể của thông tin cho phép, hoặc luật pháp yêu cầu:

- Các bản ghi xin cấp chứng chỉ, không cần biết chúng có được phê chuẩn hay không;
- Các thoả thuận của thuê bao (trừ các thông tin có trong một chứng chỉ hoặc kho lưu giữ dành cho mỗi CPS);
- Các bản ghi giao dịch (tất cả các bản ghi và vết kiểm toán của giao dịch);
- Các bản ghi vết kiểm toán do CA tạo ra và duy trì;
- Các bản ghi kiểm toán do CA, kho lưu giữ của CA (để duy trì các bản ghi này), hoặc các kiểm toán viên (không cần biết thuộc nội bộ hay công khai) tạo ra;
- Các kế hoạch khôi phục sau thảm hoạ và kế hoạch ứng biến;
- Các biện pháp an toàn nhằm kiểm soát các hoạt động phần cứng và phần mềm của CA, quản lý các dịch vụ chứng chỉ và các dịch vụ đăng ký chứng chỉ.

Các yêu cầu của cơ quan đăng ký địa phương

Cơ quan đăng ký địa phương (LRA) là những người tin cậy, được CA chỉ định (bổ nhiệm) để trợ giúp các thuê bao trong việc xin cấp chứng chỉ, phê chuẩn các yêu cầu chứng chỉ, và/hoặc giúp đỡ CA trong việc huỷ bỏ (hoặc treo) các chứng chỉ. Thông thường, CPS đưa ra các yêu cầu tối thiểu đối với một LRA, tùy thuộc vào lớp ứng dụng chứng chỉ mà LRA được phép phê chuẩn. Do việc phê chuẩn thông tin của người xin cấp chứng chỉ là yếu tố thiết yếu để đảm bảo độ tin cậy của chứng chỉ được phát hành, LRA đóng vai trò không thể thiếu được trong việc đảm bảo độ tin cậy của cơ sở hạ tầng khoá công khai.

Kết thúc các hoạt động

Mỗi CA có thời gian hoạt động cụ thể. Do vậy, CPS nên xác định rõ CA sẽ kết thúc các hoạt động của mình như thế nào. Để giảm tác động việc kết thúc dịch vụ, CPS yêu cầu cung cấp thông báo đúng lúc, chuyển trách nhiệm pháp lý cho các thực thể kế tiếp, tiếp tục duy trì các bản ghi và bồi thường (có thể).

Ví dụ, trước khi ngừng hoạt động, CPS có thể yêu cầu một CA đã kết thúc hoạt động của mình như sau:

□ Thông báo cho các CA khác (trong cơ sở hạ tầng khoá công khai) khi CA có dự định ngừng vai trò của mình, ít nhất 90 ngày trước khi ngừng hoạt động.

□ Cung cấp cho thuê bao các chứng chỉ được CA phát hành nhưng đã hết hạn hoặc bị huỷ bỏ, khi CA có dự định ngừng vai trò của mình, ít nhất 90 ngày trước khi ngừng hoạt động.

□ Huỷ bỏ tất cả các chứng chỉ chưa bị thu hồi hoặc có thời hạn tồn tại chưa kết thúc trong khoảng thời gian 90 ngày nêu trên, không cần biết thuê bao có yêu cầu huỷ bỏ hay không.

□ Gửi thông báo huỷ bỏ cho các thuê bao liên quan.

□ Cố gắng hạn chế tối thiểu tình trạng phá vỡ do ngừng các dịch vụ chứng thực đối với thuê bao của CA và những người cần kiểm tra chữ ký số (bằng cách sử dụng khoá công khai có trong các chứng chỉ còn hạn sử dụng).

□ Đưa ra các chuẩn bị thích hợp cho việc duy trì các bản ghi.

□ Thanh toán bồi thường thích hợp cho các thuê bao khi CA huỷ bỏ các chứng chỉ của thuê bao trước thời hạn.

Hoạt động tội phạm

Một CPS có thể quy định các quyền và nghĩa vụ của từng thành viên trong vấn đề này, tùy thuộc vào luật tội phạm do chính phủ đưa ra. CPS cần đưa ra một cảnh báo rõ ràng đối với việc sử dụng hoặc lạm dụng bất hợp pháp các dịch vụ chứng thực mà CPS đã đề cập đến. CPS cũng có thể khuyến khích việc phát hiện và truy tố đối với các hành vi phạm tội làm ảnh hưởng trực tiếp tới các dịch vụ chứng thực. Do cơ sở hạ tầng khoá công khai thực sự phức tạp, nên nhu cầu chuyên môn hoá trong việc bảo vệ chống lại và truy tố tội phạm của cơ sở hạ tầng khoá công khai là vô cùng quan trọng. Nhiều cơ quan thi hành luật và các tổ chức cơ sở hạ tầng máy tính thành lập các đơn vị đặc biệt nhằm phát hiện, đối phó và truy tố việc lạm dụng máy tính. CA nên xử lý thông thạo các nguồn tài nguyên có sẵn nhằm chống lại tội phạm của cơ sở hạ tầng khoá công khai, cũng như khôi phục sau các tấn công của tội phạm.

6.4 CÁC THỦ TỤC XIN CẤP CHỨNG CHỈ

Các thủ tục xin cấp chứng chỉ thực sự thiết yếu đối với một dịch

vụ chứng thực tin cậy. Các thủ tục xin cấp chứng chỉ cần thu được những thông tin tin cậy từ người xin cấp chứng chỉ theo yêu cầu phát hành, CA phê chuẩn những thông tin này, thông báo cho người xin cấp chứng chỉ biết quyền và nghĩa vụ của họ.

Sinh khoá và bảo vệ khoá

Các thủ tục xin cấp chứng chỉ nên tập trung vào các thủ tục sinh cặp khoá. Trong trường hợp cặp khoá được sử dụng cho các mục đích chữ ký số, nếu thuê bao tự tạo ra các cặp khoá, cần giảm tối thiểu tình trạng lộ khoá, không được phép để lộ khoá riêng của mình cho bất kỳ ai, kể cả CA. Trong trường hợp cặp khoá được sử dụng cho các mục đích mã hoá, trong đó có thiết lập các cơ chế khôi phục hoặc uỷ nhiệm khoá, cặp. Cặp khoá có thể do một nhà cung cấp dịch vụ tạo ra, sau đó khoá riêng được chuyển đến cho thuê bao một cách an toàn; hoặc cặp khoá có thể do thuê bao tạo ra, sau đó khoá riêng được chuyển đến cho nhà cung cấp dịch vụ một cách an toàn, nhằm đáp ứng cho các mục đích khôi phục hoặc uỷ nhiệm khoá.

Các thuê bao phải thực sự quan tâm đến việc bảo vệ khoá riêng của mình. Điều này đặc biệt quan trọng khi việc tạo và lưu giữ khoá được thực hiện bằng phần mềm, bởi vì các rủi ro xảy ra thường lớn hơn so với các thẻ bài phần cứng. Cũng cần áp dụng nghĩa vụ này cho nhà cung cấp phần mềm an toàn, hoặc ứng dụng dành cho người dùng cuối, vì các sản phẩm của họ tạo ra và lưu giữ những khoá này.

CPS có thể yêu cầu người xin cấp chứng chỉ (và thuê bao) có trách nhiệm trong việc bảo vệ khoá riêng của mình, tránh bị lộ, mất mát, khám phá, sửa đổi hoặc sử dụng trái phép. Hơn nữa, nếu xảy ra trường hợp uỷ quyền sinh cặp khoá thì trách nhiệm pháp lý (trong việc sử dụng, lưu giữ và huỷ bỏ khoá riêng) của người được uỷ quyền không hề giảm. Tuy nhiên, CA và các nhà cung cấp phần mềm nên là những người đi tiên phong trong việc bảo vệ an toàn khoá riêng.

Phê chuẩn xin cấp chứng chỉ

CPS nên chỉ ra những thông tin mà CA yêu cầu trước khi phê chuẩn và chấp thuận một yêu cầu xin cấp chứng chỉ.

Việc tiến hành các thủ tục phê chuẩn thuộc trách nhiệm của

CA. Các thủ tục này có thể rất khác nhau, tùy thuộc vào mô hình tin cậy, các rủi ro dự tính và mô hình kinh doanh cho một chứng chỉ riêng. Ví dụ, một CA có nghĩa vụ trong việc phê chuẩn các yêu cầu xin cấp chứng chỉ, chứng thực rằng:

- Người xin cấp chứng chỉ là người có tên trong yêu cầu xin cấp;
- Người xin cấp chứng chỉ nắm giữ khoá riêng cùng cặp với khoá công khai được chứng thực;
- Thông tin có trong chứng chỉ hoàn toàn chính xác; và
- Đại lý (người xin cấp chứng chỉ cho một khoá công khai nào đó) là người có quyền chính đáng đưa ra yêu cầu này.

Trong mọi trường hợp, CPS nên xác định rõ các nghĩa vụ của CA. Một khi chứng chỉ được phát hành, CA sẽ không thường xuyên có trách nhiệm tiếp tục giám sát và điều tra về độ chính xác của thông tin có trong chứng chỉ, trừ khi có thông báo về tình trạng lộ. Thuê bao có nghĩa vụ thông báo cho CA biết về bất kỳ sự thay đổi nào xảy ra đối với thông tin có trong chứng chỉ.

Khi phê chuẩn một yêu cầu xin cấp chứng chỉ, đòi hỏi quan trọng nhất là tạo ra một ràng buộc thích hợp, hoặc một liên kết được xác thực, giữa người xin cấp (hoặc, tên, số tài khoản hoặc dữ liệu khác) với khoá công khai của họ. Quá trình này sẽ thay đổi tùy thuộc vào các yêu cầu của một chính sách chứng chỉ cụ thể, hoặc lớp các chứng chỉ. Quá trình có thể bao gồm một trong các quá trình sau, hoặc sự kết hợp các quá trình này, hoặc các quá trình khác:

- Hiện diện cá nhân (*personal presence*): Yêu cầu cá nhân xin cấp chứng chỉ trình diện trước một thực thể tin cậy (chẳng hạn như, công chứng viên hoặc cơ quan đăng ký địa phương), điều này làm cho việc xác nhận nhận dạng cá nhân trở nên thuận tiện hơn. Hiện diện cá nhân có nhiều yêu cầu khác nhau, tùy thuộc vào chính sách hoặc lớp chứng chỉ, chẳng hạn như kiểu của các tài liệu nhận dạng cần phải đưa ra khi trình diện.

- Xác nhận của thành viên thứ ba đối với dữ liệu cá nhân (*third-party confirmation of personal data*): Thành viên thứ ba xác nhận thông tin cá nhân do người xin cấp chứng chỉ cung cấp, bằng cách so sánh chúng với một cơ sở dữ liệu được thành viên thứ ba duy trì cho mục đích này. Ví dụ, việc điều tra trực tuyến có thể

cung cấp sự đảm bảo nào đó đối với nhận dạng, bằng cách so sánh các thông tin nhận dạng của người xin cấp với các cơ sở dữ liệu có tổ chức.

6.5 PHÁT HÀNH CHỨNG CHỈ

Sau khi phê chuẩn yêu cầu xin cấp chứng chỉ, CA tiến hành phát hành chứng chỉ, thông báo cho chủ thể của chứng chỉ các thông tin có trong chứng chỉ. CA đưa ra các biểu diễn khác nhau cho thuê bao và thành viên tin cậy.

Các biểu diễn dành cho thuê bao

Tuỳ thuộc vào việc phát hành chứng chỉ, CA đưa ra các biểu diễn nào đó cho một thuê bao. Ví dụ, CA có thể đảm bảo với thuê bao (có tên trong chứng chỉ) như sau:

- Không có các miêu tả sai thực tế trong chứng chỉ có nguồn gốc từ CA;
- Không có các lỗi sao chép khi chuyển dữ liệu từ người xin cấp tới CA;
- Chứng chỉ đáp ứng tất cả các yêu cầu quan trọng của CPS;
- Với thuê bao, CA cũng có thể đảm bảo rằng CA sẽ cố gắng:
- Huy bỏ hoặc treo chứng chỉ ngay lập tức (trong các trường hợp quy định), và
- Thông báo cho thuê bao tình trạng thực tế có thể ảnh hưởng trực tiếp đến việc phê chuẩn và độ tin cậy của chứng chỉ do CA phát hành cho thuê bao này.

Các biểu diễn dành cho thành viên tin cậy

Thông qua việc phát hành một chứng chỉ, CA có thể đảm bảo với người tin cậy chữ ký số (có thể kiểm tra bằng cách sử dụng khoá công khai có trong chứng chỉ) rằng:

- Mọi thông tin (trong chứng chỉ, hoặc thu được từ tham chiếu có trong chứng chỉ) là chính xác, và
- CA tuân theo các hoạt động (đã được công bố) khi phát hành chứng chỉ.

Mỗi chứng chỉ có thời gian hoạt động cụ thể, ví dụ chúng ta có thể biết được thông tin này, thông qua trường "khoảng thời gian hợp lệ" của chứng chỉ X.509 (*X.509 validity period field*). Khoảng

thời gian này có thể kéo dài từ 1 đến 3 năm. Khoảng thời gian hoạt động thực tế có thể ngắn hơn, vì lý do huỷ bỏ hoặc treo. "Chứng chỉ hợp lệ" (theo Các hướng dẫn của ABA) là một chứng chỉ do CA phát hành và được thuê bao (có tên trong chứng chỉ) chấp nhận.

6.6 CHẤP NHẬN CHỨNG CHỈ

Việc chấp nhận một chứng chỉ xác định khi nhiều nghĩa vụ thiết yếu của thuê bao (chẳng hạn như các biểu diễn được đưa ra dưới đây) có hiệu lực thi hành. Chấp nhận có nghĩa là chứng chỉ được người xin cấp thừa nhận khi biết hoặc có thông báo về các nội dung có trong chứng chỉ và phù hợp với CPS.

Làm thế nào để có được sự chấp nhận bằng hợp đồng trực tuyến và các nỗ lực pháp lý hiện có cũng được đưa ra để giải quyết vấn đề này. Một CA thận trọng sẽ giải quyết vấn đề này bằng cách yêu cầu thuê bao tiến hành các hoạt động xác nhận. Ví dụ, có thể yêu cầu thuê bao nhập vào một mã riêng (chẳng hạn như PIN) trong quá trình đăng ký trực tuyến, kèm theo các hoạt động khác.

Các biểu diễn của thuê bao

Thuê bao cần đưa ra các đảm bảo đối với CA, các thuê bao khác, hoặc thành viên tin cậy. Đây chính là các biểu diễn của thuê bao: nội dung thông tin có trong chứng chỉ là chính xác. CPS nên đưa ra các biểu diễn này một cách rõ ràng. Ví dụ, CPS có thể quy định rằng, thông qua việc chấp nhận một chứng chỉ, thuê bao chứng nhận và đồng ý với CA và tất cả những người tin cậy vào nội dung chứng chỉ (tại thời điểm chấp nhận và trong suốt khoảng thời gian hoạt động của chứng chỉ, cho đến khi thuê bao có thông báo khác) như sau:

- (Trong trường hợp chứng chỉ được sử dụng cho các mục đích chữ ký số) Mỗi chữ ký số được tạo ra (bằng cách sử dụng khoá riêng cùng cặp với khoá công khai có trong chứng chỉ) là chữ ký của thuê bao;

- Không ai được phép có khoá riêng của thuê bao;
- Tất cả các biểu diễn (do thuê bao đưa ra cho CA) về thông tin có trong chứng chỉ là đúng đắn.
- Tất cả thông tin có trong chứng chỉ là sự thực.

□ Chứng chỉ được sử dụng cho các mục đích hợp pháp và được phép, phù hợp với CPS; và

□ Nếu thuê bao là người sử dụng trực tiếp, không phải là một CA. Thuê bao sẽ không sử dụng khoá riêng (cùng cặp với khoá công khai có trong chứng chỉ) cho các mục đích ký chứng chỉ, hoặc danh sách các chứng chỉ bị thu hồi (CRL), trừ khi được thoả thuận bằng văn bản giữa thuê bao và CA;

□ Thông qua việc chấp nhận một chứng chỉ, CPS cũng có thể chỉ rõ rằng thuê bao:

□ Thừa nhận rằng thuê bao đồng ý với các thuật ngữ và điều kiện được trình bày trong CPS, và/hoặc đồng ý với các tài liệu có thể áp dụng khác (chẳng hạn trong thoả thuận của thuê bao), và/hoặc:

□ Chịu trách nhiệm bảo vệ khoá riêng của mình, tiến hành các biện pháp đối phó thích hợp nhằm ngăn chặn tình trạng mất mát, lộ, sửa đổi hoặc sử dụng trái phép khóa riêng này.

Bồi thường theo thoả thuận của thuê bao

Việc bồi thường (theo thoả thuận của thuê bao nhưng có sự chấp thuận của CA) có thể được trình bày trong CPS, nhằm làm rõ thuê bao có trách nhiệm trong việc đảm bảo an toàn đối với khoá riêng của mình, đảm bảo độ chính xác của thông tin (đã cung cấp cho CA và được sử dụng khi phát hành chứng chỉ).

Công bố

CA có nghĩa vụ công bố các chứng chỉ được thuê bao chấp nhận và việc công bố một chứng chỉ trong kho lưu giữ của CA xác nhận rằng thuê bao đã chấp nhận nó.

6.7 SỬ DỤNG CHỨNG CHỈ ĐỂ KIỂM TRA CHỮ KÝ SỐ

Chúng ta có thể đưa ra một số quy định nào đó nhằm hỗ trợ việc sử dụng chứng chỉ để kiểm tra các thông báo được ký số. Một số điều khoản liên quan trong CPS có thể xác định rõ ràng nghĩa vụ của các thành viên trong việc kiểm tra chữ ký số khi thành viên này nhận được chữ ký nhưng chưa hoàn toàn tin tưởng vào nó. Những điều khoản này cũng có thể giải quyết được các vấn đề về phê chuẩn và hiệu lực của thương mại điện tử.

Quá trình kiểm tra chữ ký số

Khi nhận được một thông báo ký số, người nhận kiểm tra chữ ký số để biết chữ ký số có được tạo ra từ khoá riêng cùng cặp với khoá công khai có trong chứng chỉ của người ký hay không, đồng thời kiểm tra xem thông báo có bị sửa đổi sau khi ký hay không. Đây là điều không thể thiếu được khi tiến hành thương mại điện tử an toàn.

CPS có thể miêu tả chi tiết quá trình kiểm tra chữ ký số, chẳng hạn như, quá trình kiểm tra chữ ký số yêu cầu phê chuẩn một đường dẫn chứng thực đầy đủ từ chứng chỉ của người ký đến khoá công khai gốc, khoá này phải được phân phối thông qua các phương tiện độc lập và an toàn. CPS cũng có thể giải thích (chi tiết hơn hoặc ít chi tiết hơn) quá trình phê chuẩn một đường dẫn chứng thực theo các bước.

Nói chung, tùy thuộc vào quá trình kiểm tra trên, chữ ký số được tạo ra trong khoảng thời gian hoạt động của một chứng chỉ được xem là mối liên hệ giữa thành viên tin cậy và thuê bao (chủ thể của chứng chỉ) trừ khi:

- Thuê bao (chủ thể của chứng chỉ) có thể chứng minh rằng thông tin nhận dạng trong chứng chỉ là không đúng; hoặc
- Thuê bao có thể chứng minh rằng thuê bao đã kiểm soát khoá riêng, khoá bị mất nhưng không phải do thuê bao vi phạm trách nhiệm bảo vệ khoá riêng của mình;
- Điều này cũng giả định rằng:
- Thành viên tin cậy không có thông tin hoặc thông báo về việc vi phạm các yêu cầu của CPS, và
- Thành viên tin cậy tuân theo tất cả các yêu cầu của CPS và thành viên tin cậy đặt sự tin cậy hợp lý vào chứng chỉ (và các chữ ký số có thể kiểm tra được) trong một số trường hợp.

Các chữ ký và văn bản

Hiệu lực của các chữ ký và văn bản điện tử vẫn chưa được giải quyết hoàn toàn. CPS có thể bao gồm các điều khoản nhằm làm tăng hiệu lực pháp lý của thương mại điện tử, có vai trò như là các điều khoản ngầm định; ví dụ:

- Văn bản điện tử: là một thông báo được gắn chữ ký số, có

thể kiểm tra chữ ký số này bằng cách sử dụng khoá công khai có trong một chứng chỉ hợp lệ. Văn bản này có hiệu lực như một thông báo được viết và ký trên giấy.

□ Các chữ ký: Khi một điều luật hoặc nhu cầu thực tiễn đòi hỏi một chữ ký số hoặc đưa ra hậu quả nào đó của việc thiếu chữ ký, cần kiểm tra chữ ký số của người ký có trên một thông báo bằng cách sử dụng khoá công khai có trong một chứng chỉ hợp lệ.

6.8 VIỆC TREO VÀ HUỖ BỎ CHỨNG CHỈ

Sau đây là các trường hợp dẫn đến việc thu hồi (treo) hoặc huỷ bỏ chứng chỉ:

□ Đánh mất, bị lấy cắp, sửa đổi, khám phá trái phép, hoặc làm lộ khoá riêng (của chủ thể chứng chỉ);

□ CA xác định chứng chỉ được phát hành nhưng không tuân theo các thủ tục mà CPS đặt ra;

□ Thuê bao yêu cầu thu hồi (và CA xác nhận rằng người yêu cầu thu hồi đúng là thuê bao);

□ Chủ thể của chứng chỉ (có thể là một CA hoặc thuê bao) đã vi phạm nghĩa vụ cần thiết của CPS; hoặc

□ Việc thực thi nghĩa vụ (tuân theo CPS) của một người bị trì hoãn hoặc ngăn chặn do thảm họa tự nhiên, lỗi máy tính hoặc lỗi truyền thông, hoặc những nguyên nhân khác vượt quá khả năng kiểm soát của con người, hoặc do thông tin của người khác có nguy cơ bị lộ hoặc lộ.

Việc xác nhận tính hợp lệ đối với yêu cầu thu hồi chứng chỉ của một thuê bao đặc biệt quan trọng. Bằng chứng về tính xác thực của một yêu cầu thu hồi chứng chỉ thực sự cần thiết, nhằm chống lại tấn công từ chối dịch vụ; tuy nhiên, việc yêu cầu nhiều bằng chứng có thể gây ra các thiệt hại không cần thiết, do làm chậm trễ việc huỷ bỏ các chứng chỉ bị lộ khoá. Do đó, cần phải có các xử lý thích hợp. Ví dụ, CPS có thể quy định các yêu cầu huỷ bỏ của thuê bao phải có dạng bản ghi trên giấy, hoặc bản ghi số được xác thực thích hợp, hoặc thông báo dưới dạng tiếng nói từ thuê bao hoặc đại diện của thuê bao.

Khi treo hoặc huỷ bỏ một chứng chỉ, CA phải thông báo cho cộng đồng người dùng của mình. Ví dụ, các dịch vụ thông báo như:

công bố công khai danh sách các chứng chỉ bị thu hồi (CRL) hoặc kiểm tra tình trạng thu hồi trong thời gian thực. Với giải pháp "đẩy" (*push*), ví dụ danh sách thu hồi quảng bá, CA phải công bố các thông tin thu hồi. Với giải pháp "kéo" (*pull*), ví dụ kiểm tra tình trạng thu hồi trong thời gian thực, người dùng hoặc thành viên tin cậy phải lấy thông tin thu hồi từ CA. Nhu cầu và các kiểu dịch vụ thông báo sẽ thay đổi cùng với sự phát triển của các mô hình cơ sở hạ tầng khoá công khai và kiểu rủi ro.

Trách nhiệm của người nắm giữ khoá là bảo vệ khoá riêng của mình, trong khoảng thời gian hoạt động của chứng chỉ hoặc có thể mở rộng ra ngoài khoảng thời gian đó, bao gồm cả khoảng thời gian huỷ bỏ hoặc treo. Lý do mở rộng là làm giảm bớt các thiệt hại hoặc tình trạng lạm dụng khoá bị lộ.

6.9 SỰ ĐẢM BẢO VÀ GIỚI HẠN TRÁCH NHIỆM PHÁP LÝ

Các CA có thể đảm bảo các dịch vụ nào và việc chia nhỏ trách nhiệm pháp lý của chúng có ảnh hưởng đến độ tin cậy của cộng đồng người dùng đối với CA hay không. Phạm vi trách nhiệm pháp lý của CA sẽ phụ thuộc vào một hoặc nhiều yếu tố sau đây:

- Lệ phí phải trả cho chứng chỉ;
- Sự hiểu biết về các rủi ro trong cơ sở hạ tầng khoá công khai;
- Tính sẵn sàng và khả năng áp dụng của các công cụ (đã được chứng minh) nhằm làm giảm tình trạng lộ và gian lận;
- Việc ban hành luật có thể cung cấp (hoặc cung cấp chưa đầy đủ) phạm vi an toàn dành cho các hoạt động chứng thực;
- Tính sẵn sàng của các phương tiện đảm bảo tin cậy và kinh tế;
- Thỏa thuận giữa cộng đồng người dùng và CA;
- Khả năng cạnh tranh.

Nói chung, trách nhiệm pháp lý của các CA thương mại phù hợp với trách nhiệm pháp lý của hầu hết các ISP (nhà cung cấp dịch vụ Internet), các nhà cung cấp phần cứng và phần mềm, các nhà cung cấp dịch vụ truyền thông và VAN (mạng giá trị gia tăng), thông thường họ giới hạn trách nhiệm pháp lý của mình vào các thiệt hại trực tiếp.

Các đảm bảo

Như đã trình bày ở trên, trách nhiệm pháp lý của hầu hết các CA thương mại bao gồm toàn bộ hoặc một phần nguyên tắc phạm vi an toàn được đưa ra trong *Hướng dẫn của ABA*, quy định rằng:

Một CA tuân theo hướng dẫn này và bất kỳ luật, hoặc hợp đồng có thể được áp dụng, không phải chịu trách nhiệm pháp lý đối với bất kỳ rủi ro nào:

1) thuộc trách nhiệm của thuê bao (có chứng chỉ được CA, hoặc người khác phát hành), hoặc

2) do tin cậy vào chứng chỉ do CA phát hành, tin cậy vào chữ ký số có thể kiểm tra được bằng cách sử dụng khoá công khai có trong một chứng chỉ, hoặc tin cậy vào thông tin được biểu diễn trong chứng chỉ này hoặc kho lưu giữ.

Theo nguyên tắc này, một CA có thể tìm hiểu và biết được nghĩa vụ thực thi của mình, hoàn thành chúng và từ đó giới hạn trách nhiệm pháp lý của mình vào các nghĩa vụ đã được xác định này. Ví dụ, trong phiên bản CPS 1.1 của VeriSign, chỉ rõ rằng các CA cần đảm bảo:

- Cung cấp cơ sở hạ tầng và các dịch vụ chứng thực, bao gồm việc thiết lập và duy trì các kho lưu giữ như đã được chỉ ra trong CPS;

- Cung cấp các kiểm soát và hỗ trợ cần thiết cho các cơ sở hạ tầng khoá công khai của CA, bao gồm sinh khoá cho CA, bảo vệ khoá và các thủ tục chia sẻ bí mật đã được đưa ra trong CPS;

- Tiến hành các thủ tục phê chuẩn xin cấp cho lớp chứng chỉ xác định trong CPS;

- Phát hành các chứng chỉ theo đúng CPS, tôn trọng các biểu diễn khác nhau (dành cho các thuê bao và thành viên tin cậy) đã được đưa ra trong CPS;

- Công bố các chứng chỉ được chấp nhận theo đúng CPS;

- Thực hiện nghĩa vụ của một CA, hỗ trợ quyền cho các thuê bao và thành viên tin cậy (là các đối tượng sử dụng chứng chỉ) tuân theo CPS;

- Treo và huỷ bỏ các chứng chỉ theo các yêu cầu đã được đưa ra trong CPS;

□ Đảm bảo các quá trình kết thúc, tái xin cấp và phục hồi các chứng chỉ theo đúng CPS; và

□ Tuân theo các điều khoản linh tinh có trong CPS.

Thêm vào đó, các CA có thể đảm bảo rằng khoá riêng của họ không bị lộ, nếu xảy ra tình trạng này cần thông báo qua kho lưu giữ.

Các từ chối và giới hạn trong nghĩa vụ

Người sử dụng chứng chỉ cần biết các giới hạn trong việc sử dụng chứng chỉ, CA cần biết nghĩa vụ của mình trong việc cung cấp các dịch vụ chứng thực. Vì vậy, cũng cần có một hướng tiếp cận từ chối các đảm bảo nào đó, chẳng hạn như đảm bảo bán được hàng, đảm bảo phù hợp cho một mục đích riêng và hạn chế trách nhiệm pháp lý của CA tuân theo CPS.

Các giới hạn về thiệt hại và mất mát

CPS có thể xác định phạm vi giới hạn trách nhiệm pháp lý, bằng cách cung cấp các *cap*. *Cap* là một hợp đồng hoặc luật về các thiệt hại mà một thành viên phải chịu trách nhiệm (và *cap* mang tính bắt buộc). Nếu các thiệt hại vượt quá khuôn khổ của *cap*, các thành viên khác phải chịu thiệt hại này. Một *cap* có thể gắn liền với một lớp chứng chỉ riêng (gắn liền với một tập hợp các đảm bảo riêng và chi phí tương ứng).

Không quan hệ uỷ thác

CA không phục vụ như là người đại diện, hoặc đóng vai trò là người được uỷ thác đối với các thuê bao (trừ khi có sự yêu cầu của luật pháp hoặc hợp đồng). Điều này đặc biệt đúng khi CA bị tách khỏi các giao dịch được ký số nhưng lại do các thuê bao ký, có nghĩa là CA không phải là thành viên của các giao dịch này và không tham gia vào các quá trình ký, gán tem thời gian, hoặc truyền đi các thông báo. Trong những trường hợp này, CPS có thể quy định rằng không có quan hệ uỷ thác nào được thiết lập giữa CA và thuê bao.

6.10 CÁC ĐIỀU KHOẢN LINH TINH

Sự mâu thuẫn giữa các điều khoản

CPS có thể chỉ rõ vai trò quan trọng hàng đầu của mình, nó sẽ thay thế các tài liệu khác, cần nhận thức rõ ràng CPS là tài liệu

trung tâm trong cơ sở hạ tầng khoá công khai.

Luật quản lý

CPS nên chọn lựa luật quản lý, thực tế là thông tin được truyền đi trên các mạng truyền thông mở (chẳng hạn như Internet) vượt quá một số quyền hạn pháp lý nào đó.

Các thành viên trong cơ sở hạ tầng khoá công khai cần tin cậy vào các nguyên tắc truyền thống và nguyên tắc phát triển để có được sự lựa chọn đúng đắn và tin cậy vào sự chọn lựa đó.

Giải quyết tranh chấp

Các tranh chấp có thể được giải quyết bằng khiếu kiện hoặc thông qua các cơ chế chọn lựa, chẳng hạn như trọng tài phân xử. Một CPS nên xác định rõ các tranh chấp được giải quyết như thế nào. Với tính phức tạp của cơ sở hạ tầng khoá công khai và sự thiếu hiểu biết về nó còn nhiều, sự thích hợp cũng như lợi ích của điều khoản về kiểu "Cơ chế dàn xếp không chính thức ban đầu" trợ giúp cho các thành viên trong việc giải quyết các vấn đề, trợ giúp thông tin và công nghệ nào đó.

Thay đổi các thủ tục

Cơ sở hạ tầng khoá công khai ngày càng phát triển nhanh chóng. Ngoài luật không theo kịp với kỹ thuật, công nghệ đang trải qua nhiều biến đổi sâu sắc, vậy điều gì sẽ xảy ra đối với CPS đáp ứng và hỗ trợ trong những khoảng thời gian dài. Chính vì vậy, CPS phải có lợi từ quá trình thay đổi động.

Quá trình thay đổi mang lại cho CA khả năng bổ sung và sửa đổi CPS, tùy thuộc vào việc cung cấp cho người sử dụng (bao gồm cả thuê bao và thành viên tin cậy) thông báo đề xuất thích hợp về những thay đổi này.

6.11 SỰ TIẾN TRIỂN KHÔNG NGỪNG

Tính hoà hợp

Trong thời gian gần đây, cùng với những thành công quan trọng trong việc hoà hợp phát triển (cả về mặt pháp lý và kỹ thuật), với trao đổi dữ liệu điện tử, gửi tin điện tử và Web, các yêu cầu của cơ sở hạ tầng khoá công khai ngày càng tăng. Các hoạt động hoà hợp cơ sở hạ tầng khoá công khai được chứng tỏ trong các phạm vi

hoạt động khác nhau:

- Cộng đồng kỹ thuật (*technical community*): Với các chuẩn kỹ thuật, như X.509, đang phát triển ở mức cao và được chấp nhận rộng rãi, nhiều chuyên gia kỹ thuật có khuynh hướng tập trung vào các vấn đề chính sách và hoạt động thực tế cần giải quyết, tác động đến khả năng chứng thực chéo và liên vận hành giữa các cơ sở hạ tầng khoá công khai; Các hướng tiếp cận phổ biến trong việc quản lý trao quyền cũng đang được khai thác;

- Cộng đồng pháp lý (*legal community*): Các nỗ lực chủ yếu được tiếp tục trong các nhóm khác nhau, trong phát triển nguyên tắc của ABA và đặc biệt là các khởi xướng pháp lý khác nhau;

- Cộng đồng kinh doanh (*business community*): Cộng đồng kinh doanh, chẳng hạn như CommerceNet và phòng Thương mại Quốc tế (International Chamber of Commerce) lên chương trình làm việc trên các hướng tiếp cận chung, nhằm xây dựng và sử dụng các cơ sở hạ tầng khoá công khai, bao gồm cả các vấn đề liên quan đến tính riêng tư; và

- Các cơ quan chứng thực (*certification authorities*): Hiện nay, các cơ quan chứng thực đang đề xuất các quy định hoạt động chứng thực theo cùng quan điểm nhằm tạo ra một môi trường liên hoạt động và có khuôn phép.

Tự động hoá

Các hướng tiếp cận trước đây về CPS thường mang tính cá nhân và thủ công, quan tâm đến việc chấp nhận các thuật ngữ và điều kiện có trong CPS của thành viên khác trên cơ sở từng trường hợp, được phát triển dần từng bước, hình thành các giải pháp hiệu quả hơn, tận dụng được tính tự động trong các dạng khác nhau. Một số cách trong đó tự động hoá làm tăng ảnh hưởng của các CPS, bao gồm:

- Các công cụ phát triển CPS (*CPS development tools*): Các mẫu CPS có chứa các điều khoản và các tham chiếu chính sách chứng chỉ được mô đun hoá, có sẵn trên CD-ROM và các phương tiện khác, sẽ đơn giản hoá việc phát triển và triển khai các CPS phù hợp hơn. Ngoài ra, các công cụ mang tính địa phương hoá, quốc tế hoá sẽ góp phần phát triển CPS. Tính sẵn sàng của các tài nguyên này sẽ do các CA, cộng đồng kinh doanh đưa ra.

□ Tham chiếu và dàn xếp chính sách chứng chỉ (*certificate policy negotiation and mapping*): Các đặc tính của chứng chỉ X.509 phiên bản 3 hướng phục vụ cho việc tự động hoá truyền thông và khả năng áp dụng các chính sách chứng chỉ và hoạt động giữa các CA, thuê bao và thành viên tin cậy. Nếu có một tập hợp đủ nhỏ các chính sách chứng chỉ được chấp nhận rộng rãi, điều này sẽ làm tăng việc sử dụng các đặc tính của chứng chỉ X.509 và giảm nhu cầu can thiệp của con người khi quyết định, trên cơ sở từng cuộc giao dịch, nếu chứng chỉ được đưa ra phù hợp với một mục đích cho trước.

□ Dàn xếp hoạt động và chính sách một cách trực tuyến (*online policy and practice negotiation*): Có thể thực hiện được việc xây dựng động và chấp nhận dựa trên các thuật ngữ và điều kiện có trong CPS mà thoả mãn yêu cầu của các thành viên liên quan, trên cơ sở từng cuộc giao dịch. Điều này cần các mô đun CPS chuẩn hoá, các giao thức và công cụ dàn xếp chuyên dụng và một khung pháp lý thích hợp.

Các hướng thương mại và luật/dự luật

Việc phát triển các sử dụng thương mại được công nhận trong cơ sở hạ tầng khoá công khai nhận được đề cập nhiều trong các nguyên tắc của ABA. Việc phát triển chính sách quản lý và kỹ thuật sẽ chi phối các sử dụng thương mại. Ví dụ, nếu các cơ chế khôi phục khoá bắt buộc trở thành luật, chắc chắn các hoạt động thương mại sẽ phát triển gắn liền với các yêu cầu này. Chúng ta cũng mong đợi các sử dụng thương mại làm cho việc phát triển luật và dự luật trong cơ sở hạ tầng khoá công khai tăng nhanh.

Trước đây, các khởi xướng luật và dự luật chữ ký số chịu sự chi phối của các thành viên thuộc của chính phủ, chẳng hạn như toà án và các Bộ trưởng. Các nỗ lực pháp lý hiện nay còn có sự tham gia của các cá nhân. Sự thay đổi này sẽ mang lại các hướng tiếp cận mới nhạy cảm với các yêu cầu thương mại.

6.12 TÓM TẮT

Vai trò của *cơ quan chứng thực* thực sự quan trọng để đảm bảo an toàn thương mại điện tử. Tuy nhiên, hiệu lực của một thành viên thứ ba phụ thuộc vào các dịch vụ được công nhận của nó. Sự

công nhận này phụ thuộc vào các hoạt động của CA được quy định trong CPS.

Khái niệm CPS xuất phát từ khái niệm *cơ quan chứng thực chính sách* (PCA) và *các quy định chính sách* trong thiết kế Internet PEM. Những khái niệm này được thay thế bằng khái niệm *chính sách chứng chỉ* được giới thiệu với chứng chỉ X.509 phiên bản 3.

Các điều khoản trong một CPS phụ thuộc vào cộng đồng sử dụng nó. Nói riêng, CPS dành cho một cộng đồng khép kín (chẳng hạn một hãng, hoặc một chính phủ nào đó) có thể tập trung vào nhiều mối quan tâm khác nhau, không chỉ đơn thuần là một CPS dành cho một cơ quan chứng thực thương mại. Ở đây không có khuôn dạng chuẩn, hay danh sách các chủ đề chuẩn, hoặc tổ chức chuẩn cho một CPS, mặc dù nhiều đề xuất đã được đưa ra nhằm phát triển 1 *khung* hoặc *mẫu* CPS chuẩn; điều này làm cho việc viết và tìm hiểu các CPS thuận tiện hơn.

Trước khi một cơ quan chứng thực thương mại có thể cung cấp các dịch vụ, nó cần thiết lập các hoạt động pháp lý và kinh doanh của mình, đồng thời mô tả các kiểm soát mà nó sẽ sử dụng để đảm bảo các hoạt động tin cậy. Thông thường, một CPS nhận diện các mức dịch vụ có hiệu lực, phạm vi của các lớp chứng chỉ, các chính sách chứng chỉ, hoặc các khái niệm tương tự. Có thể miêu tả các khuôn dạng chứng chỉ, tương thích với một chuẩn được công nhận, chẳng hạn như X.509. Cấu trúc áp dụng cho mối quan hệ giữa các CA, chẳng hạn như cấu trúc phân cấp, có thể được nhận diện. Nếu CA cung cấp một dịch vụ đăng ký tên, CPS có thể miêu tả các chính sách liên quan tới dịch vụ này, bao gồm các chính sách về giải quyết tranh chấp dựa vào quyền sở hữu tên riêng. Một CPS có thể xác định rõ: có nên hỗ trợ chứng thực liên vùng hay không và nếu có thì hướng tiếp cận được thực hiện để xác định các chức năng và mức đảm bảo, hoặc sự tin cậy có thể so sánh được như thế nào.

Các cơ quan chứng thực phải sử dụng công nghệ và các thủ tục nhằm cung cấp một mức an toàn và tin cậy hợp lý. CPS, hoặc tài liệu khác mà CPS tham chiếu tới, miêu tả các biện pháp an toàn thông tin, cá nhân và vật lý được thực hiện. Các cơ quan chứng

thực cũng phải có đủ nguồn tài chính để duy trì các hoạt động và thực hiện nhiệm vụ của mình. Các cơ quan chứng thực nên lưu giữ đầy đủ các bản ghi và đáp ứng các yêu cầu được phép đối với các bản ghi này. Các cơ quan chứng thực nên tạo và lưu giữ đầy đủ các vết kiểm toán, tiến hành các hoạt động kiểm toán định kỳ dựa vào các chuẩn kiểm toán được công nhận cho hệ thống thông tin. Các điều khoản khác cũng được đưa ra như lên kế hoạch ứng biến và khôi phục sau thảm họa, bảo vệ thông tin bí mật, các yêu cầu đối với các cơ quan đăng ký địa phương (LRA) và việc kết thúc hoạt động của một cơ quan chứng thực.

Các thủ tục xin cấp chứng chỉ không những phải thu được các thông tin tin cậy từ phía người xin cấp chứng chỉ, mà còn phải khuyến và cảnh báo người xin cấp chứng chỉ về quyền và nghĩa vụ của họ. Người xin cấp chứng chỉ phải bảo vệ khoá riêng của mình, tránh để lộ, mất, khám phá, sửa đổi hoặc sử dụng trái phép đối với khoá riêng này. Cơ quan chứng thực sẽ phê chuẩn yêu cầu xin cấp chứng chỉ.

Phát hành chứng chỉ nói đến các hoạt động mà cơ quan chứng thực thực hiện khi tạo ra một chứng chỉ và thông báo cho chủ thể chứng chỉ về các nội dung có trong chứng chỉ. Tùy thuộc vào việc phê chuẩn thành công và sự chấp thuận của người xin cấp chứng chỉ, cơ quan chứng thực phát hành một chứng chỉ. Cơ quan chứng thực tạo ra các biểu diễn khác nhau cho thuê bao và thành viên tin cậy. Thuê bao có thể tiến hành một hoặc nhiều hoạt động xác nhận. Thông qua việc chấp nhận một chứng chỉ, thuê bao thừa nhận các nghĩa vụ của mình.

Trong CPS, các điều khoản khác có thể xác định nghĩa vụ của các thành viên cần kiểm tra chữ ký số trước khi tin cậy vào nó. Các điều khoản này cũng có thể giải quyết nhiều vấn đề về hiệu lực và tính bắt buộc của thương mại điện tử, chẳng hạn như đáp ứng các yêu cầu chữ ký và văn bản hình thức. CPS có thể mô tả các thủ tục treo, huỷ bỏ và kết thúc thời hạn hoạt động của chứng chỉ.

CPS mô tả cách thức trong đó các cơ quan chứng thực đảm bảo các dịch vụ và chia nhỏ trách nhiệm pháp lý của mình. Trong đó có thể bao gồm các đảm bảo chung, các từ chối đảm bảo và các giới

hạn của trách nhiệm pháp lý. Các điều khoản linh tinh có trong CPS có thể đưa ra các vấn đề, chẳng hạn như tính mẫu thuẫn của các điều khoản, luật quản lý, giải quyết tranh chấp và các thủ tục thay đổi.

Cùng với sự phát triển của các sử dụng thương mại, các luật và dự luật, các cơ sở hạ tầng khoá công khai, thương mại điện tử an toàn sẽ nhanh chóng bước sang một thời kỳ mới.

CHƯƠNG VII

LUẬT CHỮ KÝ ĐIỆN TỬ

Chương này giới thiệu luật mẫu về chữ ký điện tử của *Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc tế* (United Nations Commission on International Trade Law, viết tắt là UNCITRAL). Luật mẫu này được đưa ra vào năm 2001 và đi kèm với nó là bản hướng dẫn ban hành luật, tuy nhiên trong khuôn khổ của cuốn sách này, chúng tôi chỉ giới thiệu luật mẫu về chữ ký điện tử của UNCITRAL, được trình bày trong mục 7.1, tiếp theo là một số mục trong bản hướng dẫn ban hành luật mẫu có liên quan đến chữ ký số, được trình bày trong mục 7.2.

7.1 LUẬT MẪU VỀ CHỮ KÝ 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.

* Ủy 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 sau đây [...]."

** 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: bất kỳ giao dịch kinh doanh nào 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: Một số định nghĩa cơ bản

Phù hợp với 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 sinh 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: 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 tước đoạt 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 chỉ phôi (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 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 đáp ứng nhờ vào quan hệ với một thông báo dữ liệu nếu một chữ ký điện tử được sử dụng tin cậy, phù hợp với mục đích trong đó thông báo dữ liệu được tạo ra và truyền đi, cụ thể với tất cả các trường hợp, bao gồm mọi thoả thuận liên quan.

(2) Đoạn (1) áp dụng khi yêu cầu nằm trong quy 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) Có thể phát hiện được mọi sửa đổi đối với thông tin liên quan đến chữ ký 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 ban hành luật] có thể quyết định những chữ ký điện tử nào thoả mãn các điều khoản trong mục 6.

(2) Mọi quyết định được đưa ra trong đoạn (1) cần 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 luật quốc tế về tính riêng tư.

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 có 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 của 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 của đoạn (1).

Mục 10: 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) Việc 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 điều 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 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, thành viên tin cậy đã không tiến hành các bước hợp lý để:

(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 đối với 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.

7.2 CHỮ KÝ SỐ

Chữ ký trên tài liệu là chứng cứ, dấu hiệu để nhận dạng người đã ký lên tài liệu đó. Chữ ký số là dữ liệu được lưu giữ ở dạng điện tử. Về bản chất, chữ ký số phải đạt được độ thừa nhận như chữ ký viết tay nhưng trong thực tế chúng có nhiều điểm khác nhau.

Chữ ký viết tay là một phần vật lý của tài liệu được ký. Chữ ký số không được gắn theo kiểu vật lý như vậy trên tài liệu được ký. Chữ ký viết tay thường được kiểm tra bằng trực giác, được so sánh với chữ ký mẫu. Trong khi đó, muốn kiểm tra chữ ký số không thể tiến hành như vậy. Bản sao tài liệu có chữ ký số hoàn toàn đồng nhất với bản gốc, nhưng bản sao tài liệu với chữ ký viết tay lại không thể đồng nhất hoàn toàn với bản gốc (các thông tin và dữ liệu thể hiện trên giấy rất khó bị sửa đổi vì nó để lại dấu vết vật lý, trong khi đó, dữ liệu trong các hệ thống điện tử rất dễ dàng bị thay đổi mà người nhận tin không thể phát hiện được). Điều này cảnh báo rằng cần phải có các biện pháp hữu hiệu để ngăn chặn việc sử dụng hoặc sao chép trái phép tài liệu có chữ ký số. Trong phần này, chúng tôi giới thiệu một số mục trong bảng hướng dẫn ban hành luật chữ ký điện tử của UNCITRAL có liên quan tới chữ ký số. Đây là bản hướng dẫn ban hành luật đi kèm với luật mẫu về chữ ký số điện tử được giới thiệu trong mục 7.1. Đồng thời, qua đó chúng ta biết được vai trò của mã hoá khoá công khai, cơ sở hạ tầng khoá công khai, nhà cung cấp dịch vụ chứng thực, cơ quan chứng thực trong việc tạo và kiểm tra chữ ký số.

• Các chữ ký số dựa vào mã hoá khoá công khai

Các chữ ký số được tạo ra và kiểm tra bằng mật mã, đúng hơn là sử dụng mã hoá khoá công khai. Một cặp khoá được sinh ra, một trong hai khoá được sử dụng để tạo ra chữ ký số, được gọi là khoá riêng. Khoá còn lại được sử dụng để kiểm tra chữ ký số, được gọi là khoá công khai.

Khoá riêng và khoá công khai

Khoá riêng phải được giữ bí mật. Các khoá trong cặp khoá có

liên quan toán học với nhau, nếu một hệ mật khoá công khai được tạo ra và thiết lập an toàn, khó có thể biết được khoá riêng từ những thông tin về khoá công khai. Hầu hết các thuật toán mã sử dụng khoá công khai và khoá riêng đều dựa trên 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 được khoá công khai nhưng không thể làm giả chữ ký số bởi vì họ không biết được khoá riêng cùng cặp, họ chỉ có thể kiểm tra chữ ký số.

Nếu nhiều người muốn kiểm tra chữ ký số thì khoá công khai phải có hiệu lực hoặc được phân phối cho tất cả những người này. Bởi vì người kiểm tra chỉ có thể kiểm tra được chữ ký số khi họ có được khoá công khai của người ký và đảm bảo rằng khoá công khai này cùng cặp với khoá riêng đã được sử dụng khi tạo chữ ký số.

Hàm băm

Ngoài việc sinh ra các cặp khoá, trong quá trình tạo, kiểm tra chữ ký số và kiểm tra tính toàn vẹn của thông báo cần sử dụng hàm băm. Hàm băm dựa vào một thuật toán, với đầu vào là một thông báo M , 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, các kết quả băm sẽ khác nhau nếu thông báo ban đầu có bất kỳ thay đổi nào, chính vì vậy, chúng ta có thể kiểm tra được tính toàn vẹn của thông báo. 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. Chữ ký số được tạo ra bằng cách mã hoá tóm lược thông báo với khoá riêng và kiểm tra chữ ký số bằng cách sử dụng khoá công khai tương ứng.

Quá trình tạo và kiểm tra chữ ký số

Thông thường, quá trình tạo và kiểm tra chữ ký số bao gồm các bước sau đây:

- (a) Người ký tạo ra hoặc được cung cấp một cặp khoá;
- (b) Người ký chuẩn bị thông báo (ví dụ, theo dạng của một thông báo thư điện tử);
- (c) 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.
- (d) Người ký mã hoá tóm lược thông báo với khoá riêng. Chữ ký số chính là tóm lược thông báo được mã hoá.
- (e) Thông thường, người ký gắn chữ ký số vào thông báo.
- (f) Người ký gửi chữ ký số và thông báo (đã được mã hoá hoặc không) cho thành viên tin cậy.
- (g) 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.
- (h) Thành viên tin cậy cũng tạo ra một “tóm lược thông báo” cho thông báo nhận được, bằng cách sử dụng cùng một thuật toán băm bí mật.
- (i) Thành viên tin cậy có được tóm lược thông báo nguyên thủy, bằng cách giải mã chữ ký số nhận được bằng cách sử dụng 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 bit trong thông báo gửi đến bị sửa đổi cũng làm cho hai tóm lược thông báo khác nhau.
- (j) Khi sử dụng hệ thống chứng chỉ khoá công khai, thành viên tin cậy có được chứng chỉ từ nhà cung cấp dịch vụ chứng thực. 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. Thành viên tin cậy sử dụng khoá công khai được chứng thực có trong chứng chỉ để kiểm tra chữ ký số trên thông báo của người ký (sau khi đã kiểm tra chữ ký số của nhà cung cấp dịch vụ chứng thực có trên chứng chỉ).

• **Cơ sở hạ tầng khoá công khai (PKI)**

Việc thiết lập một cơ sở hạ tầng khoá công khai 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 sự tin cậy này, một 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 cho họ các dịch vụ;

(7) Cung cấp các dịch vụ gán nhãn thời gian;

(8) Quản lý các khoá được sử dụng cho mã hoá.

Một PKI thường dựa vào các mức cơ quan phân cấp khác nhau. Ví dụ, trong 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 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 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.

• Nhà cung cấp dịch vụ chứng thực

Để liên kết cặp khoá với một thuê bao (sẽ ký vào các thông báo

của mình trong tương lai), 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.

Để đảm bảo tính đích thực của chứng chỉ (về cả nội dung và nguồn gốc), nhà cung cấp dịch vụ chứng thực tiến hành ký số lên chứng chỉ. Chữ ký này có thể được kiểm tra bằng cách sử dụng khoá công khai của nhà cung cấp dịch vụ chứng thực nhưng lại được nhà cung cấp dịch vụ chứng thực khác chứng thực (thông qua phát hành chứng chỉ, thực chất đây là đường dẫn chứng thực), kiểm tra cho đến khi chữ ký số được tin cậy.

Chữ ký số tương ứng với một thông báo, được thuê bao tạo ra để xác thực một thông báo, hoặc được một nhà cung cấp dịch vụ chứng thực tạo ra để xác thực chứng chỉ của họ, nói chung trong trường hợp nào cũng cần gắn nhãn thời gian để chỉ ra thời điểm ký, điều này cho phép người kiểm tra xác định tính hợp lệ của một chữ ký số.

Để thuận tiện cho việc kiểm tra, chứng chỉ có thể được công bố tại một kho lưu giữ, hoặc phương tiện khác. Cụ thể, 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.

Một khi chứng chỉ được phát hành, vẫn có thể xảy ra một số trường hợp chứng chỉ không đáng tin cậy, chẳng hạn nhu 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, tùy 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 huỷ bỏ hoặc treo này.

CA có thể được 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 trong sự tin cậy vào các chứng chỉ được phát hành.

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 như, xác định xem ai là người quản lý kém gây ra sự mất mát và người sử dụng tin cậy vào các biểu diễn nào.

Phận sự của nhà cung cấp dịch vụ chứng thực hoặc cơ quan gốc là đảm bảo các yêu cầu chính sách của mình trên cơ sở phát triển. Việc lựa chọn các CA có thể dựa vào một số yếu tố, như kích thước

khoá, nhận dạng của người sử dụng. Sự tin cậy nhà cung cấp dịch vụ chứng thực phụ thuộc vào việc thực thi các chuẩn phát hành chứng chỉ, độ tin cậy của 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.

PHỤ LỤC

Trong phần này, chúng tôi sẽ giới thiệu ***“Định nghĩa chính sách chứng chỉ của CANADA”*** để bạn đọc có thể hình dung một cách cụ thể về một chính sách chứng chỉ.

ĐỊNH NGHĨA CHÍNH SÁCH CHỨNG CHỈ : CÁC CHÍNH SÁCH CHỨNG CHỈ MỨC TRUNG BÌNH DÀNH CHO CHỮ KÝ SỐ VÀ MÃ HOÁ

LỜI NÓI ĐẦU

Ủy ban cơ quan quản lý chính sách PKI của Chính phủ Canada đang xúc tiến phát triển một khung nhằm hỗ trợ cho việc viết các chính sách chứng chỉ và các quy định hoạt động chứng thực cho PKI của Chính phủ Canada.

Cơ quan quản lý chính sách (PMA) đã cộng tác với Chính phủ Liên bang Mỹ, nhằm tạo ra một khung chung. Sự cộng tác này (chủ yếu là sự tham gia của một nhóm không chính thức nghiên cứu khung chính sách Canada/Mỹ) đã đưa ra một báo cáo *Khung về quy định hoạt động chứng thực và chính sách chứng chỉ*, được công bố vào tháng 11, năm 1996. Bản báo cáo này trình bày nhiều chủ đề cần được đưa vào định nghĩa chính sách chứng chỉ hoặc CPS.

Để kiểm tra hiệu lực và tính thiết thực của khung này, PMA (cộng tác không chính thức với các chuyên gia đến từ Cơ quan an toàn Quốc gia và Viện chuẩn và công nghệ Quốc gia Mỹ) quyết định đưa ra một định nghĩa chính sách chứng chỉ. Định nghĩa chính sách chứng chỉ này nhằm vào chính sách chứng chỉ mức đảm bảo trung bình. Được chia thành 2 phần, phần I là chính sách chứng chỉ dành cho các ứng dụng chữ ký số, phần II là chính sách chứng chỉ dành cho các ứng dụng thiết lập khoá mã.

ĐỊNH NGHĨA

Dữ liệu kích hoạt: Các giá trị dữ liệu, trừ khoá, được yêu cầu để làm cho các môđun mật mã hoạt động. Chúng cần được bảo vệ (chẳng hạn, PIN).

Quy định hoạt động chứng thực (CPS): Quy định về các hoạt động mà một CA tuân theo khi phát hành các chứng chỉ.

Thực thể cuối: Một người, hoặc một hệ thống máy tính là chủ thể hoặc người sử dụng chứng chỉ, không phải là CA, hoặc RA. Thực thể cuối là một thuê bao, thành viên tin cậy, hoặc cả hai.

Thực thể: CA, RA hoặc thực thể cuối.

Cơ quan đăng ký (RA): Thực thể có trách nhiệm nhận dạng và xác thực các chủ thể của chứng chỉ, nhưng không ký và phát hành các chứng chỉ.

Thành viên tin cậy: Người hoạt động dựa vào sự tin cậy chứng chỉ và/hoặc các chữ ký số được kiểm tra bằng cách sử dụng chứng chỉ này. Trong tài liệu này, thuật ngữ "người sử dụng chứng chỉ" và "thành viên tin cậy" được sử dụng thay cho nhau.

Chủ thể: Thực thể có khoá công khai được chứng thực trong một chứng chỉ khoá công khai.

Thuê bao: Xem chủ thể.

DANH SÁCH CÁC TỪ VIẾT TẮT

CA Cơ quan chứng thực
CAA Người quản trị của cơ quan chứng thực
CAW Trạm làm việc của CA
CPS Quy định hoạt động chứng thực
CRL Danh sách các chứng chỉ bị thu hồi
DAP Giao thức truy nhập thư mục
FIPS Chuẩn xử lý thông tin Liên bang (Mỹ)
FTP Giao thức truyền tệp
HTTP Giao thức truyền siêu văn bản
I&A Nhận dạng và xác thực
IEC Ủy ban kỹ thuật điện Quốc tế
IETF Tổ công tác kỹ thuật Internet

IP Giao thức Internet
ISO Tổ chức tiêu chuẩn hoá Quốc tế
ISSO Nhân viên an ninh của hệ thống thông tin
ITU Liên minh viễn thông Quốc tế
LDAP Giao thức truy nhập thư mục nhanh
MSP Giao thức an toàn thông báo
NIST Viện chuẩn và công nghệ Quốc gia
NSA Cơ quan an toàn Quốc gia
PIN Số hiệu nhận dạng cá nhân
PKI Cơ sở hạ tầng khoá công khai
PKITWG Nhóm nghiên cứu kỹ thuật cơ sở hạ tầng khoá công khai
PKIX Cơ sở hạ tầng khoá công khai (X.509)
RA Cơ quan đăng ký
RFC Yêu cầu kiến nghị
SA Người quản trị hệ thống
SMTP Giao thức chuyển thư đơn giản
TCSEC Bộ tiêu chuẩn đánh giá hệ thống máy tính tin cậy
URI Tên tài nguyên duy nhất
URL Bộ định vị tài nguyên

PHẦN I

CHÍNH SÁCH CHỨNG CHỈ DÀNH CHO CÁC ỨNG DỤNG CHỮ KÝ SỐ

1 GIỚI THIỆU

1.1 Tổng quan

Chính sách chứng chỉ là một "tập các quy tắc được đặt tên, chỉ ra khả năng áp dụng của một chứng chỉ vào một cộng đồng riêng và/hoặc lớp ứng dụng với các yêu cầu an toàn chung" [X.509]. Định nghĩa chính sách chứng chỉ được đăng ký và gán một "*tên đối tượng*" duy nhất, tên này nằm trong trường mở rộng chuẩn của chứng chỉ X.509. Bằng cách kiểm tra trường này, hệ thống sử dụng chứng chỉ có thể xác định được chứng chỉ có mục đích sử dụng phù hợp với một ứng dụng riêng hay không.

Các chính sách chứng chỉ có khả năng áp dụng khác nhau. Ví dụ, một chính sách chứng chỉ có thể được định nghĩa và sử dụng trong miền của một CA hoặc tổ chức đơn lẻ; trong trường hợp này, chính sách chứng chỉ không khác gì một CPS trong đó quy định các hoạt động mà CA tuân theo khi phát hành các chứng chỉ [ABA].

Tuy nhiên, chính sách chứng chỉ được định nghĩa trong tài liệu này có khả năng áp dụng rộng rãi, cho tất cả các bộ và cơ quan của chính phủ Canada, Liên bang Mỹ và các môi trường tiềm ẩn khác.

Chính sách chứng chỉ trong phần này dành cho các ứng dụng chữ ký số. (Chính sách trong phần II dành cho các ứng dụng thiết lập khoá mã.) Các chứng chỉ được phát hành tuân theo chính sách này thích hợp cho việc kiểm tra định danh của các thư điện tử, máy chủ Web của các tổ chức có các quan hệ kinh doanh được thiết lập từ trước, kiểm tra tính toàn vẹn của phần mềm và các tài liệu được công bố trên một máy chủ Web cục bộ, hợp đồng mua bán hàng hoá và dịch vụ có giá trị cao.

1.2 Nhận dạng

Tên chính sách chứng chỉ: PKIPrivacyCertPcy:3.0-

Medium Assurance

Tên đối tượng: {đề được cung cấp}

1.3 Cộng đồng và khả năng áp dụng

Mục này miêu tả cộng đồng dự định sử dụng chính sách chứng chỉ này và chỉ ra các ứng dụng hỗ trợ.

Chính sách chứng chỉ này được thiết kế nhằm đáp ứng các yêu cầu của Chính phủ Canada và Liên bang Mỹ, nhưng sử dụng của nó không bị hạn chế cho các môi trường của các chính phủ này.

1.3.1 Các cơ quan chứng thực

Mọi cơ quan chứng thực (CA) thoả mãn các điều kiện sau có thể phát hành các chứng chỉ có nhận diện chính sách chứng chỉ này:

- CA cam đoan tuân theo các quy định của định nghĩa chính sách chứng chỉ này; và
- CA công bố một CPS có tham chiếu đến chính sách chứng chỉ này.

Cho phép chứng thực các CA cấp dưới, hoặc các CA ngang hàng thông qua chứng thực chéo. Để có thể quản lý tốt, CA nên xem xét kỹ các chính sách và các thủ tục hoạt động của CA ngang hàng, dàn xếp mọi bổ sung và các đảm bảo của thủ tục hoạt động, các giới hạn của việc sử dụng chứng chỉ chéo, khoảng thời gian tồn tại hợp lệ của chứng chỉ chéo, số lượng giao dịch giữa các thuê bao, các vấn đề về trách nhiệm pháp lý,... Mọi thoả thuận giữa các CA chứng thực chéo nên được lưu vào tài liệu, thuê bao của các CA này đều được biết.

1.3.2 Các cơ quan đăng ký

Mọi cơ quan đăng ký (RA) thoả mãn các điều kiện sau có thể hoạt động trong chính sách chứng chỉ này:

- RA cam đoan tuân theo các quy định của định nghĩa chính sách chứng chỉ này;
- RA nên đăng ký và có được sự phê chuẩn của một CA đã phát hành các chứng chỉ phù hợp với chính sách chứng chỉ này, như đã được trình bày trong mục 1.3.1.

Một RA có thể sử dụng các đại lý, trong đó mỗi đại lý chịu trách nhiệm trực tiếp đối với các giao dịch mà nó thực hiện thay mặt cho

RA. Do chính sách này yêu cầu người đăng ký chứng chỉ phải xuất hiện trước RA, nên số lượng RA và các đại lý của nó tùy thuộc vào vị trí vật lý của các thuê bao của CA.

1.3.3 Các thực thể cuối

Các thuê bao được chứng thực tuân theo chính sách này nên độc lập hoặc kết hợp với một nhà tài trợ được CA công nhận.

Thông thường, nhà tài trợ là một đối tượng liên kết với thuê bao (ví dụ, người làm công, người sử dụng dịch vụ, hoặc dạng khách hàng khác). Nhà tài trợ nên cung cấp tên, các chi tiết liên hệ (bao gồm địa chỉ thư điện tử hoặc số hòm thư, số điện thoại) và thông tin nhận dạng tổ chức của từng thực thể cuối được CA chứng thực. Thông tin này được CA sử dụng làm thông tin hoặc tài liệu đăng ký khác cho những người xin cấp chứng chỉ, để sinh ra các giá trị cho trường tên chủ thể, đồng thời kiểm tra tính xác thực của các yêu cầu chứng thực mà CA và RA nhận được.

Nếu thuê bao là một cá nhân độc lập, thì cơ sở cho việc nhận dạng và xác thực được thiết lập trực tiếp giữa thuê bao và CA hoặc RA.

1.3.4 Khả năng áp dụng

Chính sách chứng chỉ này dành cho các ứng dụng kiểm tra chữ ký số. Chính sách này áp dụng cho CA và các đại lý của CA, các kho lưu giữ chứng chỉ hoặc CRL mà CA và người điều hành của CA sử dụng, các thực thể được CA chứng thực.

1.3.4.1 Các ứng dụng thích hợp

Các chứng chỉ được phát hành tuân theo chính sách này thích hợp cho việc kiểm tra định danh của điện tử, máy chủ Web của các tổ chức có các quan hệ kinh doanh được thiết lập từ trước, kiểm tra tính toàn vẹn của phần mềm và các tài liệu được công bố trên một máy chủ Web cục bộ, hợp đồng mua bán hàng hoá và dịch vụ có giá trị cao. Chính sách chứng chỉ có thể được sử dụng với các giao thức ứng dụng khác nhau, chẳng hạn như S/MIME, giao thức truyền siêu văn bản an toàn (S-HTTP), giao thức an toàn thông báo (MSP) và giao thức truy nhập thư mục (DAP).

1.3.4.2 Các ứng dụng được phê chuẩn

Không quy định.

1.3.4.3 Các ứng dụng bị ngăn cấm

Không quy định.

1.4 Các chi tiết liên hệ

1.4.1 Tổ chức quản lý đặc tả

Chính sách chứng chỉ này do Cơ quan quản lý chính sách PKI của Chính phủ Canada quản lý, Ottawa, Ontario, Canada.

1.4.2 Người liên hệ

Chủ tịch, Ủy ban cơ quan quản lý chính sách PKI của Chính phủ Canada

Văn phòng Ủy ban tài chính

300 Laurier Ave.W.

Ottawa, Ontario. K1A 0R5

1.4.3 Người quyết định khả năng phù hợp của CPS với chính sách

Như trong mục 1.4.2.

2. CÁC ĐIỀU KHOẢN CHUNG

2.1 Trách nhiệm pháp lý

2.1.1 Trách nhiệm pháp lý của CA

2.1.1.1 Các đảm bảo và giới hạn đối với các đảm bảo

CA đảm bảo và cam kết thực hiện:

- Cung cấp các dịch vụ chứng thực và kho lưu giữ phù hợp với chính sách chứng chỉ này;
- Cung cấp các kiểm soát yêu cầu tuân theo các mục 4 ÷ 6 của định nghĩa chính sách chứng chỉ này;
- Tiến hành các thủ tục xác thực được đưa ra trong mục 3 của định nghĩa chính sách chứng chỉ này;
- Phát hành các chứng chỉ phù hợp với định nghĩa chính sách chứng chỉ này và tôn trọng các biểu diễn dành cho thuê bao và thành viên tin cậy được đưa ra trong bất kỳ CPS được công bố nào;
- Công bố các chứng chỉ trong một kho lưu giữ để cộng đồng người sử dụng có thể dễ dàng tìm kiếm;
- Hỗ trợ quyền của các thuê bao và thành viên tin cậy (người sử dụng chứng chỉ) phù hợp với các luật và dự luật có thể áp dụng;

- Hủy bỏ các chứng chỉ và phát hành các CRL (danh sách các chứng chỉ bị thu hồi) phù hợp với mục 4 của định nghĩa chính sách chứng chỉ này (điều khoản treo chứng chỉ là tùy chọn đối với CA);

- Đảm bảo cấp mới các chứng chỉ khi hết hạn;

- Tuân theo tất cả các điều khoản trong mục 2 của định nghĩa chính sách chứng chỉ này và bất kỳ điều khoản pháp lý có trong một CPS được công bố.

Ngoài các đảm bảo trên, các CA có thể đưa ra các đảm bảo khác (không yêu cầu). Thêm vào đó, luật có thể yêu cầu thêm các đảm bảo khác đối với các CA.

2.1.1.2 Các từ chối

CA có thể đưa ra các từ chối và các giới hạn nghĩa vụ trong CPS của mình, không mâu thuẫn với các đảm bảo đã được đưa ra trong mục 2.1.1.1.

2.1.1.3 Các giới hạn mất mát

Trong CPS của mình, CA có thể đưa ra một quy định loại trừ các yếu tố thiệt hại xác định, bao gồm các thiệt hại gián tiếp, đặc biệt, ngẫu nhiên, do hậu quả, hoặc các thiệt hại do mất mát lợi nhuận, dữ liệu, hoặc phát sinh khi kết nối với các dịch vụ của CA.

CA có thể xác định một giới hạn cho các thiệt hại, phạm vi đối với một **cap** (là một hợp đồng hoặc luật về các thiệt hại mà một thành viên phải chịu trách nhiệm), cho các thiệt hại phát sinh từ việc sử dụng chứng chỉ được phát hành tuân theo chính sách này.

2.1.1.4 Các loại trừ khác

Một CA có thể quy định các loại trừ khác trong CPS của mình, không mâu thuẫn với các điều khoản của định nghĩa chính sách chứng chỉ này.

2.1.2 Trách nhiệm pháp lý của cơ quan đăng ký (RA)

2.1.2.1 Các đảm bảo và giới hạn đối với các đảm bảo

Các RA đảm bảo và cam kết thực hiện:

- Cung cấp các kiểm soát yêu cầu trong mục 4÷6 của định nghĩa chính sách chứng chỉ này;

- Tiến hành các thủ tục xác thực trong mục 3 của định nghĩa chính sách chứng chỉ này;

- Thực hiện nghĩa vụ của một RA và hỗ trợ quyền của các thuê bao và thành viên tin cậy (người sử dụng các chứng chỉ) phù hợp với các luật và dự luật của liên bang, nước và địa phương.

- Tuân theo tất cả các điều khoản trong mục 2 của định nghĩa chính sách chứng chỉ này và bất kỳ điều khoản pháp lý nào có trong một CPS được công bố.

2.1.2.2 Các từ chối

CA có thể đưa ra các từ chối và giới hạn nghĩa vụ trong CPS của mình, không làm mâu thuẫn với các đảm bảo được đưa ra trong mục 2.1.2.1.

2.1.2.3 Các giới hạn mất mát

CA có thể đưa ra một quy định loại trừ các yếu tố thiệt hại xác định, bao gồm các thiệt hại gián tiếp, đặc biệt, ngẫu nhiên hoặc do hậu quả, hoặc các thiệt hại do mất mát lợi nhuận, dữ liệu, hoặc phát sinh khi kết nối với các dịch vụ của RA.

Một CPS có thể quy định giới hạn cho các thiệt hại.

2.1.2.4 Các loại trừ khác

Không quy định.

2.2 Các nghĩa vụ

2.2.1 Các nghĩa vụ của CA

2.2.1.1 Độ chính xác của các biểu diễn

Bằng cách công bố một chứng chỉ trong kho lưu giữ công khai của mình, CA chứng nhận với tất cả những người tin cậy vào thông tin có trong chứng chỉ rằng CA đã phát hành chứng chỉ cho thuê bao (có tên trong chứng chỉ) và thuê bao này đã chấp nhận chứng chỉ.

2.2.1.2 Bảo vệ khoá riêng của CA

CA nên bảo vệ khoá riêng của mình, phù hợp với các điều khoản có trong mục 6 của định nghĩa chính sách chứng chỉ này.

2.2.1.3 Các giới hạn trong việc sử dụng khoá riêng của CA

Khoá riêng của CA được sử dụng cho việc phát hành các chứng chỉ tuân theo chính sách chứng chỉ này chỉ nên được sử dụng vào việc ký các chứng chỉ và CRL (tuỳ chọn). Nếu CA hỗ trợ các chính sách khác, nhất định chúng phải được nhận diện trong CPS.

2.2.2 Nghĩa vụ của cơ quan đăng ký

2.2.2.1 Độ chính xác của các biểu diễn

Không quy định.

2.2.2.2 Bảo vệ khoá riêng của RA

RA nên bảo vệ khoá riêng của mình, phù hợp với các điều khoản có trong mục 6 của định nghĩa chính sách chứng chỉ này.

2.2.2.3 Các giới hạn trong việc sử dụng khoá riêng của RA

Khoá riêng được RA sử dụng cho các mục đích liên quan đến chức năng của RA không nên sử dụng cho bất kỳ mục đích nào khác mà không có sự chấp thuận của CA.

2.2.3 Các nghĩa vụ của thuê bao

2.2.3.1 Các biểu diễn

Bằng cách chấp nhận một chứng chỉ được phát hành phù hợp chính sách chứng chỉ này, thuê bao chứng nhận (tại thời điểm chấp nhận chứng chỉ và trong suốt khoảng thời gian hoạt động của chứng chỉ, cho đến khi thuê bao có thông báo khác) như sau:

- Không có ai khác ngoài thuê bao có khoá riêng của thuê bao;
- Tất cả các biểu diễn do thuê bao đưa ra cho CA hoặc RA về các thông tin trong chứng chỉ là đúng đắn;
- Chứng chỉ được sử dụng cho các mục đích hợp pháp và được phép, phù hợp với chính sách chứng chỉ này.

2.2.3.2 Việc bảo vệ khóa riêng của thực thể cuối

Thuê bao nên duy trì kiểm soát khoá riêng của mình, bảo vệ nó theo đúng mục 6 của định nghĩa chính sách chứng chỉ này, tiến hành các biện pháp phòng ngừa hợp lý, nhằm ngăn chặn tình trạng mất mát, khám phá, sửa đổi hoặc sử dụng trái phép.

2.2.3.3 Các giới hạn trong sử dụng khoá riêng của thực thể cuối

Không quy định.

2.2.4 Nghĩa vụ của thành viên tin cậy

2.2.4.1 Sử dụng các chứng chỉ cho mục đích thích hợp

Trách nhiệm đảm bảo rằng một chứng chỉ được sử dụng cho mục đích thích hợp là trách nhiệm của thành viên tin cậy, sau khi xem xét định nghĩa chính sách chứng chỉ này và CPS (nếu thấy cần thiết).

2.2.4.2 Trách nhiệm kiểm tra

Người dùng nên sử dụng chứng chỉ này theo đúng thủ tục phê chuẩn đường dẫn chứng thực đã được xác định trong ISO/IEC 9594-8 (ITU-T X.509).

2.2.4.3 Trách nhiệm kiểm tra tình trạng huỷ bỏ/treo

Đây là trách nhiệm của thành viên tin cậy, kiểm tra tình trạng huỷ bỏ hoặc treo của chứng chỉ trước khi sử dụng nó.

2.3 Trách nhiệm tài chính

2.3.1 Các thành viên tin cậy bồi thường

Trách nhiệm pháp lý của thực thể cuối nên phù hợp với các luật có thể áp dụng.

2.3.2 Các mối quan hệ uỷ thác

Việc phát hành các chứng chỉ phù hợp với chính sách chứng chỉ này không làm cho CA trở thành một đại lý, người được uỷ thác, hoặc đại diện khác cho các thuê bao hoặc thành viên tin cậy.

Sự trợ giúp của RA trong việc phát hành các chứng chỉ phù hợp với chính sách chứng chỉ này không làm cho RA trở thành một đại lý, người được uỷ thác, hoặc đại diện khác cho các thuê bao hoặc thành viên tin cậy.

2.4 Việc Làm sáng tỏ và sự bắt buộc tuân theo

2.4.1 Luật quản lý

Các luật và dự luật khác nhau sẽ được áp dụng, tùy thuộc vào phạm vi quyền hạn trong đó các chứng chỉ được phát hành và sử dụng. Đây là trách nhiệm của các thực thể, cần quan tâm để đảm bảo tuân theo tất cả các dự luật và luật có thể áp dụng.

2.4.2 Khả năng chia tách, tồn tại, hợp nhất

Không quy định.

2.4.3 Các thủ tục giải quyết tranh chấp

Trước tiên, cố gắng giải quyết mọi tranh chấp thông qua một người dân xếp độc lập và được chấp thuận.

Một khi có sự tham gia của người dân xếp mà vẫn không giải quyết được tranh chấp thì lúc đó mới cần đến trọng tài phân xử,

phù hợp với các luật có thể áp dụng. [Để giải quyết các tranh chấp giữa các quốc gia, các thủ tục cần được xác định rõ.]

Các thủ tục giải quyết tranh chấp nên được xác định rõ trong CPS.

2.5 Lệ phí

2.5.1 Lệ phí phát hành và cấp lại chứng chỉ

CA có thể ấn định lệ phí phát hành chứng chỉ, tùy thuộc vào thoả thuận giữa CA và thuê bao, theo đúng bảng lệ phí đã được công bố.

2.5.2 Lệ phí truy cập chứng chỉ

Lệ phí truy cập chứng chỉ có thể do CA hoặc kho lưu giữ ấn định, tùy thuộc vào thoả thuận giữa CA và thuê bao, đúng theo bảng lệ phí đã được công bố.

2.5.3 Lệ phí truy cập thông tin về luật và tình trạng thu hồi

Lệ phí truy cập thông tin về tình trạng thu hồi có thể được ấn định, tùy thuộc vào thoả thuận giữa CA và thuê bao, đúng theo bảng lệ phí đã được công bố.

2.5.4 Lệ phí cho các dịch vụ khác, chẳng hạn thông tin về chính sách

Không có lệ phí nào được ấn định cho việc cung cấp các bản sao của định nghĩa chính sách chứng chỉ này thông qua phương tiện vật lý và trực tuyến, hoặc cung cấp một cách trực tuyến các bản sao của CPS hỗ trợ chính sách chứng chỉ này.

2.5.5 Chính sách hoàn lại phí

Không quy định.

2.6 Công bố và kho lưu giữ

2.6.1 Việc công bố thông tin của CA

CA sử dụng chính sách này nên công bố trong kho lưu giữ của mình tất cả các CPS tham chiếu đến chính sách này, bản sao của tất cả các chứng chỉ có chứa tên chính sách này và các CRL thông báo tình trạng thu hồi của các chứng chỉ đó.

2.6.2 Tần xuất công bố

Các chứng chỉ nên được công bố ngay sau khi phát hành. Việc

công bố CRL nên phù hợp với mục 4.4. Việc công bố CPS nên phù hợp với mục 8.

2.6.3 Các kiểm soát truy nhập

Không cần kiểm soát việc tìm hiểu định nghĩa chính sách chứng chỉ, hoặc CPS. Kiểm soát truy nhập vào các chứng chỉ, tình trạng chứng chỉ (nếu được cung cấp như một dịch vụ của CA), hoặc các CRL là tùy chọn, theo ý muốn của CA. ở đây nên có các kiểm soát truy nhập thích hợp để kiểm soát những người có thể ghi hoặc sửa đổi tất cả các mục như vậy.

2.6.4 Các kho lưu giữ

Có thể yêu cầu một kho lưu giữ để công bố các thông tin (được nhận diện trong mục 2.6.1). Kho lưu giữ này có thể do CA, hoặc một tổ chức nào đó điều hành.

2.7 Kiểm toán theo yêu cầu

Các CA hoạt động tuân theo chính sách này cần được kiểm toán (ít nhất) hàng năm, do một hãng kiểm toán độc lập, được công nhận và tin cậy tiến hành. Hoạt động này cũng nên áp dụng cho các RA. Kết quả kiểm toán được đệ trình lên CA gốc. Nếu phát hiện có sai phạm, các CA chứng thực khác có thể:

- (1) Huỷ bỏ ngay lập tức chứng chỉ của CA;
- (2) Cho phép CA tiếp tục hoạt động trong vòng 30 ngày để giải quyết nốt mọi vấn đề trước khi huỷ bỏ;
- (3) Chỉ ra các sai phạm, nhưng cho phép CA tiếp tục hoạt động cho đến lần kiểm toán tiếp theo.

Các quyết định này tùy thuộc vào từng tình huống cụ thể, tính nghiêm trọng của các sai phạm và đề nghị của kiểm toán viên. Nếu chứng chỉ của một CA bị huỷ bỏ, CA cần thông báo cho tất cả các thuê bao của mình, chỉ rõ CA sẽ tiếp tục như thế nào, quan tâm đến các luật và dự luật có thể áp dụng.

Các kết quả kiểm toán mới nhất nên được công bố trong kho lưu giữ; các kết quả khác có thể nhận được từ CA .

2.8 Tính bí mật

CA không nên truy nhập vào khoá riêng của bất kỳ thực thể

nào được CA chứng thực. RA không nên truy nhập vào khoá riêng của bất kỳ thực thể cuối có các yêu cầu chứng thực được RA xử lý.

Nói chung, không nên cho phép truy nhập và xem xét tùy ý các nhật ký kiểm toán. Chỉ nên cho phép xem xét các bản ghi giao dịch cá nhân, mặc dù thực thể có thể xem xét tất cả các bản ghi hoạt động có sự tham gia của thực thể trong một giai đoạn nào đó.

Thông tin nhận dạng hoặc các thông tin khác của cá nhân hay công ty có trong các chứng chỉ không được coi là bí mật, trừ khi có sự bắt buộc của luật pháp, hoặc các thoả thuận đặc biệt. Mọi thông tin khác về cá nhân hoặc công ty do CA hoặc RA nắm giữ được coi là thông tin bí mật và không nên để lộ nếu thuê bao không cho phép, trừ khi luật pháp yêu cầu.

2.9 Quyền sở hữu trí tuệ

Khóa riêng và khóa công khai là tài sản của đối tượng nắm giữ khóa riêng hợp pháp, đối tượng này có thể là CA, RA, hoặc thuê bao. Trừ khi có quy định khác trong CPS, chứng chỉ là tài sản của CA phát hành.

3. NHẬN DẠNG VÀ XÁC THỰC

Mục này trình bày các hoạt động được tiến hành khi nhận dạng và xác thực các cá nhân và tổ chức có trong quá trình chứng thực.

3.1 Đăng ký ban đầu

3.1.1 Các kiểu tên

Các dạng tên X.509 có thể được sử dụng cho các chủ thể của chứng chỉ là Directory Name, RFC822, DNS, URI, hoặc địa chỉ IP. Các CA và RA nên có Directory Name (tên thư mục), nhưng cũng có thể có nhiều tên lựa chọn theo các dạng khác.

3.1.2 Yêu cầu đặt tên có nghĩa

Trong Directory Name, tên của một tổ chức và tên thông thường (Common Name) của cá nhân phải hợp pháp khi sử dụng. Nói chung, ở đây không có yêu cầu: tên trong các dạng tên khác phải có nghĩa, mặc dù trong yêu cầu xin cấp chứng chỉ, người xin cấp chứng chỉ phải chứng minh việc sử dụng một tên hợp pháp. Các điều khoản chi tiết có thể được đưa ra trong CPS.

3.1.3 Các nguyên tắc trong việc làm sáng tỏ các dạng tên

Xem mục 3.1.2

3.1.4 Tính duy nhất của các tên

Các tên nên rõ ràng, phân biệt với tất cả các tên chủ thể có trong các chứng chỉ do cùng một CA phát hành.

3.1.5 Các thủ tục giải quyết tranh chấp yêu cầu tên

Không quy định. Điều này do riêng CA và các thuê bao của CA tự thoả thuận.

3.1.6 Sự công nhận, xác thực và vai trò của nhãn hiệu đăng ký trong I&A

Không quy định. Điều này do riêng CA và các thuê bao của CA tự thoả thuận.

3.1.7 Phương pháp chứng minh quyền sở hữu đối với khoá riêng

Quá trình đăng ký nên bao gồm thêm một giai đoạn, trong đó người xin cấp chứng chỉ chứng minh quyền sở hữu đối với khoá riêng, bằng cách tạo ra một thông báo được ký số bằng khoá riêng này.

3.1.8 Xác thực định danh của tổ chức

Trong chứng chỉ được phát hành cho một tổ chức, CA và RA nên xác nhận tên của thực thể kinh doanh, cũng như địa chỉ và các thông tin đăng ký khác, bằng cách điều tra từ một nguồn thích hợp. Với một tổ chức thương mại, yêu cầu tổ chức đưa ra ít nhất 2 tài liệu nhận dạng.

3.1.9 Xác thực định danh của cá nhân

Quá trình đăng ký chứng chỉ của thuê bao có thể khởi đầu từ người xin cấp (người muốn trở thành thuê bao), CA, RA, hoặc nhân viên của một tổ chức (là người đang phối hợp thiết lập mạng của một tổ chức). Tuy nhiên, người xin cấp cần tự giới thiệu mình với CA hoặc RA để được xác thực trước khi chứng chỉ được phát hành. CA hoặc RA nên kiểm tra xem người xin cấp chứng chỉ có nhu cầu sử dụng chứng chỉ hay không, nếu chủ thể của chứng chỉ có các thuộc tính hoặc đặc quyền riêng, thì người xin cấp cũng có các thuộc tính hoặc đặc quyền tương ứng.

3.1.9.1 Số lượng nhận dạng được yêu cầu

Khi xác thực người xin cấp chứng chỉ, CA, hoặc RA nên phê chuẩn 2 mẫu nhận dạng. Ít nhất, một mẫu nhận dạng có ảnh, chẳng hạn như thẻ nhận dạng của chính phủ hoặc quân đội, hoặc thẻ hộ chiếu. CA hoặc RA nên lưu lại các kiểu nhận dạng được sử dụng để thiết lập định danh người dùng.

3.1.9.2 Thủ tục xác nhận

Tiến hành đối chiếu với cơ sở dữ liệu của một tổ chức hoặc thành viên thứ ba (đã được phê chuẩn) để xác nhận các chi tiết mà cá nhân đưa ra.

3.1.9.3 Cần giới thiệu trực tiếp

Cá nhân nên tự giới thiệu trực tiếp với CA hoặc RA.

3.2 Thay thế khoá định kỳ

Các cặp khoá nên được thay thế định kỳ và một chứng chỉ mới được phát hành. Yêu cầu thay khoá định kỳ có thể được xác thực dựa vào một chữ ký số sử dụng cặp khoá cũ.

3.3 Thay thế khoá sau khi huỷ bỏ

Việc xác thực yêu cầu thay thế khoá sau khi huỷ bỏ phụ thuộc vào lý do huỷ bỏ. Với huỷ bỏ không phải do lộ khoá, yêu cầu thay thế khoá có thể được xác thực dựa vào một chữ ký số sử dụng cặp khoá cũ. Trong trường hợp huỷ bỏ do lộ khoá, việc xác thực sẽ được thực hiện như khi đăng ký ban đầu.

3.4 Yêu cầu huỷ bỏ

Yêu cầu huỷ bỏ có thể được xác thực dựa vào một chữ ký số sử dụng cặp khoá cũ.

4. CÁC YÊU CẦU HOẠT ĐỘNG

Mục này trình bày các yêu cầu hoạt động bắt buộc đối với CA, RA và các thực thể cuối trong chính sách này, bao gồm: xử lý các yêu cầu huỷ bỏ chứng chỉ, nhật ký kiểm toán và lưu trữ thông tin giao dịch.

4.1 Xin cấp chứng chỉ

Để có được một chứng chỉ, người xin cấp chứng chỉ nên thực

hiện đầy đủ các thủ tục sau đây:

- Tạo ra một cặp khoá và chứng minh cho CA biết đây là cặp khoá được sử dụng cho một mục đích cụ thể;
- Bảo vệ khoá riêng trong cặp khoá này, tránh làm lộ khoá;
- Đưa ra một tên phân biệt; và
- Đề trình yêu cầu xin cấp chứng chỉ cho CA.

4.2 Phát hành chứng chỉ

Việc CA phát hành một chứng chỉ chứng tỏ rằng CA đã phê chuẩn yêu cầu xin cấp chứng chỉ.

4.3 Chấp nhận chứng chỉ

Sau khi chứng chỉ được phát hành, thuê bao nên gửi xác nhận chấp nhận chứng chỉ cho CA. Quá trình này tùy thuộc vào môi trường ứng dụng cụ thể. Thông qua việc chấp nhận chứng chỉ, thuê bao chấp thuận tất cả các thuật ngữ và điều kiện có trong định nghĩa chính sách chứng chỉ này và CPS có thể áp dụng.

4.4 Treo và huỷ bỏ các chứng chỉ

Chứng chỉ của thực thể cuối bị huỷ bỏ khi thông tin có trong chứng chỉ bị thay đổi hoặc lỗi thời, hoặc khi khoá riêng (cùng cặp với khoá công khai có trong chứng chỉ) bị lộ hoặc nghi ngờ bị lộ. Ví dụ, tên của thuê bao, vai trò hoặc đặc quyền của người nắm giữ thay đổi, kết thúc hoặc tạm thời ngừng công việc, hoặc loại bỏ chức năng của hệ thống cuối. Lộ khoá bao gồm truy nhập trái phép hoặc nghi ngờ truy nhập trái phép vào khoá riêng, mất hoặc nghi ngờ mất khóa, khoá bị đánh cắp hoặc nghi ngờ bị đánh cắp, hoặc các khoá bị phá hỏng. CA có thể huỷ bỏ một chứng chỉ khi biết thuê bao không đáp ứng được nghĩa vụ (đã được đưa ra trong chính sách chứng chỉ này, trong CPS, hoặc trong bất kỳ thỏa thuận, dự luật hoặc luật bắt buộc khác). Các huỷ bỏ cần được thực hiện ngay sau khi phát hiện ra tình trạng lộ, hoặc các lý do huỷ bỏ bắt buộc khác.

Các thực thể sau đây có thể yêu cầu huỷ bỏ chứng chỉ của một thực thể cuối:

- Thực thể cuối/người nắm giữ chứng chỉ,

- CA phát hành, hoặc
- RA, thay mặt cho nhà tài trợ của thực thể cuối hoặc thực thể cuối.

Thuê bao có thể tạo ra một yêu cầu huỷ bỏ bằng điện tử, trong trường hợp này, thuê bao ký lên yêu cầu huỷ bỏ bằng cách sử dụng khoá riêng (cùng cặp với khoá công khai có trong chứng chỉ bị yêu cầu huỷ bỏ). RA có thể nhận (trực tiếp hoặc thông qua điện thoại) yêu cầu huỷ bỏ chứng chỉ từ thuê bao. RA có thể tìm kiếm xác nhận huỷ bỏ theo cách riêng, ví dụ, gọi điện cho nhà tài trợ của thuê bao trước khi chuyển tiếp yêu cầu huỷ bỏ này cho CA. CA có thể tạo ra một yêu cầu huỷ bỏ nếu biết hoặc nghi ngờ xảy ra tình trạng lộ. Tất cả các yêu cầu huỷ bỏ và hoạt động mà CA tiến hành sau đó cần được lưu lại.

Theo chính sách này, CA được yêu cầu nhằm hỗ trợ huỷ bỏ chứng chỉ, nhưng việc treo chứng chỉ là tùy chọn. CPS nên xác định rõ các điều khoản về việc treo chứng chỉ. Thông tin về chứng chỉ bị huỷ bỏ cần được cập nhật vào CRL cho đến khi thời hạn tồn tại hợp lệ (được ấn định trước) của nó kết thúc.

CA nên phát hành định kỳ các CRL. Khi thực thể cuối tải về một CRL từ một kho lưu giữ, thực thể nên kiểm tra tính đích thực của CRL, bằng cách kiểm tra chữ ký số có trên CRL và đường dẫn chứng thực liên quan. Các chứng chỉ có thể được lưu giữ cục bộ trên hệ thống của thành viên tin cậy, nhưng trước khi sử dụng các chứng chỉ này, cần kiểm tra tình trạng huỷ bỏ của chúng.

Tùy chọn, có thể sử dụng biện pháp "kiểm tra tình trạng thu hồi trực tuyến" cho giao dịch tới một máy chủ tin cậy. Mọi hỗ trợ cho thu hồi trực tuyến cần được xác định rõ trong CPS.

4.5 Các thủ tục kiểm toán an toàn

Các chức năng kiểm toán an toàn của hệ thống/máy tính được đưa ra sau đây. Để phục vụ cho các mục đích kiểm toán, CA nên ghi nhật ký về việc tạo ra các bản ghi kiểm toán (có đặc quyền hoặc không), việc cài đặt phần mềm mới và các cập nhật đối với phần mềm, thời gian hoặc các thông tin miêu tả khác về dự phòng, tắt và khởi động lại hệ thống, thời gian cập nhật phần cứng, thời gian kết xuất nhật ký kiểm toán, thời gian kết xuất thông tin giao

dịch được lưu trữ.

Các nhật ký kiểm toán cần được đảm bảo tính toàn vẹn và gắn tem thời gian. Việc gắn tem thời gian cần được tiến hành cho mỗi lần ghi. Người quản trị của CA cần ký số hàng ngày lên các nhật ký. Các nhật ký kiểm toán cần được kiểm tra và tích hợp (ít nhất) hàng tháng.

4.6 Lưu trữ các bản ghi

Các CA cần lưu trữ và sẵn sàng đáp ứng các yêu cầu hợp pháp, cung cấp tài liệu liên quan đến CPS (có thể áp dụng) của CA, cung cấp tài liệu về các hoạt động, thông tin cần thiết cho mỗi lần xin cấp chứng chỉ và thông tin cần thiết cho chứng chỉ khi phát hành. Với mỗi chứng chỉ, các bản ghi cần lưu thêm các thông tin về việc tạo, phát hành, sử dụng, treo, huỷ bỏ, kết thúc thời hạn tồn tại của chứng chỉ. Các bản ghi này nên lưu tất cả các bằng chứng liên quan thuộc sở hữu của CA, bao gồm:

- Các yêu cầu chứng chỉ và tất cả các thông báo liên quan đã trao đổi với RA, thực thể cuối và thư mục;
- Nội dung có trong các chứng chỉ được phát hành;
- Các yêu cầu cấp lại chứng chỉ và tất cả các thông báo đã trao đổi với thực thể cuối;
- Các yêu cầu huỷ bỏ chứng chỉ và tất cả các thông báo đã trao đổi với người đưa ra yêu cầu và/hoặc người nắm giữ chứng chỉ;
- Các CRL được công bố trong thư mục;
- Các nhật ký kiểm toán.

Các lưu trữ cần được duy trì và bảo vệ, tránh bị sửa đổi hoặc phá hoại trong khoảng thời gian đã được xác định rõ trong CPS, thường không thể ngắn hơn 7 năm. Nói chung, không nên để lộ các nội dung được lưu trữ, trừ khi luật pháp yêu cầu. Các bản ghi giao dịch cá nhân có thể để lộ, tùy thuộc vào yêu cầu của bất kỳ thực thể nào có trong giao dịch, hoặc các đại diện được công nhận. CA cần đảm bảo tính sẵn sàng việc lưu trữ, ngay cả khi hoạt động của CA bị gián đoạn hoặc đình chỉ.

Trong trường hợp các dịch vụ của CA bị gián đoạn hoặc đình chỉ, CA nên gửi thông báo điện tử cho tất cả các thuê bao, đảm bảo rằng khả năng lưu trữ luôn sẵn sàng. Tất cả các yêu cầu truy

nhập thông tin lưu giữ cần được gửi tới CA trước khi kết thúc dịch vụ.

4.7 Thay đổi khoá

Trong vòng 3 tháng trước khi kết thúc thời hạn sử dụng của một khoá riêng, thuê bao có thể yêu cầu phát hành một chứng chỉ mới cho một cặp khoá mới, miễn là chứng chỉ trước đó chưa bị huỷ bỏ. Việc cấp lại lần hai có thể tiến hành trực tuyến mà không cần xác thực lại chủ thể.

Các chứng chỉ mới do CA phát hành trong vòng 3 tháng trước khi kết thúc thời hạn sử dụng của một khoá riêng.

Không nên cấp lại các chứng chỉ bị huỷ bỏ hoặc đã hết hạn sử dụng. CA hoặc RA nên xác thực các thực thể không có chứng chỉ hợp lệ khi họ xin cấp chứng chỉ.

4.8 Tình trạng lộ và khôi phục sau thảm hoạ

Các thủ tục khôi phục/ dự phòng dành cho CA cần được xác định rõ trong CPS.

4.9 Kết thúc hoạt động của CA

Phù hợp với các thủ tục do tổ chức quản lý chính sách xác định.

5. CÁC KIỂM SOÁT AN TOÀN CÁ NHÂN, VẬT LÝ VÀ THỦ TỤC

Mục này trình bày các kiểm soát an toàn vật lý, thủ tục và cá nhân do CA, RA và thực thể cuối yêu cầu nhằm bảo vệ các hoạt động của họ.

5.1 Các kiểm soát an toàn vật lý

5.1.1 Các kiểm soát an toàn vật lý dành cho CA

Cần tiến hành các kiểm soát an toàn vật lý đối với các truy nhập vào phần cứng và phần mềm của CA. Các kiểm soát này bao gồm trạm làm việc, các môđun hoặc thẻ bài phần cứng mật mã bên ngoài của CA.

Chỉ nên cho phép các đối tượng thực hiện một trong các tập đặc quyền được mô tả trong mục 5.2.1 truy nhập vào trạm làm việc của CA. Có thể kiểm soát truy nhập thông qua danh sách kiểm soát truy nhập vào trạm làm việc của CA. Nếu không thể thực thi

danh sách này tại một vị trí cụ thể, cần đảm bảo rằng trạm làm việc của CA và các tài nguyên liên quan khác được khoá lại trong một phòng hoặc khu vực cất giữ an toàn khi không sử dụng đến.

Các phương tiện của CA cũng cần một nơi để lưu giữ dự phòng và được phân phối vừa đủ để tránh mất mát, làm giả hoặc sử dụng trái phép các thông tin được lưu giữ. Việc lưu giữ dự phòng cần khi khôi phục dữ liệu và lưu giữ thông tin quan trọng. Phương tiện lưu giữ dự phòng cũng cần được lập tại một vị trí khác, phòng trường hợp xảy ra thảm hoạ tự nhiên đối với các phương tiện chính.

Cần tiến hành kiểm tra an toàn toàn đối với các phương tiện tại trạm làm việc của CA ít nhất 24 tiếng/lần. Nếu chúng là phương tiện tham gia liên tục, có thể tiến hành kiểm tra lần lượt bằng trực giác để đảm bảo rằng trạm làm việc và các thiết bị/thẻ bài mật mã liên quan được cất giữ an toàn khi không sử dụng đến, do vậy, các hệ thống an toàn vật lý (chẳng hạn như khoá cửa hoặc chuông) cần hoạt động chính xác. Nếu chúng không phải là phương tiện tham gia liên tục, cần hướng dẫn kiểm tra an toàn và ghi nhật ký trước khi người cuối cùng kết thúc công việc.

5.1.2 Các kiểm soát an toàn vật lý dành cho RA

Theo chính sách này, chức năng của RA có thể khác nhau. Trong một số trường hợp, RA chỉ đơn giản là người thu thập dữ liệu, trợ giúp cho CA trong việc thu thập thông tin về việc đăng ký và huỷ bỏ từ phía người sử dụng, tiến hành xác thực người dùng và chuyển tiếp các kết quả cho CA. Trong một số trường hợp khác, khi các thẻ bài phân cứng mật mã được sử dụng, RA có thêm chức năng như nạp chứng chỉ vào thẻ bài. Kiểm soát an toàn vật lý của các kiểu RA khác nhau.

Nếu RA chỉ đóng vai trò là người kiểm tra/chuyển tiếp thông tin, thì kiểm soát an toàn vật lý bắt buộc là sử dụng một tủ lưu các tệp có thể khoá được, để lưu giữ các bản ghi về đăng ký của thực thể cuối và các thẻ bài được sử dụng để truy nhập vào trạm làm việc của RA. Trạm làm việc phần cứng và phần mềm có thể được để trong môi trường văn phòng thông thường.

Nếu trạm làm việc của RA nắm giữ các thông tin bí mật của thực thể cuối (bao gồm các tham số về khoá của thực thể cuối) thì

kiểm soát an toàn vật lý của RA nên ngang bằng với các kiểm soát an toàn vật lý của CA (đã được trình bày trong mục 5.1.1).

5.1.3 Các kiểm soát an toàn vật lý dành cho thực thể cuối

Thực thể cuối nên bảo vệ vật lý đối với mật khẩu hoặc PIN được dùng để truy nhập vào hệ thống của thực thể cuối. Thông thường, mật khẩu hoặc PIN được ghi nhớ và không nên viết ra. Nếu một PIN hoặc mật khẩu cần phải viết ra, nó nên được lưu giữ trong một tủ lưu các tệp có khoá hoặc một vật đựng chỉ có người được chỉ định truy nhập vào đó.

Nếu thực thể cuối sử dụng một thẻ bài mật mã trong đó chứa khoá riêng, thẻ bài cần được bảo vệ tương tự như các thẻ chứa thông tin cá nhân có giá trị, chẳng hạn như thẻ tín dụng hoặc bằng lái xe. PIN hoặc mật khẩu (được sử dụng để truy nhập thẻ bài) không bao giờ được lưu giữ ở cùng vị trí, chẳng hạn trên chính thẻ bài. Nếu khoá riêng được mã hoá và lưu giữ trên một đĩa mềm hoặc phương tiện không an toàn khác, thì đĩa mềm hoặc phương tiện này cần được cất giữ trong một tủ lưu các tệp có khoá hoặc vật đựng khi không sử dụng đến.

Trạm làm việc có chứa các khoá riêng được mã hoá trên ổ cứng phải được đảm bảo an toàn vật lý và được bảo vệ với một sản phẩm kiểm soát truy nhập thích hợp.

5.2 Các kiểm soát thủ tục

5.2.1 Các tập đặc quyền tin cậy

5.2.1.1 Các tập đặc quyền tin cậy dành cho CA

Để đảm bảo một thành viên không thể phá vỡ toàn bộ tình trạng an toàn, trách nhiệm tại trạm làm việc của một CA cần được tách thành các tập đặc quyền và chia sẻ cho các cá nhân. Khả năng của mỗi account trên trạm làm việc của CA bị giới hạn, ứng với tập đặc quyền mà account đó nắm giữ.

Khuyến nghị rằng, CA (hỗ trợ chính sách chứng chỉ này) nên có ít nhất 3 tập đặc quyền khác nhau, chẳng hạn như các tập đặc quyền sau đây:

(a) Người quản trị của CA (CAA)

Tập đặc quyền của CAA bao gồm:

- Tạo chứng chỉ;
- Lập trình và phân phối an toàn các thẻ bài mật mã của thuê bao;

- Tạo, phân phối và quản lý các CRL;
- Các chức năng quản trị liên quan tới việc duy trì cơ sở dữ liệu của CA và hỗ trợ điều tra tình trạng lộ.

(b) Người quản trị của hệ thống (SA)

Tập đặc quyền của SA bao gồm:

- Định cấu hình ban đầu cho hệ thống, trong đó khởi động boot an toàn và đóng trạm làm việc;
- Thiết lập ban đầu đối với tất cả các account mới;
- Thiết lập cấu hình mạng ban đầu;
- Tạo ra các hệ thống khẩn cấp khởi động lại phương tiện để khôi phục những mất mát nghiêm trọng của hệ thống;
- Tiến hành sao chép dự phòng hệ thống, khôi phục và cập nhật phần mềm, bao gồm lưu giữ và phân phối an toàn các sao chép dự phòng và các nâng cấp tại một vị trí khác. Các sao chép dự phòng cần được tiến hành ít nhất một lần/tuần, đồng thời kiểm tra tính toàn vẹn của phần cứng.
- Thay đổi tên máy chủ và/hoặc địa chỉ mạng.

(c) Nhân viên an ninh của hệ thống thông tin (ISSO)

Tập đặc quyền của ISSO bao gồm:

- Gán các đặc quyền an toàn và kiểm soát truy nhập của người dùng;
- Gán mật khẩu cho tất cả các account mới;
- Lưu giữ các bản ghi của hệ thống theo yêu cầu;
- Xem xét lại nhật ký kiểm toán trước khi xóa bỏ để biết được CAA có tuân theo chính sách an toàn hệ thống hay không. Việc xem xét nhật ký kiểm toán cần được tiến hành ít nhất 11 lần/tuần.
- Hướng dẫn hoặc giám sát hàng năm đối với bảng kiểm kê các bản ghi của CA.

Lưu ý rằng, ISSO (không trực tiếp tham gia vào quá trình phát hành chứng chỉ) chỉ thực hiện chức năng giám sát, bằng cách xem xét các bản ghi của hệ thống hoặc nhật ký kiểm toán, để đảm bảo rằng những người khác đang hoạt động theo đúng trách nhiệm

của họ và theo đúng chính sách an toàn đã được đề ra.

5.2.1.2 Tập đặc quyền tin cậy dành cho RA

Nếu RA thực hiện tất cả các chức năng của một CA, ngoại trừ việc ký các chứng chỉ, thì RA cũng cần có các kiểm soát thủ tục tương tự như CA.

Nếu RA chỉ đóng vai trò là người thu thập thông tin, nhằm trợ giúp CA trong việc đăng ký các thực thể mới, thì không quy định các kiểm soát thủ tục đặc biệt nào.

5.2.1.3 Tập đặc quyền tin cậy dành cho các thực thể cuối

Không quy định.

5.2.2 Số lượng người yêu cầu / nhiệm vụ

Với một CA, cần ít nhất 1 cá nhân thực hiện từng tập đặc quyền trong 3 tập đặc quyền được trình bày ở trên.

Việc sinh cặp khoá và thiết lập các thẻ bài của CA yêu cầu số thành viên tham gia tích cực ít nhất là 3 cá nhân, đây là những cá nhân có các tập đặc quyền của CAA và ISSO.

5.2.3 Việc xác thực và nhận dạng cho từng tập đặc quyền

Tuỳ thuộc vào các hoạt động thông thường đối với các vị trí nhạy cảm này.

5.3 Các kiểm soát an toàn cá nhân

5.3.1 Các kiểm soát an toàn cá nhân dành cho CA

Cá nhân đảm nhận tập đặc quyền của CAA nên là người tin cậy, trung thành và chính trực, có thể chứng minh được sự hiểu biết và nhận thức về an toàn của mình trong các hoạt động hàng ngày.

Tất cả cá nhân trong vị trí nhạy cảm này (bao gồm cả vị trí CAA và ISSO) nên:

- Không được gán thêm các nhiệm vụ khác mà có thể gây cản trở cho trách nhiệm và nhiệm vụ của họ;
- Không được chủ tâm giảm bớt nhiệm vụ quy định vì lý do không thể hoàn thành nhiệm vụ của mình;
- Được một cơ quan phê chuẩn bổ nhiệm; và
- Được đào tạo để hoàn thành nhiệm vụ của mình.

Các tổ chức của CA cũng nên xác định rõ các yêu cầu đặc biệt, chẳng hạn như các yêu cầu về quyền công dân, địa vị xã hội, phẩm chất tư cách, kiểm tra thẻ tín dụng,... Các yêu cầu này cần được xác định trong CPS có thể áp dụng.

5.3.2 Các kiểm soát an toàn cá nhân dành cho RA

Các khả năng của RA có thể khác nhau tùy thuộc vào hệ thống và các kiểm soát cá nhân gắn liền với RA cũng sẽ khác nhau.

Khi RA thực hiện tất cả các chức năng của CA, ngoại trừ việc ký các chứng chỉ, các kiểm soát cá nhân của RA cũng giống như các kiểm soát cá nhân dành cho CA được trình bày ở trên (ngoài trừ việc đào tạo phải tùy thuộc vào các chức năng của RA).

Nếu RA chỉ đóng vai trò là người kiểm tra/chuyển tiếp thông tin, thì các yêu cầu ít nghiêm ngặt hơn. Tổ chức của RA cần đảm bảo rằng, cá nhân thực hiện các nhiệm vụ của RA phải là người tin cậy, được đào tạo để có thể thực hiện phần mềm của RA, cũng như các chính sách và hoạt động đăng ký theo hướng dẫn này.

5.3.3 Các kiểm soát an toàn cá nhân dành cho thực thể cuối

Các thực thể cuối cần biết mọi hoạt động an toàn mà họ tuân theo khi bảo vệ trạm làm việc, cũng như các thiết bị mật mã của họ. CA có trách nhiệm đào tạo đối với tất cả các thực thể cuối trong miền của mình.

6. CÁC KIỂM SOÁT AN TOÀN KỸ THUẬT

Mục này trình bày các điều khoản về việc quản lý cặp khoá riêng/công khai dành cho CA, RA, thực thể cuối và các kiểm soát kỹ thuật tương ứng.

6.1 Sinh và cài đặt cặp khoá

6.1.1 Sinh cặp khoá

Mỗi thực thể cuối tạo ra một cặp khoá cho riêng mình.

6.1.2 Chuyển giao khoá riêng cho thực thể

Xem mục 6.1.1.

6.1.3 Chuyển giao khoá công khai cho người phát hành chứng chỉ

Ngăn chặn, không cho phép sửa đổi hoặc thay thế thủ công,

hoặc qua một trao đổi trực tuyến có ký nhận.

6.1.4 Chuyển giao khoá công khai của CA cho người dùng

Cơ chế phân phối khoá gốc được sử dụng ở đây do tổ chức quản lý chính sách đưa ra.

6.1.5 Kích thước khoá

Kích thước khoá tối thiểu là 1024 bit lấy theo modulo p đối với DSA, hoặc 1024 bit lấy theo modulo n đối với RSA.

6.1.6 Sinh các tham số khoá công khai

Với DSA, các tham số nên được một cơ quan trung tâm sinh ra và cung cấp.

6.1.7 Kiểm tra chất lượng tham số

Với DSA, chất lượng của các tham số cần được kiểm tra, phù hợp với FIPS PUB 186, trong hệ thống sinh khi các tham số được sinh ra.

6.1.8 Sinh khoá phần mềm/phần cứng

Với CA và RA, việc sinh khoá cần được thực hiện trong phần cứng. Với các thực thể cuối, việc sinh khoá có thể được thực hiện trong phần cứng hoặc phần mềm.

6.1.9 Mục đích sử dụng khoá (Như X.509 phiên bản 3)

Các khoá có thể được sử dụng cho các mục đích chữ ký số hoặc chống chối bỏ; Các khoá của CA cũng có thể được sử dụng cho các mục đích ký chứng chỉ hoặc ký CRL.

6.2 Bảo vệ khoá riêng

6.2.1 Các chuẩn dành cho mô đun mật mã

Khoá của CA nên được tạo ra và duy trì trong một mô đun mật mã, ít nhất được phê chuẩn ở mức 2 của FIPS 140-1, với mức 3 trong khuyến nghị [FIPS].

RA nên tiến hành tất cả các hoạt động mật mã trong mô đun mật mã, ít nhất được phê chuẩn ở mức 1 của FIPS 140-1.

Thực thể cuối nên sử dụng các mô đun phần cứng mật mã khi bảo vệ khoá riêng, hoặc sử dụng các thuật toán mật mã được phê chuẩn để mã hoá các khoá riêng của người dùng khi lưu giữ trong

bộ nhớ máy tính, hoặc phương tiện từ khi không sử dụng đến. Các khoá riêng (được lưu giữ) có thể được mã hoá trong một ổ cứng khi và chỉ khi hệ thống được đảm bảo an toàn vật lý, hoặc được bảo vệ với một sản phẩm kiểm soát truy nhập thích hợp.

6.2.2 Khoá riêng có nhiều người kiểm soát

Với CA, yêu cầu cần 2 người kiểm soát. Với RA và các thực thể, chỉ chấp nhận một người kiểm soát.

6.2.3 Lưu trữ, sao lưu dự phòng và uỷ nhiệm khoá riêng

Khoá riêng không cần uỷ nhiệm. Tùy chọn, một thực thể có thể sao lưu dự phòng khoá riêng của mình (xem mục 4.6). Không nên lưu trữ các khoá riêng.

6.2.4 Khoá riêng được sử dụng trong mô đun mật mã

Nếu sử dụng một mô đun mật mã, khoá riêng được sinh ra và duy trì trong mô đun đó.

6.2.5 Phương pháp huỷ bỏ khoá riêng

Khi không sử dụng đến khoá riêng được sử dụng cho mục đích tạo chữ ký, tất cả các bản sao của khoá riêng cần được huỷ bỏ an toàn.

6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá

6.3.1 Lưu trữ khoá công khai

Tất cả khoá công khai do CA lưu trữ.

6.3.2 Khoảng thời gian sử dụng khoá công khai và khoá riêng

Với các CA, mọi khoá riêng được sử dụng cho mục đích ký chứng chỉ có khoảng thời gian sử dụng không quá 2 năm, chứng chỉ được phát hành cho khoá công khai có khoảng thời gian tồn tại hợp lệ không quá 10 năm.

Với các RA và thực thể cuối, một khoá riêng được sử dụng cho mục đích ký có khoảng thời gian sử dụng tới 5 năm, hoặc ngắn hơn nếu được xác định rõ trong chứng chỉ, chứng chỉ được phát hành cho khoá công khai có khoảng thời gian tồn tại hợp lệ không quá 10 năm.

6.4 Dữ liệu kích hoạt

Không quy định.

6.5 Các kiểm soát an toàn máy tính

Trạm làm việc của CA (CAW) nên cung cấp đủ các kiểm soát an toàn máy tính cho việc tách bạch các tập đặc quyền được mô tả trong mục 5.2.

CAW nên được đánh giá ít nhất tại mức TCSEC C2 (mức EAL3 Bộ tiêu chuẩn chung, hoặc ngang bằng với mức được định nghĩa trong bộ tiêu chuẩn thích hợp khác) [TCSEC]. Trạm làm việc (không được đánh giá theo một bộ tiêu chuẩn được chấp nhận) có thể được sử dụng như CAW nếu một người (được tổ chức quản lý chính sách công nhận) xác định được trạm làm việc và hệ điều hành của nó cung cấp một mức (có thể chấp nhận được) các chức năng kiểm soát truy nhập tùy ý (có nghĩa là dựa vào định danh), nhận dạng, xác thực và kiểm toán.

Nếu CAW được kết nối với một mạng bên ngoài, nó cần được bảo vệ bằng bức tường lửa đủ mạnh để chống lại các tấn công có thể xảy ra trên mạng.

Các kiểm soát an toàn máy tính trên trạm làm việc do RA sử dụng phụ thuộc vào tập đặc quyền dành cho RA. Khi RA nạp chứng chỉ vào thẻ bài phần cứng, RA nên đáp ứng các yêu cầu xác định trên CAW. Nếu RA chỉ đơn giản là người kiểm tra/chuyển tiếp thông tin, thì các trạm làm việc mà nó sử dụng không yêu cầu đánh giá TCSEC nhưng phải hỗ trợ hợp ý cho các nhật ký kiểm toán, kiểm soát truy nhập và gán tem thời gian cho các mục đích giải trình.

6.6 Các kiểm soát kỹ thuật đối với chu kỳ tồn tại

6.6.1 Các kiểm soát phát triển hệ thống

Một trong các hướng tiếp cận sau đây cần được sử dụng nhằm chống sửa đổi phần mềm thực hiện chức năng của CA và RA:

1. Phần mềm được phát triển trong một môi trường có kiểm soát, chẳng hạn trong môi trường được đánh giá tương đương với mức T2 hoặc cao hơn trong "Phương pháp luận phát triển phần mềm tin cậy" (TSMD).

2. Tổ chức điều hành trạm làm việc của CA hoặc RA cần thu được và xem xét chương trình nguồn thực hiện ứng dụng, kiểm tra

lôgic để không tạo thêm các bản sao khoá riêng hoặc sử dụng các chức năng mật mã. Do sử dụng trình biên dịch, gọi các thư viện và các công cụ khác khi tạo ra chương trình từ chương trình nguồn, sự khó khăn khi phân tích chương trình nguồn, nên điều này này ít được lựa chọn.

3. Các trạm làm việc của CA và RA có thể dựa vào các sản phẩm thương mại sẵn có, không lạm dụng các kiểm soát phát triển trong đó.

6.6.2 Các kiểm soát quản lý an toàn

Xem mục 5.2. Các tập đặc quyền này nên được thực hiện và tuân theo và thực hiện.

6.7 Các kiểm soát an toàn mạng

Khi trạm làm việc của CAW và RA kết nối với một mạng, nó cần được bảo vệ bằng một bức tường lửa thích hợp, như đã được quy định trong mục 6.5.

Bức tường lửa này cần được định cấu hình cho phép thông qua một tập tối thiểu các chức năng. Chỉ các giao thức được nhận diện, như các giao thức cần thiết để hoàn thành chức năng của CA hoặc RA, cần được phép thông qua; các giao thức khác không được phép thông qua. Ví dụ điển hình, CA hoặc RA chỉ cần một giao thức thư điện tử (chẳng hạn là SMTP), một giao thức Web (chẳng hạn là HTTP) và/hoặc một giao thức truy nhập thư mục (chẳng hạn là LDAP). Tất cả các giao thức ứng dụng khác, chẳng hạn như TELNET hoặc FTP, không được phép thông qua bức tường lửa này.

Thêm vào đó, trạm làm việc cũng được định cấu hình chỉ cung cấp chức năng tối thiểu cho các dịch vụ của CA và RA. Tất cả các cổng truyền thông không quá cần thiết cần được vô hiệu hoá và đóng các chương trình phần mềm sử dụng các cổng này.

6.8 Các kiểm soát kỹ thuật mật mã

Các thiết bị mật mã do CA và RA sử dụng nên tương thích với mức 2 của FIPS 140-1. Mức 3 được lựa chọn nhiều hơn.

6.9 Đảm bảo an toàn máy tính

Xem mục 6.5 và 6.6.1.

6.10 Đảm bảo an toàn chu kỳ tồn tại

Chương trình thực hiện ứng dụng của CA cần được tổ chức (nắm giữ bản chương trình chính) ký số lên đó. Giá trị của chữ ký được cấp cho người sử dụng trong một phương tiện độc lập với ứng dụng.

Tại thời điểm cài đặt, tiến hành phê chuẩn phần mềm dựa vào giá trị của chữ ký biết trước. Nếu giá trị không đúng, không nên cài đặt phần mềm này. Tổ chức nắm giữ bản chương trình chính nên được thông báo tình trạng này.

Nên tiến hành kiểm tra đối với chương trình khi bắt đầu ứng dụng, hoặc kiểm tra định kỳ khi ứng dụng đang thực hiện, nhằm chống lại tình trạng sửa đổi trái phép. Cần tính toán giá trị băm hoặc giá trị của chữ ký (chỉ yêu cầu một giá trị băm; có thể thêm chữ ký nếu muốn) của phần mềm và so sánh với giá trị biết trước có trong phần mềm được phân phối. Nếu không trùng khớp, cần dừng ngay quá trình xử lý phần mềm và thông báo cho ISSO của trạm làm việc. Hàm băm được sử dụng trong quá trình phê chuẩn nên là một hàm băm được phê chuẩn, chẳng hạn như SHA-1. Không nên thực hiện ứng dụng quá 24 giờ mà không có kiểm tra.

Các kiểm soát đảm bảo chu kỳ tồn tại trong trạm làm việc mà RA sử dụng phụ thuộc vào tập đặc quyền của RA. Khi RA nạp chứng chỉ vào thẻ bài phần cứng, RA cần thỏa mãn các yêu cầu trên trạm làm việc của CAW. Nếu RA chỉ đơn giản là người kiểm tra/chuyển tiếp thông tin thì không có yêu cầu đảm bảo an toàn chu kỳ tồn tại nào trên trạm làm việc mà RA sử dụng.

7. CÁC KHÁI LƯỢC CỦA CHỨNG CHỈ VÀ CRL

Mục này trình bày các nguyên tắc trong việc sử dụng các trường và mở rộng của chứng chỉ X.509 và CRL.

7.1 Các Khái lược và phiên bản của chứng chỉ

CA nên phát hành các chứng chỉ X.509 phiên bản 3, phù hợp với khái lược chứng chỉ của IETF PKIX [HOU].

7.2 Tên đối tượng của chính sách

Tên đối tượng dành cho chính sách này là {...] để được cung

cấp]...}

7.3 Các tên đối tượng của thuật toán ký

Việc ký các chứng chỉ (được phát hành tuân theo chính sách này) nên sử dụng một trong các thuật toán sau đây:

- DSA với SHA-1 {iso (1) member-body (2) us (840) x9-57 (10040) x9algorithm (4) dsa-with-sha1 (3)}, như được định nghĩa trong ANSI X9.57; DSA được định nghĩa trong Chuẩn chữ ký số (DSS) - FIPS 186.
- RSA với SHA-1 {iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 29}, như được định nghĩa trong "Các thỏa thuận tại hội thảo khoa học của các nhà thực thi môi trường hệ thống mở NIST".

7.4 Sử dụng của các trường tên

CA và RA nên có một tên chính theo dạng Directory Name và nên sử dụng tên này trong trường thích hợp của chứng chỉ hoặc CRL (không phải là một trường mở rộng). Ngoài ra có thể sử dụng các tên lựa chọn khác cho trường "Các tên lựa chọn".

Nếu thực thể cuối có một Directory Name, thực thể cuối nên sử dụng tên này cho trường "Tên chủ thể của chứng chỉ". Không có quy định nào về việc sử dụng các trường mở rộng "Các tên lựa chọn".

7.5 Các ràng buộc tên và dạng tên dành cho các ràng buộc tên

CA phát hành chỉ quy định các Directory Name cho trường "Các ràng buộc đối với tên" của chứng chỉ.

7.6 Các trường mở rộng của chứng chỉ và tính thiết yếu của chúng

Tuỳ thuộc vào các điều khoản có trong khai lược IETF PKIX [HOU].

7.7 Sử dụng của các ràng buộc chính sách

Do CA phát hành tuỳ chọn.

7.8 Các qualifier của chính sách

Như được định nghĩa trong khai lược PKIX, các kiểu qualifier có thể được sử dụng với chính sách chứng chỉ này là:

- Con trỏ đến CPS
- Thông báo của người sử dụng

7.9 Xử lý ngữ nghĩa cho mở rộng chính sách chứng chỉ thiết yếu

Người sử dụng chứng chỉ (được phát hành với mở rộng "Chính sách của chứng chỉ" là thiết yếu và có chứa tên của chính sách chứng chỉ này) chấp thuận tất cả các thuật ngữ và điều kiện có trong định nghĩa chính sách chứng chỉ này. Ngoài ra, nếu qualifier kiểu *Con trỏ đến CPS* xuất hiện trong chứng chỉ này, thì người sử dụng chấp thuận tất cả các thuật ngữ và điều kiện có trong CPS này.

7.10 Số lượng phiên bản CRL

CA sẽ hỗ trợ CRL phiên bản 2 của X.509.

7.11 CRL, các mở rộng của CRL entry và tính thiết yếu của chúng

Tuỳ thuộc vào các điều khoản có trong khái lược IETF PKIX.

8. QUẢN LÝ ĐẶC TẢ

8.1 Các thủ tục thay đổi đặc tả

8.1.1 Các mục có thể thay đổi không cần thông báo

Các thay đổi có thể được tiến hành trên đặc tả mà không cần thông báo là hiệu chỉnh lỗi soạn thảo hoặc in ấn, hoặc thay đổi các chi tiết liên hệ.

8.1.2 Các thay đổi cần thông báo

8.1.2.1 (a) Danh sách các mục

1. Mọi mục trong chính sách chứng chỉ này có thể được thay đổi với 90 ngày thông báo.

2. Việc thay đổi các mục không làm ảnh hưởng chính đến đa số các thuê bao hoặc thành viên tin cậy sử dụng chính sách này, có thể được thực hiện với 30 ngày thông báo.

8.1.2.1 (b) Các cơ chế thông báo

Tất cả những thay đổi được đề xuất có thể ảnh hưởng chính đến người sử dụng chính sách chứng chỉ này, sẽ được thông báo bằng văn bản cho CA (đã đăng ký với tổ chức quản lý chính sách) và được công bố trên Web site của tổ chức này. CA nên công bố các thay đổi được đề xuất này trên kho lưu giữ của mình và tham khảo ý kiến của các thuê bao, bằng văn bản hoặc thư điện tử đối với các thay đổi được đề xuất đó.

8.1.2.2 Khoảng thời gian đưa ra kiến nghị

Những người bị ảnh hưởng có thể đệ trình kiến nghị của mình cho tổ chức quản lý chính sách như sau:

- Với các thay đổi phù hợp với (a) của 8.1.2.1, tổ chức cần nhận được kiến nghị trong 15 ngày kể từ ngày thông báo đầu tiên.
- Với các thay đổi phù hợp với (b) của 8.1.2.1, tổ chức cần nhận được kiến nghị trong 45 ngày kể từ ngày thông báo đầu tiên.

8.1.2.3 Các cơ chế giải quyết kiến nghị

Mọi hoạt động xảy ra như là kết quả của các kiến nghị được đưa ra phù hợp với 8.1.2.2 đều do tổ chức quản lý chính sách quyết định.

8.1.2.4 Khoảng thời gian dành cho thông báo thay đổi cuối cùng

Nếu thay đổi được thực hiện như là kết quả của các kiến nghị theo đúng 8.1.2.2 và 8.1.2.3, cần đưa ra thông báo về việc thực hiện chúng, phù hợp với 8.1.2.1, ít nhất 30 ngày trước khi thay đổi có hiệu lực.

8.1.3 Các mục thay đổi yêu cầu một chính sách mới

Nếu tổ chức quản lý chính sách quyết định thay đổi một chính sách có ảnh hưởng chính đến đa số những người sử dụng chính sách, tổ chức quản lý chính sách có thể gán một tên đối tượng mới cho chính sách được sửa đổi này.

8.2 Việc công bố và thông báo các chính sách

8.2.1 Các mục không được công bố trong CPS

Không nên áp dụng.

8.2.2 Việc phân phối định nghĩa chính sách chứng chỉ và CPS

Định nghĩa chính sách này sẽ được công bố:

- Bằng dạng điện tử trên Web site: <https://...>[được cung cấp];
- Bằng dạng điện tử qua thư điện tử với [địa chỉ để được cung cấp].

Một bản sao của chính sách chứng chỉ này sẽ được công bố trên Web site của tổ chức quản lý chính sách. CA phát hành chứng chỉ (có nhận diện chính sách chứng chỉ này) nên công bố các bản sao của chính sách chứng chỉ này trên các kho lưu giữ của mình.

8.3 Các thủ tục phê chuẩn CPS

Phù hợp với các thủ tục được tổ chức quản lý chính sách xác định.

PHẦN II

CHÍNH SÁCH CHỨNG CHỈ DÀNH CHO CÁC ỨNG DỤNG THIẾT LẬP KHOÁ MÃ

1. GIỚI THIỆU

1.1 Tổng quan

Chính sách chứng chỉ là một "tập hợp các quy tắc chỉ ra khả năng ứng dụng của một chứng chỉ vào một cộng đồng riêng và/hoặc lớp ứng dụng với các yêu cầu an toàn chung" [X.509]. Định nghĩa chính sách chứng chỉ được đăng ký và gán một "*tên đối tượng*" duy nhất, tên này nằm trong trường mở rộng chuẩn của chứng chỉ X.509. Bằng cách kiểm tra trường này, hệ thống sử dụng chứng chỉ có thể xác định được chứng chỉ có mục đích sử dụng phù hợp với một ứng dụng riêng hay không.

Các chính sách chứng chỉ có khả năng áp dụng khác nhau. Ví dụ, một chính sách chứng chỉ có thể được định nghĩa và sử dụng trong miền của một CA hoặc tổ chức đơn lẻ; trong trường hợp này, chính sách chứng chỉ không khác gì một CPS trong đó quy định các hoạt động mà CA tuân theo khi phát hành các chứng chỉ [ABA].

Tuy nhiên, chính sách chứng chỉ được định nghĩa trong tài liệu này có khả năng áp dụng rộng rãi, cho tất cả các bộ và cơ quan của chính phủ Canada, Liên bang Mỹ và các môi trường tiềm ẩn khác.

Chính sách chứng chỉ trong phần I dành cho các ứng dụng chữ ký số. Chính sách chứng chỉ trong phần II dành cho các ứng dụng thiết lập khoá mã, bao gồm các kỹ thuật thoả thuận khoá và chuyển khoá. Các chứng chỉ được phát hành tuân theo chính sách này có thể đảm bảo tính bí mật cho các truyền thông Web hoặc thư điện tử, cụ thể bảo vệ các thông tin nhạy cảm nhưng không được phân loại của Mỹ hoặc các thông tin được xác định trước của Canada.

Chính sách chứng chỉ này giống hệt với chính sách chứng chỉ được định nghĩa trong phần I của tài liệu này, ngoại trừ các mục

nhỏ sau đây, chúng được thay thế vào các mục tương ứng trong phần I.

1.2 Nhận dạng

Tên chính sách chứng chỉ: PKIPrivacyCertPcy:3.0-MediumAssurance

Tên đối tượng: {để được cung cấp}

1.3 Cộng đồng và khả năng áp dụng

1.3.1 Khả năng áp dụng

Dành cho các chứng chỉ khoá công khai được sử dụng cho thiết lập khoá mã, bao gồm các kỹ thuật thoả thuận khoá và chuyển khoá. Chính sách này được áp dụng cho CA và các đại lý của CA, RA và các đại lý của RA, các kho lưu giữ chứng chỉ và CRL mà CA và người điều hành của CA sử dụng, các thực thể cuối được CA chứng thực.

1.3.1.1 Các ứng dụng phù hợp

Các chứng chỉ được phát hành tuân theo chính sách này có thể đảm bảo tính bí mật cho các truyền thông Web hoặc thư điện tử. Chính sách chứng chỉ có thể được sử dụng với các giao thức ứng dụng khác nhau, chẳng hạn như S/MIME, giao thức truyền siêu văn bản an toàn (S-HTTP), giao thức an toàn thông báo (MSP) và giao thức truy nhập thư mục (DAP).

2. CÁC ĐIỀU KHOẢN CHUNG

2.1 Tính bí mật

CA và/hoặc RA có thể nắm giữ khoá riêng của các thực thể mà họ chứng thực hoặc hỗ trợ nếu CA hoặc RA điều hành dịch vụ uỷ nhiệm hoặc khôi phục/sao lưu dự phòng khoá riêng, đồng thời đảm bảo rằng thuê bao được thông báo trước về tình trạng này. Nếu CA và/hoặc RA nắm giữ các khoá riêng, chúng cần được bảo vệ phù hợp với các điều khoản an toàn kỹ thuật được trình bày trong mục 6 và không một thành viên nào khác được phép khám phá khoá riêng mà không có sự đồng ý trước của thuê bao, hoặc yêu cầu của luật pháp.

Nói chung, không nên để lộ các nhật ký kiểm toán, chỉ có thể để lộ các bản ghi giao dịch cá nhân, mặc dù thực thể có thể được phép xem xét tất cả các bản ghi hoạt động mà thực thể đã tham gia.

Thông tin nhận dạng, hoặc các thông tin khác về cá nhân hoặc tổ chức có trong chứng chỉ không được coi là bí mật, trừ khi có sự quy định các luật hoặc các thoả thuận đặc biệt. Các thông tin khác về cá nhân hoặc tổ chức mà CA hoặc RA nắm giữ được coi là bí mật và không nên để lộ nếu không có sự đồng ý trước của thuê bao, trừ khi luật pháp yêu cầu.

3. NHẬN DẠNG VÀ XÁC THỰC

3.1 Đăng ký ban đầu

3.1.1 Phương pháp chứng minh quyền sở hữu đối với khoá riêng

Quá trình đăng ký nên bao gồm một giai đoạn trong đó ứng dụng chứng minh quyền sở hữu đối với khoá riêng, ví dụ, bằng cách tạo ra một thông báo được mã hoá bằng khoá riêng này.

4. CÁC YÊU CẦU HOẠT ĐỘNG

Không có gì thay đổi so với Phần I.

5. CÁC KIỂM SOÁT AN TOÀN CÁ NHÂN, VẬT LÝ VÀ THỦ TỤC

Không có gì thay đổi so với Phần I.

6. CÁC KIỂM SOÁT AN TOÀN KỸ THUẬT

6.1 Sinh và cài đặt cặp khoá

6.1.1 Sinh cặp khoá

Thuê bao có thể tạo ra một cặp khoá cho riêng mình, hoặc cặp khoá có thể do các thực thể khác tạo ra, như CA, RA hoặc thành viên thứ ba tin cậy khác.

6.1.2 Chuyển giao khoá riêng cho thực thể

Nếu cặp khoá do một thực thể khác tạo ra (không phải là thuê bao), thì khoá riêng cần được chuyển giao:

1. Trong một thẻ bài phần cứng, thông qua quá trình chuyển giao thẻ bài an toàn, trong đó có một thủ tục thích hợp cho việc xác thực người nhận thẻ bài; hoặc

2. Thông qua một giao dịch trực tuyến, trong đó khoá riêng được bảo vệ nhờ vào một *khoá mã sử dụng 1 lần*.

6.1.3 Kích thước khoá

Kích thước khoá nên tối thiểu là 1024 bit lấy theo modulo p cho KEA, hoặc 1024 bit cho RSA hoặc Diffie-Hellman.

6.1.4 Sinh các tham số khoá công khai

Với KEA hoặc Diffie-Hellman, các tham số nên được một cơ quan trung tâm tạo ra và cung cấp.

6.1.5 Các mục đích sử dụng khoá (Như X.509 phiên bản 3)

Các khoá có thể được sử dụng cho mã hoá khoá hoặc thoả thuận khoá.

6.2 Bảo vệ khoá riêng

6.2.1 Uỷ nhiệm khoá riêng

Trong miền của một CA cụ thể, các khoá riêng có thể được uỷ nhiệm, với điều kiện chính sách uỷ nhiệm được xác định đầy đủ trong CPS và đảm bảo từng thuê bao được thông báo về chính sách này tại thời điểm hoặc trước khi phát hành chứng chỉ.

6.2.2 Sao lưu dự phòng khoá riêng

Trong miền của một CA cụ thể, các khoá riêng có thể được sao lưu dự phòng, với điều kiện chính sách dự phòng được xác định đầy đủ trong CPS và đảm bảo từng thuê bao được thông báo về chính sách này tại thời điểm hoặc trước khi phát hành chứng chỉ.

6.2.3 Lưu trữ khoá riêng

Trong miền của một CA cụ thể, các khoá riêng có thể được lưu trữ, với điều kiện chính sách lưu trữ được xác định đầy đủ trong CPS và đảm bảo từng thuê bao được thông báo về chính sách này tại thời điểm hoặc trước khi phát hành chứng chỉ.

6.2.4 Khoá riêng được sử dụng trong mô đun mật mã

Không quy định.

6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá

6.3.1 Lưu trữ khoá công khai

Không yêu cầu CA lưu trữ các khoá công khai.

6.3.2 Khoảng thời gian sử dụng của khoá công khai và khoá riêng

Với các CA, mọi khóa riêng được sử dụng cho mục đích ký chứng chỉ có khoảng thời gian sử dụng không quá 2 năm, chứng chỉ được phát hành cho khoá công khai có khoảng thời gian tồn tại hợp lệ không quá 10 năm.

Với các RA, một khóa riêng được sử dụng cho mục đích ký có khoảng thời gian sử dụng tối 5 năm, hoặc ngắn hơn nếu được xác định rõ trong chứng chỉ, chứng chỉ được phát hành cho khoá công khai có khoảng thời gian tồn tại hợp lệ không quá 10 năm.

Với các thực thể cuối, khoá công khai được chứng thực có khoảng thời gian sử dụng không quá 5 năm; ở đây không có giới hạn nào đối với khoảng thời gian sử dụng của một khóa riêng.

7. CÁC KHÁI LƯỢC CỦA CHỨNG CHỈ VÀ CRL

7.2 Tên đối tượng của chính sách

Tên đối tượng dành cho chính sách này là {...[để được cung cấp]...}

8. QUẢN LÝ ĐẶC TẢ

Không có gì thay đổi so với phần I.

TÀI LIỆU THAM KHẢO CỦA ĐỊNH NGHĨA CHÍNH SÁCH NÀY

[ABA] American Bar Association, Section of Science & Technology, *Digital Signature Guidelines* (1996).

[FIPS] U.S Department of Commerce, *Security Requirements for Cryptography Modules*, Federal Information Processing Standards Publication FIPS PUB 140-1, 1994.

[CHO] S. Chokhani and W.Ford, "Certificate Policy and Certification Practice Statement Framework", Internet Draft <draft-ietf-pkix-ipki-part 4- 00.txt>.

[HOU] R.Housley, W.Ford, T.Polk, D.Solo, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, Internet Draft: draft-ietf-pkix-ipki-part 1- 04.txt, 03/26/1997.

[TCSEC] U.S. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, National Computer Security Center, Fort Meade, MD, December 1985.

[TSDM] U.S. Department of Defense, "*Trusted Software Methodology*", Volume 1, SDI-S-SD-91-000007, Department of Defense, Strategic Defense Initiative Organization, 17 June 1992.

[X.509] ISO/IEC 9594-8, *Information Technology Open System Interconnection The Directory: Authentication Framework*. ITU-T X.509 Recommendation.

CÁC TỪ VIẾT TẮT

ACL	Access Control List - Danh sách kiểm soát truy nhập
ASN.1	Abstract Syntax Notation One Bảng cú pháp trừu tượng số 1
ANSI	Ameriacan National Standards Institute - Viện chuẩn Quốc gia Mỹ
CA	Certificate authority - Cơ quan chứng thực
CERT	Computer Emergency Response Team - Nhóm phản ứng khẩn cấp các sự cố về máy tính
CGI	Common Gateway Interface - Giao diện cửa chung
CKL	Compromised Key List - Danh sách khoá bị lộ
CPS	Certification Practice Statement - Quy định hoạt động chứng thực
DARPA	Defense Advanced Research Projects Agency
DCE	Distributed Computing Environment - Môi trường tính toán phân tán
DES	Data Encryption Standard - Chuẩn mã hoá dữ liệu
DSS	Digital Signature Standard - Chuẩn chữ ký số
DIT	Directory Information Tree - Cây thông tin thư mục
DMS	Defence Messaging System - Hệ thống gửi tin của Bộ Quốc phòng
DN	Distinguished Name - Tên phân biệt
DNS	Domain Name Server - Máy chủ tên miền
DSA	Digital Signature Algorithm - Thuật toán chữ ký số
ECMA	European Computer Manufacturers Association - Hội những nhà sản xuất máy tính châu Âu

EDI	Electronic Data Interchange - Trao đổi dữ liệu điện tử
EFT	Electronic Funds Transfer - Chuyển tiền điện tử
FTP	File Transfer Protocol - Giao thức truyền tệp
GUI	Graphical User Interface - Giao diện đồ hoạ người dùng
HTML	Hypertext Markup Language - Ngôn ngữ đánh dấu siêu văn bản
HTTP	Hypertext Transfer Protocol - Giao thức truyền siêu văn bản
ITU	International Telecommunication Union - Liên minh viễn thông Quốc tế
IOS	International Organization for Standardization - Tổ chức tiêu chuẩn hoá Quốc tế
IPRA	Internet Policy Registration Authority - Cơ quan đăng ký chính sách Internet
ISP	Internet Service Provider - Nhà cung cấp dịch vụ Internet
KDC	Key Distribution Center – Trung tâm phân phối khoá
LRA	Local Registration Authority - Cơ quan đăng ký địa phương
LDAP	Lightweight Directory Access Protocol - Giao thức truy nhập thư mục
MISSI	Multi-level Information System Security Initiative - Khởi sinh an toàn hệ thống thông tin đa mức
MIT	Massachusetts Institute of Technology - Viện công nghệ Massachusetts
NDS	Netware Directory Service - Dịch vụ thư mục Netware
NAP	Network Access Point - Điểm truy nhập mạng
NIST	National Institute of Standards and Technology - Viện chuẩn và công nghệ Quốc gia
NSA	National Security Agency - Cơ quan an toàn Quốc

	gia
NSF	National Science Foundation – Tổ chức khoa học Quốc gia
ORA	Organization Registration Authority - Cơ quan đăng ký của tổ chức
OSF	Open Software Foundation - Tổ chức phần mềm mở
OSI	Open Systems Interconnection - Kết nối các hệ thống mở
PAA	Policy Approving Authority - Cơ quan phê chuẩn chính sách
PAC	Privilege Attribute Certificate - Chứng chỉ thuộc tính đặc quyền
PCA	Policy Certification Authority - Cơ quan chứng thực chính sách
PAserver	Privilege Attribute server - Máy chủ thuộc tính đặc quyền
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number - Số hiệu nhận dạng cá nhân
PKIX	Public Key Infrastructure (X.509) - Cơ sở hạ tầng khoá công khai (X.509)
RDN	Relative Distinguished Name - Tên phân biệt liên quan
SET	Secure Electronic Transaction - Giao dịch điện tử an toàn
SDSI	Simple Distributed Security Infrastructure - Cơ sở hạ tầng an toàn được phân tán đơn giản
SGML	Standard Generalized Markup Language - Ngôn ngữ đánh dấu tổng quát chuẩn
SHA	Secure Hash Algorithm - Thuật toán băm an toàn
S-HTTP	Secure Hypertext Transfer Protocol - Giao thức truyền siêu văn bản an toàn

SNMPv3	Simple Network Management Protocol Version 3 - Giao thức quản lý mạng đơn giản phiên bản 3
SPKI	Simple Public-Key Infrastructure - Cơ sở hạ tầng khoá công khai đơn giản
SSI	Server Side Include
SSL	Secure Socket Layer - Tầng Socket an toàn
URL	Uniform Resource Locator - Bộ định vị tài nguyên
VAN	Value Added Network - Mạng giá trị gia tăng
WIPO	World Intellectual Property Organization - Tổ chức sở hữu trí tuệ thế giới

MỘT SỐ KHÁI NIỆM

A

ACL (Danh sách kiểm soát truy nhập) - Danh sách hoặc cơ sở dữ liệu liên kết với một đối tượng để nhận dạng tất cả các chủ thể có thể truy nhập đối tượng và các quyền truy nhập của chúng.

Active content(Nội dung động) - Là 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 bằng tính dựa vào Web.

Applet - Tên một chương trình được thực hiện trong chương trình khác, nó không thể thực hiện trực tiếp trên một máy tính.

Asymmetric Encryption (Mã hoá phi đối xứng) - Đồng nghĩa với mã hoá khoá công khai.

B

Browser (Trình duyệt) - Đồng nghĩa với Web browser, đây là một phần mềm giúp người sử dụng đọc được các tài liệu HTML và dịch chuyển từ một tài liệu HTML này sang tài liệu HTML khác.

Buffer (Bộ đệm) - Một vùng nhớ trong máy tính, được sử dụng để lưu giữ tạm thời các dữ liệu được đọc vào/ra từ một tệp hoặc một cơ sở dữ liệu.

C

Cache - Vùng nhớ tốc độ cao, được sử dụng để lưu giữ các trang Web.

Catalog - Trên các site thương mại điện tử, đây là một danh sách các loại hàng hoá và dịch vụ (có thể chứa ảnh và mô tả), thường được lưu giữ trong một cơ sở dữ liệu.

Certification Authority (Cơ quan chứng thực) - Đây là một cơ quan phát hành chứng chỉ số cho các tổ chức hoặc các cá nhân.

Cipher text (Bản mã) - Văn bản khó hiểu, được tạo ra sau khi đi qua hệ thống mật mã.

Clear text (Bản rõ) - Văn bản hoặc thông tin chưa được mã hoá.

Commodity (Hàng hoá) - Một sản phẩm hoặc dịch vụ được chuẩn hoá và nhiều người biết đến.

Common Gateway Interface (Giao diện của chung) - Giao thức mô tả phương pháp chuẩn truyền thông chung giữa một máy chủ Web và một trình ứng dụng ngoại trú, cho phép các máy chủ Web tương tác dễ dàng với các gói phần mềm khác để tạo ra các trang Web cho khách hàng.

Cookies - Các bit thông tin về người truy cập Web site, chúng được các Web site tạo ra và lưu giữ trên các máy khách.

D

DES - Chuẩn mã hoá dữ liệu được chính phủ Mỹ thông qua, sử dụng khi mã hoá các thông tin nhạy cảm.

Digital Certificate (Chứng chỉ số) - Được gắn kèm với thông báo thư điện tử hoặc dữ liệu được nhúng vào một trang Web. Người ta sử dụng nó để kiểm tra nhận dạng của người gửi hoặc Web site.

Digital Signature (Chữ ký số) - Khối dữ liệu được gắn kèm với một thông báo, cho phép bên nhận có thể xác nhận nội dung thông báo và/hoặc chứng minh rằng nó chỉ có thể có nguồn gốc từ bên gửi hợp pháp. Chữ ký số là kết quả thu được sau khi mã hoá tóm lược thông báo.

E

EDI (Trao đổi dữ liệu điện tử) - Truyền dữ liệu từ máy tính này sang máy tính khác theo một khuôn dạng chuẩn.

F

FTP (Giao thức truyền tệp) - Giao thức cho phép người sử dụng truyền các tệp qua Internet.

G

Gateway server firewall (Bức tường lửa máy chủ cổng nối)

- Lọc các luồng thông tin, tùy thuộc vào các ứng dụng mà các máy khách (trên mạng tin cậy) yêu cầu.

GUI (Giao diện đồ hoạ người dùng) - Là một cách đưa ra các hàm điều khiển chương trình và cung cấp cho người dùng.

H

Hash algorithm (Thuật toán băm) - Một tiện ích an toàn kết hợp tất cả các ký tự có trong một thông báo để tạo ra một số có độ dài cố định (thông thường độ dài là 128 bit) và được gọi là dấu vân tay của thông báo.

Hash value (Giá trị băm) - Giá trị thu được sau khi áp dụng hàm băm lên một thông báo.

HTML (Ngôn ngữ đánh dấu siêu văn bản) - Ngôn ngữ đánh dấu siêu văn bản của Internet. Nó chứa các mã được gán cho văn bản.

HTTP (Giao thức truyền siêu văn bản) - Một giao thức của Internet. Nó có trách nhiệm trong việc truyền và hiển thị các trang Web.

Hypertext Link (Liên kết siêu văn bản) - Con trỏ trong tài liệu HTML, trỏ đến các vị trí khác nhau trong cùng một tài liệu, hoặc trỏ đến một tài liệu HTML khác.

I

Integrity (Tính toàn vẹn) - Một loại an toàn máy tính chống lại các thao tác không được phép do chủ ý hoặc vô ý, đồng thời bảo đảm duy trì hiệu lực của dữ liệu để chắc chắn rằng dữ liệu không bị sửa đổi.

ISP (Nhà cung cấp dịch vụ Internet) - Các công ty bán quyền truy nhập Internet trực tiếp cho những người sử dụng Internet.

K

Key (Khoá) - Đây là một số (thường là số nhị phân dài), được sử dụng với thuật toán mã hoá để "giữ bí mật" các ký tự của một thông báo, vì vậy không thể giải mã được chúng nếu không có khoá.

M

Mail bomb (Bom thư) - Một kiểu tấn công trên hệ thống mạng

máy tính, nó xảy ra khi có nhiều người (hàng trăm hay hàng ngàn người) đều gửi thông báo tới một địa chỉ cụ thể, vượt quá giới hạn thư tín được phép của người nhận và làm cho các hệ thống thư tín bị trục trặc.

Mail Server (Máy chủ thư tín) - Tập phần mềm và phần cứng, được sử dụng để quản lý và lưu giữ thư điện tử qua Internet.

Mailing list - Danh sách địa chỉ thư điện tử chuyển tiếp các thông báo cho người nhận (các thuê bao).

Masquerading - Một loại tấn công giả danh một người, một Web site hay một đối tượng nào đó.

N

Necessity (Tình sẵn sàng) - Một loại an toàn máy tính chống các hiểm họa làm trễ hoặc chối bỏ dữ liệu.

P

Packet filter firewall (Bức tường lửa lọc gói) - Biện pháp lọc gói, kiểm tra tất cả các luồng dữ liệu vào ra giữa một mạng tin cậy cục bộ và Internet.

PEM: Tên của tập các chuẩn cho Internet được đề xuất năm 1993, do tổ công tác kỹ thuật Internet (IETF) nghiên cứu nhằm mục đích đảm bảo an toàn thư trên Internet.

PGP: Tên sản phẩm phần mềm bảo vệ thông báo gửi trên mạng.

Privacy (Tính riêng tư) - Quyền của một cá nhân, một kiểu kiểm soát nào đó đối với những thông tin của cá nhân đó. Hay quyền của một cá nhân về mức độ muốn chia sẻ thông tin của chính mình với các cá nhân khác.

Private key (Khoá riêng) - Khoá được sử dụng để mã hoá và giải mã thông báo.

Private Key Encryption (Mã hoá khoá riêng) - Quá trình mã hoá và giải mã thông báo sử dụng cùng một khoá, yêu cầu cả bên gửi lẫn bên nhận thông báo phải biết khoá và giữ bí mật khoá này.

Proxy server firewall (Bức tường lửa máy chủ uỷ quyền) - Thay mặt cho mạng tin cậy, truyền thông với Internet.

Public key (Khóa công khai) - Đây là một khoá trong một cặp khoá, được sử dụng để mã hoá các thông báo và được phân phối công khai.

Public Key Encryption (Mã hoá khoá công khai) - Quá trình mã hoá và giải mã các thông báo sử dụng một cặp khoá. Một khoá được sử dụng để mã hoá, khoá còn lại để giải mã, khoá này được giữ kín.

Pull (Kỹ thuật kéo) - Kỹ thuật được sử dụng khi một cá nhân tìm kiếm thông tin trên Web, bằng cách sử dụng liên kết siêu văn bản.

Push (Kỹ thuật đẩy) - Kỹ thuật chuyển giao tự động các thông tin xác định từ một máy chủ Web tới một máy tính của người sử dụng.

R

Router (Bộ định tuyến) - Một máy tính xác định đường dẫn cho các luồng thông tin trong mạng. Nó quyết định đường đi tốt nhất cho các gói dữ liệu khi đi đến đích.

S

Save area (Vùng lưu) - Nơi các chương trình lưu giữ thông tin thiết yếu trước khi việc kiểm soát các thông tin này được chuyển cho các chương trình khác.

Secrecy (Tính bí mật) - Một loại an toàn máy tính, bảo vệ dữ liệu không bị lộ trước những đối tượng trái phép.

Secure envelope (Phong bì an toàn) - Một tiện ích an toàn đóng gói một thông báo và đảm bảo tính bí mật, toàn vẹn và xác thực máy khách/chủ.

Security policy (Chính sách an toàn) - Tập hợp các quy tắc, các luật và các thủ tục quy định cách thức tổ chức, bảo vệ và phân bố các tài sản của một tổ chức. Trong đó có thể mô tả các tài sản cần được bảo vệ, lý do tại sao phải bảo vệ chúng, trách nhiệm của các thành viên trong việc bảo vệ, những hoạt động được chấp nhận

và không được chấp nhận.

Session key (Khoá phiên) - Khoá được sử dụng trong một thuật toán mã hoá để tạo ra bản mã từ bản rõ trong một phiên giao dịch an toàn.

Shopping cart - Một trình tiện ích thương mại điện tử, nó lưu giữ vết các danh mục được chọn mua và tự động hoá quá trình mua.

Sniffer - Một chương trình móc nối vào Internet và ghi lại các thông tin đi qua một bộ định tuyến, trên đường đi từ nguồn tới đích.

Spoofing - Một kiểu tấn công, đồng nghĩa với **Masquerading**.

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 tệp mật khẩu, hoặc gửi ngược trở lại một vị trí đặc biệt.

SSL (Tầng Socket an toàn)- Một giao thức được sử dụng để truyền các thông tin riêng tư qua Internet một cách an toàn.

Steganography (Ngụy trang ký) - Sự che dấu thông tin (chẳng hạn như các lệnh) bằng cách đặt nó trong một đoạn thông tin khác.

Symmetric encryption (Mã hoá đối xứng) - Đồng nghĩa với mã hoá khoá riêng.

Symmetric key (Khoá đối xứng) - Đồng nghĩa với khoá riêng.

T

Trojan horse (Con ngựa thành Troia) - Một chương trình ẩn bên trong chương trình khác hoặc trang Web, che dấu mục đích thực sự của nó (thông thường là phá hoại).

U

URL (Bộ định vị tài nguyên)- Biểu diễn địa chỉ IP của một trang Web, giao thức được sử dụng để truy nhập vào trang và vị

trí của trang.

V

VAN (Mạng giá trị gia tăng) - Đây là một công ty độc lập, nó cung cấp kết nối và các dịch vụ giao dịch EDI cho các nhà kinh doanh.

Virtual community (Cộng đồng ảo) - Tập hợp một nhóm người có thể chia sẻ các mối quan tâm chung trên Internet.

W

Web client (Máy khách Web) - Máy tính được kết nối với Internet, người ta sử dụng nó để tải xuống các trang Web.

Web server (Máy chủ Web) - Máy tính được kết nối với Internet, lưu giữ các tệp dưới dạng HTML, chúng có hiệu lực công khai trong suốt một kết nối Internet.

TÀI LIỆU THAM KHẢO

1. G.P.SCHNEISER and J.T.Perry, "Electronic Commerce", Course Technology, 2000.
2. J.R.Vacca, "Internet Security Secrets", IDG books Worldwide, Inc., 1996.
3. W-Ford, "Computer Communications Security: Principles, Standard Protocols and Techniques", Prentice Hall, Inc., 1994.
4. D.Stinson, "Cryptography: Theory and Practice", CRC Press, 1995.
5. B.Schneider, "Applied Cryptography", 2nd edition, Wiley, 1995.
6. Davies and Price, "Security for Computer Networks".
7. U.S.Department of Commerce, "Digital Signature Standard (DSS)", Federal Information Processing Standards Publication FIPS PUB 186, 1994.
8. American National Standard Institute, ANSI X9.57, Certificate Management, 1997.
9. ISO/IEC 9594, Information Technology- Open Systems Interconnection- The Directory.
10. ISO/IEC 9594-8, Information - Technology- Open Systems Interconnection- The Directory: Authentication Framework.
11. ISO/IEC 9594-8, Information - Technology - Open Systems Interconnection- ASN.1: Specification of Basic Notation.
12. ISO/IEC 9834-1, Information- Technology- Open Systems Interconnection- Procedures for the operation of OSI Registration Authorities: General procedures.
13. ANSI X9.55, 1997
14. ISO/IEC 8824.
15. ISO/IEC 9594-8.
16. S.Kent, "Internet Privacy Enhanced Mail", Communications of the ACM, vol.36, No.8, 1993.
17. S.Kent, "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate- Based Key Management", RFC 1422, Internet activities Board, 1993.
18. Visa International, Mastercard International, Secure Electronic Transaction S

MỤC LỤC

Chương I: Các hiểm hoạ đối với an toàn thương mại điện tử.....	4
1.1 Thương mại điện tử là gì ?.....	4
1.2 Các hiểm hoạ đối với an toàn thương mại điện tử.....	12
1.2.2 Các hiểm hoạ đối với sở hữu trí tuệ.....	16
1.2.3 Các hiểm hoạ đối với thương mại điện tử.....	17
1.2.4 CERT.....	32
1.3 Tóm tắt.....	32
Chương II: Những mục tiêu của an toàn thương mại điện tử..	35
2.1 Giới thiệu.....	35
2.2 Bảo vệ các tài sản thương mại điện tử.....	35
2.3 Bảo vệ sở hữu trí tuệ.....	37
2.4 Bảo vệ các máy khách.....	38
2.5 Bảo vệ các kênh thương mại điện tử.....	45
2.6 Đảm bảo tính toàn vẹn giao dịch.....	56
2.7 Bảo vệ máy chủ thương mại.....	59
2.8 Tóm tắt.....	63
Chương III: Một số kỹ thuật an toàn cho thương mại điện tử.....	65
3.1 Mã hoá đối xứng.....	65
3.2 Mã hoá khoá công khai.....	67
3.2.1 Các nguyên lý của các hệ mật khoá công khai.....	67
3.2.2 Quản lý khoá.....	75
3.3 Xác thực thông báo và các hàm băm.....	84
3.3.1 Các yêu cầu xác thực.....	84

3.3.2 Các hàm xác thực.....	85
3.4 Chữ ký số.....	95
2.4.1 Các yêu cầu	95
3.4.2 Chuẩn chữ ký số.....	99
3.5 Tóm tắt	103
Chương IV: Chứng chỉ điện tử.....	105
4.1 Giới thiệu về các chứng chỉ khoá công khai	105
4.1.1 Đường dẫn chứng thực.....	108
4.1.2 Thời hạn hợp lệ và việc thu hồi	110
4.1.3. Các mối quan hệ mang tính pháp lý	110
4.2 Quản lý cặp khoá công khai và khoá riêng	111
4.2.1 Quá trình sinh cặp khoá.....	112
4.2.2 Bảo vệ khoá riêng	113
4.2.3 Cập nhật cặp khoá	113
4.3 Phát hành các chứng chỉ.....	116
4.3.1 Xin cấp một chứng chỉ	116
4.3.2 Quá trình tạo chứng chỉ.....	117
4.3.3 Xác thực chủ thể	117
4.3.4 Cơ quan đăng ký địa phương.....	118
4.3.5 Cập nhật chứng chỉ.....	119
4.4 Phân phối chứng chỉ	120
4.4.1 Chứng chỉ kèm theo chữ ký.....	120
4.4.2 Phân phối thông qua dịch vụ thư mục.....	120
4.4.3 Các giải pháp phân phối khác	122
4.5 Khuôn dạng chứng chỉ X.509.....	122
4.5.1 Khuôn dạng chứng chỉ cơ bản	122
4.5.2 Tên trong X.509	124

4.5.3 Đăng ký đối tượng.....	126
4.5.4 Khuôn dạng chứng chỉ X.509 mở rộng (v.3).....	129
4.5.5 Đặt tên trong phiên bản 3 của X.509.....	132
4.5.6 Các trường mở rộng chuẩn của chứng chỉ.....	134
4.5.7 Ký hiệu và mã của ASN.1.....	138
4.6 Việc thu hồi chứng chỉ.....	138
4.6.1 Yêu cầu thu hồi.....	138
4.6.2 Danh sách các chứng chỉ bị thu hồi (CRL).....	139
4.6.3 Việc quảng bá các CRL.....	141
4.6.4 Sự thu hồi ngay lập tức.....	142
4.6.5 Dòng thời gian xử lý thu hồi.....	144
4.7 CRL theo X.509.....	146
4.7.1 Khuôn dạng CRL.....	147
4.7.2 Các trường mở rộng chung.....	149
4.7.3 Các điểm phân tán CRL.....	150
4.7.4 Các Delta-CRL.....	152
4.7.5 Các CRL gián tiếp.....	152
4.7.6 Treo chứng chỉ.....	153
4.8 Cập khoá và thời hạn hợp lệ của chứng chỉ.....	154
4.8.1 Các cặp khoá liên quan đến mã hoá.....	155
4.8.2 Các cặp khoá dùng cho ký số.....	155
4.8.3 Cập khoá dùng cho mục đích ký của CA.....	157
4.9 Chứng thực thông tin uỷ quyền.....	157
4.9.1 Thông tin uỷ quyền trong các chứng chỉ X.509.....	158
4.9.2 Các chứng chỉ thuộc tính.....	159
4.9.3 Các chứng chỉ thuộc tính đặc quyền.....	160
4.9.4 Cơ sở hạ tầng an toàn được phân tán đơn giản.....	162

4.9.5 Cơ sở hạ tầng khoá công khai đơn giản	163
4.10 Tóm tắt	164
Chương V: Cơ sở hạ tầng khoá công khai.....	166
5.1 Các yêu cầu	166
5.2 Các cấu trúc quan hệ của CA	168
5.2.1 Cấu trúc phân cấp tổng quát.....	168
5.2.2 Cấu trúc phân cấp với liên kết bổ sung.....	171
5.2.3 Cấu trúc phân cấp trên - xuống	172
5.2.4 Cơ sở hạ tầng PEM	173
5.2.5 Các cây phân cấp	176
5.2.6 Mô hình chứng thực của PGP.....	177
5.2.7 Mô hình tin cậy ràng buộc tăng dần	179
5.2.8 Chứng chỉ được ký chồng chéo nhiều lần.....	183
5.3 Các chính sách của chứng chỉ X.509	184
5.3.1 Khái niệm chính sách chứng chỉ	184
5.3.2 Mở rộng Các chính sách chứng chỉ (Certificate Policies).....	186
5.3.3 Trường mở rộng Ánh xạ chính sách (Policy Mapping)	188
5.3.4 Mở rộng Các ràng buộc chính sách (Policy Constraints).....	189
5.3.5 Các nội dung của một chính sách chứng chỉ.....	190
5.4 Các ràng buộc tên X.509	191
5.5 Tìm các đường dẫn chứng thực và phê chuẩn.....	193
5.5.1 Tìm đường dẫn chứng thực.....	193
5.5.2 Phê chuẩn đường dẫn chứng thực.....	196
5.6 Các giao thức quản lý chứng chỉ.....	197
5.7 Ban hành luật	197
5.7.1 Công nghệ.....	198
5.7.2 Phạm vi và chi tiết.....	199

5.7.3 Các văn bản và chữ ký.....	199
5.7.4 Chất lượng và các chuẩn của CA.....	200
5.7.5 Các chuẩn về thuê bao.....	201
5.7.6 Chia nhỏ trách nhiệm pháp lý.....	201
5.8 Hai mô hình PKI.....	202
5.8.1 Cơ sở hạ tầng SET.....	202
5.8.2 Cơ sở hạ tầng DoD MISSI.....	206
Chương VI: Quy định Hoạt động chứng thực.....	210
6.1 Khái niệm.....	210
6.2 Biểu diễn một CPS.....	212
6.3 Nền tảng cho các hoạt động chứng thực.....	214
6.4 Các thủ tục xin cấp chứng chỉ.....	223
6.5 Phát hành chứng chỉ.....	226
6.6 Chấp nhận chứng chỉ.....	227
6.7 Sử dụng chứng chỉ để kiểm tra chữ ký số.....	228
6.8 Việc treo và huỷ bỏ chứng chỉ.....	230
6.9 Sự đảm bảo và giới hạn trách nhiệm pháp lý.....	231
6.10 Các điều khoản linh tinh.....	233
6.11 Sự tiến triển không ngừng.....	234
6.12 Tóm tắt.....	236
Chương VII: Luật chữ ký điện tử.....	240
7.1 Luật mẫu về Chữ ký điện tử của UNCITRAL.....	240
7.2 Chữ ký số.....	246
Phụ lục: Định nghĩa chính sách chứng chỉ CANADA.....	253
Lời nói đầu.....	253
Định nghĩa.....	254
Danh sách các từ viết tắt.....	254

Phần I: Chính sách chứng chỉ dành cho các ứng dụng chữ ký số ...256

1	Giới thiệu.....	256
1.1	Tổng quan	256
1.2	Nhận dạng.....	256
1.3	Cộng đồng và khả năng áp dụng.....	257
1.3.1	Các cơ quan chứng thực	257
1.3.2	Các cơ quan đăng ký	257
1.4	Các chi tiết liên hệ	259
1.4.2	Người liên hệ	259
1.4.3	Người quyết định khả năng phù hợp của CPS với chính sách	259
2.	Các Điều khoản chung.....	259
2.1	Trách nhiệm pháp lý.....	259
2.2	Các nghĩa vụ	261
2.3	Trách nhiệm tài chính	263
2.4	Việc Làm sáng tỏ và sự bắt buộc tuân theo	263
2.5	Lệ phí.....	264
2.6	Công bố và kho lưu giữ	264
2.7	Kiểm toán theo yêu cầu	265
2.8	Tính bí mật.....	266
2.9	Quyền sở hữu trí tuệ.....	266
3.	Nhận dạng và xác thực	266
3.1	Đăng ký ban đầu.....	266
3.1.2	Yêu cầu đặt tên có nghĩa	266
3.1.3	Các nguyên tắc trong việc làm sáng tỏ các dạng tên.	267
3.1.4	Tính duy nhất của các tên	267
3.1.5	Các thủ tục giải quyết tranh chấp yêu cầu tên.....	267

3.1.6 Sự công nhận, xác thực và vai trò của nhãn hiệu đăng ký trong I&A.....	267
3.1.7 Phương pháp chứng minh quyền sở hữu đối với khoá riêng.....	267
3.1.8 Xác thực định danh của tổ chức	267
3.1.9 Xác thực định danh của cá nhân.....	267
3.2 Thay thế khoá định kỳ.....	268
3.3 Thay thế khoá sau khi huỷ bỏ.....	268
3.4 Yêu cầu huỷ bỏ.....	268
4. Các yêu cầu hoạt động	268
4.1 Xin cấp chứng chỉ.....	269
4.2 Phát hành chứng chỉ.....	269
4.3 Chấp nhận chứng chỉ.....	269
4.4 Treo và huỷ bỏ các chứng chỉ	269
4.5 Các thủ tục kiểm toán an toàn.....	270
4.6 Lưu trữ các bản ghi.....	271
4.7 Thay đổi khoá.....	272
4.8 Tình trạng lộ và khôi phục sau thảm hoạ.....	272
4.9 Kết thúc hoạt động của CA.....	272
5. các kiểm soát an toàn cá nhân, vật lý và thủ tục	272
5.1 Các kiểm soát an toàn vật lý	272
5.1.1 Các kiểm soát an toàn vật lý dành cho CA.....	272
5.1.2 Các kiểm soát an toàn vật lý dành cho RA.....	273
5.1.3 Các kiểm soát an toàn vật lý dành cho thực thể cuối.....	274
5.2 Các kiểm soát thủ tục.....	274
5.2.1 Các tập đặc quyền tin cậy.....	274
5.2.2 Số lượng người yêu cầu/ nhiệm vụ	276

5.2.3 Việc xác thực và nhận dạng cho từng tập đặc quyền	276
5.3 Các kiểm soát an toàn cá nhân	276
5.3.1 Các kiểm soát an toàn cá nhân dành cho CA	276
5.3.2 Các kiểm soát an toàn cá nhân dành cho RA	277
5.3.3 Các kiểm soát an toàn cá nhân dành cho thực thể cuối	277
6. Các kiểm soát an toàn kỹ thuật	277
6.1 Sinh và cài đặt cặp khoá	277
6.1.1 Sinh cặp khoá	277
6.1.2 Chuyển giao khoá riêng cho thực thể	278
6.1.3 Chuyển giao khoá công khai cho người phát hành chứng chỉ	278
6.1.4 Chuyển giao khoá công khai của CA cho người dùng	278
6.1.5 Kích thước khoá	278
6.1.6 Sinh các tham số khoá công khai	278
6.1.7 Kiểm tra chất lượng tham số	278
6.1.8 Sinh khóa phần mềm/phần cứng	278
6.1.9 Mục đích sử dụng khoá (Nhu X.509 phiên bản 3)	278
6.2 Bảo vệ khoá riêng	278
6.2.1 Các chuẩn dành cho mô đun mật mã	278
6.2.2 Khoá riêng có nhiều người kiểm soát	279
6.2.3 Lưu trữ, sao lưu dự phòng và uỷ nhiệm khoá riêng	279
6.2.4 Khoá riêng được sử dụng trong mô đun mật mã	279
6.2.5 Phương pháp huỷ bỏ khoá riêng	279
6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá	279
6.3.1 Lưu trữ khoá công khai	279
6.3.2 Khoảng thời gian sử dụng khoá công khai và khoá riêng	279
6.4 Dữ liệu kích hoạt	280

6.5 Các kiểm soát an toàn máy tính	280
6.6 Các kiểm soát kỹ thuật đối với chu kỳ tồn tại	280
6.6.1 Các kiểm soát phát triển hệ thống	280
6.6.2 Các kiểm soát quản lý an toàn	281
6.7 Các kiểm soát an toàn mạng	281
6.8 Các kiểm soát kỹ thuật mật mã	282
6.9 Đảm bảo an toàn máy tính	282
6.10 Đảm bảo an toàn chu kỳ tồn tại	282
7. Các Khái lược của chứng chỉ và CRL	282
7.1 Các Khái lược và phiên bản của chứng chỉ	283
7.2 Tên đối tượng của chính sách	283
7.3 Các tên đối tượng của thuật toán ký	283
7.4 Sử dụng của các trường tên	283
7.5 Các ràng buộc tên và dạng tên dành cho các ràng buộc tên	283
7.6 Các trường mở rộng của chứng chỉ và tính thiết yếu của chúng	283
7.7 Sử dụng của các ràng buộc chính sách	284
7.8 Các qualifier của chính sách	284
7.9 Xử lý ngữ nghĩa cho mở rộng chính sách chứng chỉ thiết yếu	284
7.10 Số lượng phiên bản CRL	284
7.11 CRL, các mở rộng của CRL entry và tính thiết yếu của chúng	284
8. Quản lý đặc tả	284
8.1 Các thủ tục thay đổi đặc tả	284
8.1.1 Các mục có thể thay đổi không cần thông báo	284
8.1.2 Các thay đổi cần thông báo	284
8.1.3 Các mục thay đổi yêu cầu một chính sách mới	285

8.2 Việc công bố và thông báo các chính sách.....	285
8.2.1 Các mục không được công bố trong CPS.....	285
8.2.2 Việc phân phối định nghĩa chính sách chứng chỉ và CPS.....	285
8.3 Các thủ tục phê chuẩn CPS.....	286
Phần II: Chính sách chứng chỉ dành Cho các ứng dụng thiết lập khoá mã	287
1. Giới thiệu.....	287
1.1 Tổng quan	287
1.2 Nhận dạng.....	288
1.3 Cộng đồng và khả năng áp dụng.....	288
1.3.1 Khả năng áp dụng	288
2. Các điều khoản chung.....	288
2.1 Tính bí mật.....	288
3. Nhận dạng và xác thực	289
3.1 Đăng ký ban đầu.....	289
3.1.1 Phương pháp chứng minh quyền sở hữu đối với khoá riêng.....	289
4. Các yêu cầu hoạt động	289
5. Các kiểm soát an toàn cá nhân, vật lý và thủ tục	289
6. Các kiểm soát an toàn kỹ thuật	289
6.1 Sinh và cài đặt cặp khoá.....	289
6.1.1 Sinh cặp khoá.....	289
6.1.2 Chuyển giao khoá riêng cho thực thể.....	289
6.1.3 Kích thước khoá	290
6.1.4 Sinh các tham số khoá công khai.....	290
6.1.5 Các mục đích sử dụng khoá (Như X.509 phiên bản 3)....	290
6.2 Bảo vệ khóa riêng	290
6.2.1 Uỷ nhiệm khoá riêng	290

6.2.2 Sao lưu dự phòng khoá riêng.....	290
6.2.3 Lưu trữ khoá riêng	290
6.2.4 Khoá riêng được sử dụng trong mô đun mật mã	290
6.3 Các khía cạnh khác liên quan tới việc quản lý cặp khoá ...	290
6.3.1 Lưu trữ khoá công khai	290
6.3.2 Khoảng thời gian sử dụng của khoá công khai và khoá riêng	291
7. Các khái lược của chứng chỉ và CRL.....	291
7.2 Tên đối tượng của chính sách.....	291
8. Quản lý đặc tả	291
Các từ viết tắt và một số khái niệm	297
Tài liệu tham khảo.....	304

Ts. Nguyễn Nam Hải – Ks. Đào Thị Hồng Vân – Ts. Phạm Ngọc Thuý

CHỨNG THỰC TRONG THƯƠNG MẠI ĐIỆN TỬ

Chịu trách nhiệm xuất bản : PGS, TS, TÔ ĐĂNG HẢI

Biên tập : KIÊN TRUNG

Sửa bõng : KIÊN TRUNG

Vẽ bìa : HƯƠNG LAN

33 – 339

KHKT - 2003

In 500 bản khổ 16x24 cm tại Nhà in Khoa học Công nghệ
Giấy phép XB số 113-248, cấp ngày 18/8/2003.
In xong và nộp lưu chiểu tháng 3/2004.

203238



Giá: 42.000^d