TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 7817-1 : 2007
ISO/IEC 11770-3 : 1996

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – KỸ THUẬT MẬT MÃ – QUẢN LÝ KHÓA – PHẦN 1 – KHUNG TỔNG QUÁT

Information technology – Cryptographic techniques
Key management - Part 1: Framework

HÀ NỘI - 2007

Mục lục Trang

Lời nói đầu

TCVN 7817-1 : 2007 hoàn toàn tương đương với **ISO/IEC 11770-1 : 1996**

TCVN 7817-1 : 2007 do Tiểu ban Kỹ thuật Tiêu chuẩn TCVN/JTC 1/SC 27 "Các kỹ thuật mật mã" biên soạn, Ban Cơ yếu Chính phủ đề nghị, Bộ Khoa học và Công nghệ công bố.

Xuất bản lần 1

Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa
Phần 1: Khung tổng quát

Information technology – Cryptographic techniques – Key management - Part 1: Framework

1 Phạm vi áp dụng

Tiêu chuẩn này:

1. Xác định mục tiêu về quản lý khóa;
2. Mô tả mô hình tổng quát của cơ chế quản lý khóa;
3. Định nghĩa các khái niệm cơ bản về quản lý khóa sử dụng trong cả ba phần của tiêu chuẩn này;
4. Đưa ra các dịch vụ quản lý khóa;
5. Nêu ra các đặc điểm đặc trưng cho mỗi cơ chế quản lý khóa;
6. Xác định các yêu cầu về quản lý dữ liệu khóa trong một chu trình khóa.
7. Mô tả tổng quát về việc quản lý dữ liệu khóa trong một chu trình khóa.

Khung tổng quát này xác định một mô hình chung về quản lý khóa độc lập với việc sử dụng thuật toán mật mã. Tuy nhiên, một số cơ chế phân phối khóa có thể phụ thuộc vào các tính chất của thuật toán cụ thể, chẳng hạn các tính chất của các thuật toán phi đối xứng.

Các cơ chế quản lý khóa cụ thể được đưa ra ở các phần khác của bộ TCVN về quản lý khóa. Các cơ chế quản lý khóa dựa trên mật mã đối xứng được đưa ra ở Phần 2 của bộ tiêu chuẩn (ISO/IEC 11770-2 : 1999, *Kỹ thuật mật mã - Quản lý khóa - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng*). Các cơ chế phi đối xứng được đưa ra ở Phần 3 (TCVN 7817-3 : 2007, *Kỹ thuật mật mã - Quản lý khóa - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng*). Tiêu chuẩn này trình bày nội dung cần thiết nhằm cung cấp hiểu biết cơ bản cho việc áp dụng Phần 2 và Phần 3 của bộ tiêu chuẩn. Các ví dụ về sử dụng cơ chế quản lý khóa được đưa ra ở ISO 8732 và ISO 11166. Nếu vấn đề chống chối bỏ được yêu cầu trong quản lý khóa thì có thể sử dụng ISO/IEC 13888.

Tiêu chuẩn này đề cập đến cả hai khía cạnh của việc quản lý khóa là quản lý theo cách tự động và quản lý theo cách thủ công, bao gồm phần giới thiệu về các thành phần dữ liệu và chuỗi thao tác tuần tự được thực hiện trong các dịch vụ quản lý khóa. Tuy nhiên, nội dung phần này không đề cập chi tiết về các giao thức trao đổi khóa.

Cũng giống như các dịch vụ an toàn khác, quản lý khóa chỉ có thể được cung cấp trong ngữ cảnh chính sách an toàn được xác định. Việc định nghĩa các chính sách an toàn nằm ngoài phạm vi của bộ tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viễn dẫn dưới đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng bản mới nhất, bao gồm cả các sửa đổi.

- ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic reference Model – Part 2: Secirity Architecture (Các hệ thống xử lý thông tin - Liên kết các Hệ thống mở - Kiểu tham chiếu cơ bản - Phần 2: Kiến trúc an toàn).
- ISO/IEC 9798-1:1991, Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model (Công nghệ thông tin- Kỹ thuật mật mã – Các cơ chế Xác thực thực thể - Phần 1: Mô hình chung).
- ISO/IEC10181-1:1996, Information technology – Open Systems Interconnection – Security framework for open systems: Overview (Công nghệ thông tin - Liên kết các Hệ thống mở - Khung an toàn cho các hệ thống mở: Tổng quan).

3 Các thuật ngữ và định nghĩa

Các thuật ngữ sau đã được định nghĩa trong ISO/IEC 7498-2:

Tính toàn vẹn dữ liệu (data integrity)

Xác thực nguồn gốc dữ liệu (data origin authentication)

Chữ ký số (digital signature)

Thuật ngữ sau đã được định nghĩa trong ISO/IEC 9798-1

Xác thực thực thể (entity authentication)

Các thuật ngữ sau đã được định nghĩa trong ISO/IEC 10181-1:

Tổ chức thẩm quyền về an toàn (security authority)

Miền an toàn (security domain)

Bên thứ ba tin cậy (TTP – Trusted Third Party)

Tiêu chuẩn này áp dụng các định nghĩa sau:

3.1

Kỹ thuật mật mã phi đối xứng (asymmetric cryptographic technique)

Kỹ thuật mật mã sử dụng hai phép biến đổi có liên quan đến nhau, phép biến đổi công khai (sử dụng một khóa công khai) và phép biến đổi bí mật (sử dụng một khóa bí mật). Cả hai phép biến đổi này có tính chất là khi đã biết phép biến đổi công khai cũng không thể tính toán ra được phép biến đổi bí mật.

3.2

Cơ quan chứng thực (CA – certification authority)

Trung tâm được tin cậy tạo và đưa ra các chứng chỉ khóa công khai. Ngoài ra, CA có thể đảm nhận việc tạo và đưa ra khóa cho các thực thể.

3.3

Giải mã (decipherment)

Phép nghịch đảo của phép mã hóa tương ứng.

3.4

Mã hóa (encipherment)

Phép biến đổi khả nghịch lên dữ liệu bằng một thuật toán mật mã để tạo ra bản mã nhằm mục đích che dấu nội dung thông tin của dữ liệu.

3.5

Khóa (key)

Một dãy ký tự sử dụng trong một phép biến đổi mật mã (mã hóa, giải mã, tính toán hàm kiểm tra mật mã, tạo hoặc xác minh chữ ký số).

3.6

Thỏa thuận khóa (key agreement)

Tiến trình kiến tạo một khóa bí mật dùng chung giữa hai thực thể theo cách mà không bên nào có thể tự mình định trước được giá trị cho khóa.

3.7

Xác nhận khóa (key confirmation)

Sự đảm bảo cho một thực thể rằng một thực thể khác đã được định danh đang sở hữu một khóa đúng.

3.8

Điều khiển khóa (key control)

Khả năng lựa chọn khóa hoặc tham số sử dụng trong một phép tính toán khóa.

3.9

Trung tâm phân phối khóa (KDC – Key Distribution Centre)

Một thực thể được tin cậy trong việc tạo, thu nhận hoặc phân phối khóa cho các thực thể có chia sẻ khóa với nó.

3.10

Dữ liệu khóa (key material)

Dữ liệu (khóa, giá trị khởi đầu) cần thiết để thiết lập và duy trì các mối quan hệ về khóa mật mã.

3.11

Quản lý khóa (key management)

Quản trị và sử dụng việc tạo, đăng ký, chứng nhận, tái đăng ký, phân phối, thiết đặt, cất giữ, cất giữ, thu hồi, dẫn xuất, hủy bỏ dữ liệu khóa tuân theo một chính sách an toàn nào đó.

3.12

Trung tâm truyền khóa (KTC – Key Translation Centre)

Một thực thể được tin cậy trong việc truyền khóa mật mã giữa các thực thể có dùng chung cùng một khóa với KTC.

3.13

Khóa riêng (private key)

Khóa thuộc một cặp khóa phi đối xứng của một thực thể chỉ được sử dụng bởi thực thể đó.

CHÚ THÍCH: Trong hệ chữ ký phi đối xứng thì khóa bí mật dùng cho phép biến đổi ký. Trong hệ mật phi đối xứng thì khóa bí mật dùng cho phép giải mã.

3.14

Khóa công khai (public key)

Khóa thuộc cặp khóa phi đối xứng của một thực thể được công bố công khai.

3.15

Chứng chỉ khóa công khai (Public key information)

Thông tin khóa công khai của một thực thể được ký bởi cơ quan có thẩm quyền chứng thực vì thế chống được sự giả mạo.

3.16

Thông tin khóa công khai (public key information)

Thông tin đặc thù cho một thực thể đơn lẻ có chứa ít nhất một định danh riêng biệt về thực thể và ít nhất một khóa công khai của thực thể đó. Ngoài ra có thể có thêm các thông tin khác liên quan đến tổ chức thẩm quyền cấp chứng chỉ (CA), thực thể và khóa công khai được chứa trong thông tin khóa

công khai chẳng hạn như thời hạn hiệu lực của khóa công khai, thời hạn hiệu lực của khóa bí mật tương ứng và định danh của các thuật toán được sử dụng.

3.17

Số ngẫu nhiên (random number)

Tham số biến thiên theo thời gian mà giá trị của nó không thể đoán trước được.

3.18

Khóa bí mật (secret key)

Khóa sử dụng cho kỹ thuật mật mã đối xứng và chỉ được dùng bởi một tập thực thể xác định.

3.19

Số tuần tự (sequence number)

Tham số biến thiên theo thời gian mà giá trị của nó được nhận từ một dãy số không có sự lặp lại trong một khoảng thời gian xác định.

3.20

Kỹ thuật mật mã đối xứng (symmetric cryptographic technique)

Kỹ thuật mật mã sử dụng cùng một khóa mật cho các phép thực hiện các phép biến đổi của cả bên truyền và bên nhận. Nếu không biết thông tin về khóa bí mật thì không thể thực hiện được biến đổi của bên truyền cũng như bên nhận.

3.21

Tem thời gian (time stamp)

Một tham số biến thiên theo thời gian đánh dấu một thời điểm trong một hệ tham chiếu về thời gian thông thường.

3.22

Tham số biến thiên theo thời gian (time variant parameter)

Một mục dữ liệu được sử dụng bởi một thực thể để kiểm tra rằng một thông điệp không được tái sử dụng, chẳng hạn như số ngẫu nhiên, số tuần tự hoặc tem thời gian.

4 Thảo luận chung về Quản lý khóa

Quản lý khóa là việc quản trị và sử dụng liên quan đến việc tạo, đăng ký, chứng nhận, bỏ đăng ký, phân phối, cài đặt, cất giữ, cất giữ, thu hồi, dẫn xuất, hủy bỏ vật liệu khóa.

Mục tiêu của quản lý khóa là quản trị và sử dụng an toàn các dịch vụ quản lý khóa, do đó việc bảo vệ các khóa là điều tối quan trọng.

Các thủ tục quản lý khóa phụ thuộc vào các cơ chế mật mã, sử dụng cho khóa và chính sách an toàn. Quản lý khóa cũng bao gồm cả các chức năng được thực hiện trong thiết bị mật mã.

4.1 Bảo vệ khóa

Khóa là thành phần trọng tâm của bất cứ hệ thống an toàn nào dựa trên kỹ thuật mật mã. Việc bảo vệ khóa một cách thích hợp phụ thuộc vào một số nhân tố như kiểu áp dụng đối với mỗi khóa được dùng, các mối đe dọa mà chúng phải đối mặt, các tình huống khác nhau có thể phải tính đến,…Trước hết, phụ thuộc vào kỹ thuật mật mã được sử dụng, chúng cần được bảo vệ trước khả năng bị lộ, sửa đổi, phá hủy và tái sử dụng. Phụ lục A đưa ra các ví dụ về các nguy cơ đe dọa có thể đối với khóa. Tính hiệu lực của khóa sẽ bị giới hạn theo thời gian và số lần sử dụng. Các ràng buộc này được xác định bởi thời gian và khối lượng dữ liệu cần thiết để tạo nên sự tấn công phục hồi khóa và giá trị chiến lược về thông tin được bảo vệ theo thời gian. Những khóa được dùng để sinh khóa khác cần được bảo vệ ở mức cao hơn các khóa đã được sinh ra. Một khía cạnh quan trọng khác của việc bảo vệ khóa là phải tránh việc sử dụng khóa sai mục đích, chẳng hạn như sử dụng một khóa dùng để mã hóa các khóa làm một khóa để mã hóa dữ liệu.

Bảo vệ khóa bằng kỹ thuật mật mã

Một số mối đe dọa lên dữ liệu khóa có thể tránh được bằng cách sử dụng kỹ thuật mật mã. Ví dụ, việc mã hóa sẽ giúp chống được khả năng lộ khóa và sử dụng bất hợp pháp, các cơ chế toàn vẹn dữ liệu giúp chống được việc sửa đổi, các cơ chế xác thực nguồn gốc dữ liệu và chữ ký số hoặc xác thực thực thể giúp chống được sự mạo danh.

Các cơ chế tách biệt mật mã sẽ giúp ngăn ngừa sử dụng sai. Việc tách biệt về mặt chức năng sử dụng như vậy có thể thực hiện bằng cách gắn thông tin vào khóa. Chẳng hạn, việc gắn thông tin điều khiển vào một khóa sẽ đảm bảo rằng một khóa xác định được sử dụng cho các nhiệm vụ xác định (ví dụ: mã hóa khóa, toàn vẹn dữ liệu); việc điều khiển khóa được yêu cầu cho việc chống chối bỏ khi sử dụng kỹ thuật đối xứng.

Bảo vệ khóa bằng kỹ thuật phi mật mã

Tem thời gian có thể được sử dụng để hạn chế việc sử dụng khóa trong một khoảng thời gian xác định. Cùng với số tuần tự, chúng còn có thể bảo vệ tránh được việc tái sử dụng các thông tin thỏa thuận khóa được ghi lại.

Bảo vệ khóa bằng phương tiện vật lý

Thông thường mỗi thiết bị mật mã được dùng trong một hệ thống an toàn đều đòi hỏi rằng các dữ liệu khóa mà nó sử dụng phải được bảo vệ chống lại các nguy cơ về sửa đổi, xóa bỏ và khả năng bi lộ, ngoại trừ các khóa công khai. Mỗi thiết bị thường tạo ra một khu vực an toàn để cất giữ khóa, sử dụng khóa và thực thi thuật toán mật mã. Các phương pháp cho vấn đề này có thể là:

- Nạp dữ liệu khóa từ một thiết bị lưu trữ khóa an toàn tách biệt.
- Tương tác với các thuật toán mật mã được triển khai trong các thiết bị an toàn thông minh riêng biệt (chẳng hạn như thẻ thông minh, thẻ nhớ,….).

- Cất giữ dữ liệu khóa ở một vị trí ngoại tuyến (ví dụ, trên đĩa mềm).

Các khu vực an toàn thông thường được bảo vệ bởi các cơ chế an toàn vật lý.

Bảo vệ khóa bằng phương tiện tổ chức

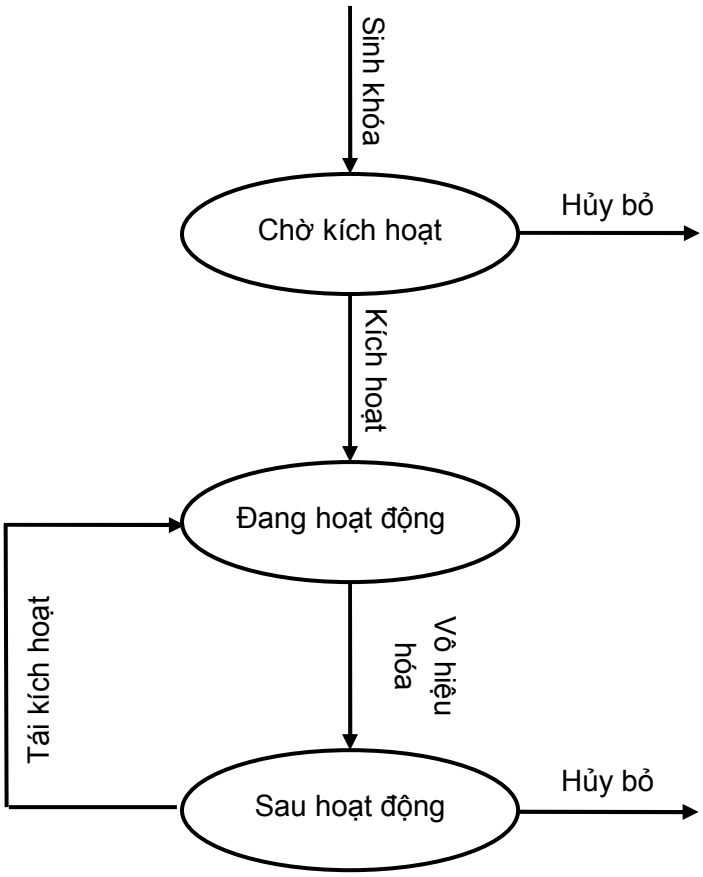
Một phương tiện bảo vệ khóa khác là tổ chức chúng theo dạng khóa có cấu trúc có phân cấp. Ngoại trừ ở tầng dưới cùng, các khóa ở cùng một tầng của hệ thống phần cấp chỉ được sử dụng để bảo vệ khóa ở tầng dưới kế tiếp. Chỉ có khóa ở mức dưới cùng của cấu trúc khóa là thực sự được sử dụng cho các dịch vụ an toàn dữ liệu. Cấu trúc phân cấp này chỉ cho phép sử dụng mỗi khóa có giới hạn vì thế hạn chế được việc tiết lộ khóa và gây khó khăn đối với các tấn công. Chẳng hạn, khi một khóa phiên đơn lẻ bị tổn thương thì chỉ ảnh hưởng đến thông tin được bảo vệ bởi khóa đó.

Sử dụng không gian an toàn là muốn nói đến các đe dọa làm lộ, sửa đổi và xóa bỏ khóa bởi các thực thể không có thẩm quyền. Tuy nhiên, vẫn còn nguy cơ rằng những người quản trị hệ thống - những người có thẩm quyền thực hiện các chức năng quản lý nào đó trên các thành phần của dịch vụ quản lý khóa sử dụng sai một số đặc quyền truy cập dành cho họ. Đặc biệt, những người này có thể tìm cách có được khóa chủ (là khóa ở tầng cao nhất trong cấu trúc phân cấp). Việc để lộ khóa chủ có thể cho phép người nắm giữ nó khám phá hoặc điều phối tất cả các khóa còn lại được bảo vệ bởi nó (tất cả khóa còn lại trong cấu trúc khóa phân cấp). Bởi vậy, tốt nhất là hạn chế ở mức thấp nhất việc truy cập đến khóa này, có thể sắp xếp sao cho cho không để duy nhất một người nắm giữ khóa chủ. Yêu cầu này có thể thực hiện được bằng cách chia khóa này ra thành nhiều thành phần khóa (điều khiển kép hoặc điều khiển nhiều lần) hoặc sử dụng các lược đồ mật mã riêng (*Lược đồ Phân chia Bí mật*).

4.2 Mô hình chung của vòng đời khóa

Khóa mật mã sẽ trải qua một loạt các trạng thái tạo nên một vòng đời của khóa. Có ba trạng thái cơ bản trong một vòng đời của khóa là:

- **Chờ kích hoạt**: Ở trạng thái chờ kích hoạt thì khóa đã được tạo ra nhưng chưa được kích hoạt để sử dụng.
- **Đang hoạt động**: Ở trạng thái này khóa được sử dụng để xử lý thông tin mật mã.
- **Sau hoạt động**: Ở trạng thái này khóa chỉ được dùng để cho việc giãi mã hoặc kiểm tra chữ ký.



Hình 1 – Vòng đời của Khóa

GHI CHÚ: Một người sử dụng khóa ở trạng thái Sau hoạt động cần phải được đảm bảo rằng dữ liệu đã được xử lý mật mã bằng khóa đó không được sử dụng trước khi khóa bị chuyển sang chế độ Sau hoạt động. Sự đảm bảo này được thực hiện bởi một tham biến thời gian tin cậy.

Khóa nếu được phát hiện ra đã bị tổn thương ngay lập tức sẽ được chuyển sang trạng thái Sau hoạt động và có thể đòi hỏi sự xử lý đặc biệt. Khóa được coi là đã bị tổn thương nếu bị sử dụng bất hợp pháp hoặc nghi ngờ bị sử dụng bất hợp pháp.

Hình 1 trình bày các trạng thái và các thao tác chuyển trạng thái tương ứng với từng trạng thái.

Hình 1 cũng trình bày về một mô hình chu trình khóa tổng quan. Các mô hình vòng đời khác có thể có thêm chi tiết mà chúng có thể là các trạng thái con của ba trạng thái nêu trên. Phần lớn vòng đời khóa đều đòi hỏi hoạt động lưu trữ. Hoạt động này có thể liên quan với bất kỳ trạng thái nào ở trên phụ thuộc vào các chi tiết cụ thể của vòng đời khóa.

4.2.1 Thao tác chuyển đổi giữa các trạng thái khóa

Khi một khóa chuyển từ một trạng thái này sang một trạng thái khác nó sẽ thực hiện một trong các thao tác chuyển trạng thái (transition) như đã nói ở Hình 1, bao gồm:

- **Sinh khóa**: Đây là tiến trình tạo ra một khóa. Tiến trình sinh khóa nên được thực hiện tuân theo quy tắc sinh khóa cho trước. Quá trình này có thể thực thi cùng một thủ tục kiểm tra để xem các quy tắc sinh khóa có được thực hiện đúng hay không.
- **Kích hoạt**: Là việc đưa một khóa trở nên khả dụng đối với các thao tác mật mã.
- **Vô hiệu hóa**: Là việc giới hạn sử dụng khóa. Thao tác chuyển trạng thái này có thể xảy ra khi khóa hết thời hạn sử dụng hoặc cần phải thu hồi.
- **Tái kích hoạt**: Cho phép chuyển khóa từ trạng thái Sau hoạt động về trạng thái Đang hoạt động để sử dụng cho các thao tác mật mã.
- **Hủy bỏ**: Kết thúc một vòng đời khóa. Thao tác chuyển trạng thái này thực hiện hủy bỏ khóa về mặt logic cũng như hủy bỏ về mặt vật lý một khóa.

Các thao tác chuyển trạng thái có thể được khởi tạo (triggered) bằng các sự kiện như việc yêu cầu có một khóa mới, khóa bị tổn thương, khóa đã hết hạn và hoàn thành một vòng đời khóa. Tất cả thao tác chuyển trạng thái này sẽ bao gồm một số các dịch vụ về quản lý khóa. Mối quan hệ giữa các thao tác chuyển trạng thái và dịch vụ có thể tìm thấy ở Bảng 1. Mô tả về các dịch vụ được trình bày ở Mục 5.

Bất kỳ một tiếp cận mật mã cụ thể nào cũng chỉ đòi hỏi một tập con các dịch vụ đưa ra ở Bảng 1.

4.2.2 Thao tác chuyển trạng thái, Dịch vụ và Khóa

Khóa cho các kỹ thuật mật mã cụ thể sẽ sử dụng theo cách kết hợp giữa các dịch vụ khác nhau trong suốt một vòng đời khóa. Sau đây là ví dụ cho hai trường hợp cụ thể.

Đối với kỹ thuật mật mã đối xứng, sau khi sinh ra một khóa, việc chuyển từ trạng thái Chờ kích hoạt sang trạng thái Đang hoạt động sẽ bao gồm dịch vụ cài đặt khóa và có thể bao gồm dịch vụ đăng ký và phân phối khóa. Trong một số trường hợp, việc cài đặt khóa có thể bao gồm cả việc dẫn xuất của một khóa xác định nào đó. Thời gian sống của khóa nên được giới hạn trong một khoảng thời gian xác định. Việc Vô hiệu hóa kết thúc trạng thái Đang hoạt động của một khóa thông thường dựa vào việc khóa bị hết hạn. Nếu một khóa ở trạng thái Đang hoạt động được phát hiện là bị tổn thương hoặc nghi ngờ bị tổn thương thì dịch vụ hủy bỏ khóa sẽ được dùng để đưa khóa này về trạng thái Sau hoạt động. Nếu khóa đang được lưu trữ được yêu cầu lại thì nó có thể được tái kích hoạt và có thể cần được cài đặt hoặc phân phối lại trước khi chuyển sang trạng thái Đang hoạt động hoàn toàn. Nếu không, sau khi Vô hiệu hóa, khóa có thể được hủy đăng ký và bị phá hủy.

Đối với kỹ thuật phi đối xứng, một cặp khóa (khóa riêng và khóa công khai) được tạo ra và cả hai khóa này được chuyển sang trạng thái Chờ kích hoạt. Chú ý rằng vòng đời của hai khoá này có mối liên hệ với nhau nhưng không đồng nhất với nhau. Trước khi được chuyển sang trạng thái Đang hoạt động, khoá riêng theo tuỳ chọn có thể được đăng ký và phân phối đến người dùng và luôn được cài đặt. Các thao tác chuyển trạng thái Đang hoạt động và Sau hoạt động đối với khóa riêng bao gồm Vô hiệu hóa, tái kích hoạt và hủy bỏ, tương tự như đã được mô tả ở phần dành cho kỹ thuật đối xứng. Khi một khóa công khai được chứng thực thì thông thường CA sẽ tạo ra một chứng chỉ có chứa một khóa công khai để đảm bảo tính hợp lệ và tính sở hữu đối với khóa công khai. Chứng chỉ khóa công khai này có thể

được đưa vào một thư mục hoặc dịch vụ tương tự để phân phối hoặc được chuyển trở lại cho chủ sở hữu để phân phối. Mỗi khi chủ sở hữu khóa gửi thông tin được ký bởi khóa riêng thì có thể kèm theo cả chứng chỉ công khai của mình. Cặp khóa sẽ được kích hoạt khi khóa công khai được chứng thực. Khi cặp khóa được sử dụng cho chữ ký thì khóa công khai có thể vẫn được giữ mãi ở trạng thái Đang hoạt động hoặc Sau hoạt động sau khi khóa riêng tương ứng đã bị vô hiệu hóa hoặc bị hủy bỏ. Có thể vẫn cần phải truy cập đến khóa công khai cho mục đích kiểm tra chữ ký số đã được tạo ra trước đây mặc dù khóa bí mật kết hợp với khóa công khai này đã hết hạn sử dụng. Khi sử dụng kỹ thuật phi đối xứng cho mục tiêu mã hóa thì mặc dù khóa công khai dùng để mã hóa đã bị vô hiệu hóa hoặc hủy bỏ nhưng khóa riêng tương ứng với nó vẫn được duy trì ở trạng thái Đang hoạt động hoặc Sau hoạt động nhằm phục vụ cho việc giải mã.

Tùy vào cách sử dụng hoặc ứng dụng khóa để xác định các dịch vụ cho khóa. Ví dụ, một hệ thống có thể quyết định là không cần đăng ký các khóa phiên vì tiến trình đăng ký có thể lâu hơn vòng đời khóa. Ngược lại, khi sử dụng kỹ thuật đối xứng cho các chữ ký số cần thiết phải đăng ký khóa bí mật.

Thao tác chuyển trạng thái	Dịch vụ	Ghi chú
Sinh khóa	sinh khóa	bắt buộc
	đăng ký khóa	tùy chọn thực hiện ở thao tác chuyển trạng thái này hoặc ở thao tác chuyển trạng thái Kích hoạt
	tạo chứng chỉ khóa	tùy chọn
	phân phối khóa	tùy chọn
	dự trữ khóa	tùy chọn
Kích hoạt	tạo chứng chỉ khóa	tùy chọn
	phân phối khóa	tùy chọn
	dẫn xuất khóa	tùy chọn
	cài đặt khóa	bắt buộc
	cất giữ khóa	tùy chọn
	đăng ký khóa	tùy chọn thực hiện ở thao tác chuyển trạng thái này hoặc ở thao tác chuyển trạng thái Sinh khóa

Bỏ kích hoạt	dự trữ khóa	tùy chọn
	lưu trữ phòng khóa	tùy chọn thực hiện ở thao tác chuyển trạng thái này hoặc ở thao tác chuyển trạng thái Hủy khóa
	hủy bỏ khóa	tùy chọn
Tái kích hoạt	tạo chứng chỉ khóa	tùy chọn
	phân phối khóa	tùy chọn
	dẫn xuất khóa	tùy chọn
	cài đặt khóa	bắt buộc
	cất giữ khóa	tùy chọn
Hủy khóa	bỏ đăng ký khóa	bắt buộc, nếu có đăng ký
	hủy bỏ khóa	bắt buộc
	lưu trữ phòng khóa	tùy chọn thực hiện ở thao tác chuyển trạng thái này hoặc ở thao tác chuyển trạng thái Vô hiệu hóa

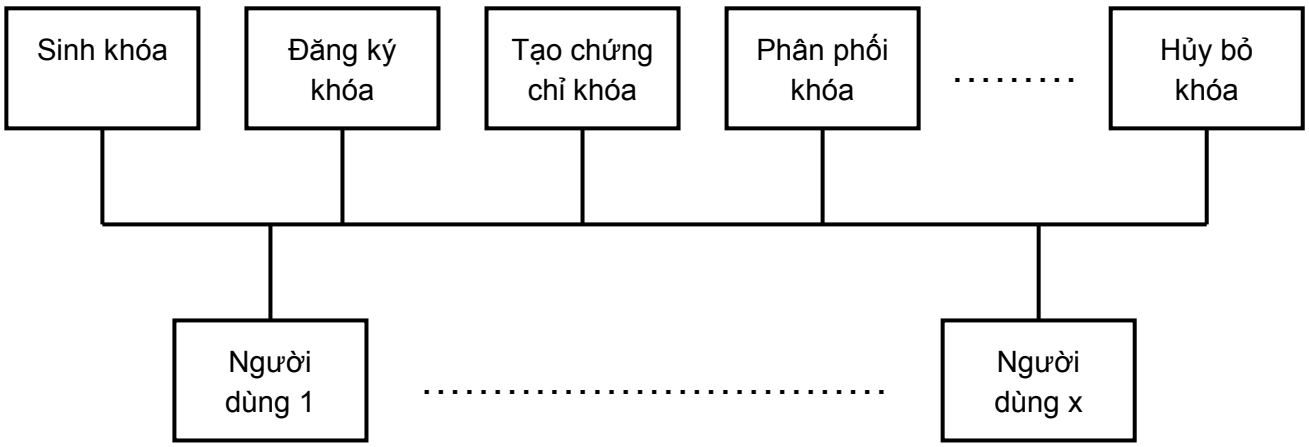
Bảng 1 - Thao tác chuyển trạng thái và Dịch vụ

5 Các khái niệm về Quản lý khóa

5.1 Các dịch vụ quản lý khóa

Mục này mô tả một cấu trúc tổng quát về quản lý khóa để làm rõ các dịch vụ quản lý khóa cũng như cách chúng kết hợp lẫn nhau và cách chúng được hỗ trợ.

Việc quản lý khóa dựa trên các dịch vụ cơ bản bao gồm sinh khóa, đăng ký, chứng nhận, phân phối, cài đặt, cất giữ, dẫn xuất, lưu trữ, vô hiệu hóa, bỏ đăng ký và hủy bỏ khóa. Các dịch vụ này có thể là một phần của một hệ thống quản lý khóa hoặc được cung cấp bởi các nhà cung cấp dịch vụ khác. Tùy thuộc vào kiểu dịch vụ mà các nhà cung cấp dịch vụ phải đáp ứng một số yêu cầu an toàn tối thiểu nào đó (chẳng hạn trao đổi an toàn) được tin cậy bởi tất cả thực thể. Ví dụ, nhà cung cấp dịch vụ có thể là bên thứ ba tin cậy. Hình 2 đưa ra các dịch vụ quản lý khóa được đặt ở cùng cấp độ và có thể được sử dụng bởi những người dùng khác nhau (con người hoặc tiến trình). Những người dùng này có thể sử dụng các phương tiện quản lý khóa khác nhau trong những ứng dụng khác nhau, sử dụng các dịch vụ cụ thể theo nhu cầu. Các dịch vụ về quản lý khóa đã được liệt kê ở Bảng 1.



Hình 2 – Các dịch vụ quản lý khóa

5.1.1 Sinh khóa

Sinh khóa là dịch vụ tạo ra các khóa theo một cách an toàn dùng cho một thuật toán mật mã cụ thể. Điều này nghĩa là khóa được tạo ra theo một phương thức không thể dự đoán được và tuân theo sự phân bố quy định trước. Phân bố này được áp đặt bởi một thuật toán mật mã sử dụng nó và đòi hỏi một mức bảo vệ mật mã. Việc sinh một số loại khóa, chẳng hạn khóa chủ, đòi hỏi phải có sự quan tâm đặc biệt bởi nếu biết khóa chủ có thể dẫn đến khả năng truy cập được tất cả các khóa liên quan hoặc các khóa được dẫn xuất.

5.1.2 Đăng ký khóa

Dịch vụ đăng ký khóa kết hợp một khóa với một thực thể. Nó được cung cấp bởi tổ chức có thẩm quyền đăng ký và thường được áp dụng khi sử dụng kỹ thuật mật mã đối xứng. Khi một thực thể muốn đăng ký một khóa nó phải liên hệ với tổ chức đăng ký có thẩm quyền. Tiến trình đăng ký khóa bao gồm một yêu cầu đăng ký và xác nhận cho việc đăng ký này.

Tổ chức có thẩm quyền đăng ký duy trì sự đăng ký cho các khóa và thông tin liên quan một cách an toàn. Phụ lục B đưa ra chi tiết các thông tin về quản lý khóa.

Đăng ký và tái đăng ký là các dịch vụ do cơ quan có thẩm quyền đăng ký cung cấp.

5.1.3 Tạo chứng chỉ khóa

Dịch vụ tạo chứng chỉ khóa là việc kết hợp một khóa công khai với một thực thể được thực hiện bởi bên có thẩm quyền chứng thực. Khi một yêu cầu về chứng chỉ khóa được chấp nhận thì cơ quan chứng thực sẽ tạo ra một chứng chỉ khóa. Các chứng chỉ khóa công khai được đề cập chi tiết hơn ở Phần 3 của bộ tiêu chuẩn đa phần này.

5.1.4 Phân phối khóa

Phân phối khóa là một tập các thủ tục để cung cấp các đối tượng thông tin quản lý khóa (xem ví dụ ở Phụ lục B) một cách an toàn cho các thực thể có thẩm quyền. Một trường hợp đặc biệt về phân phối khóa là việc truyền dữ liệu khóa được kiến tạo giữa các thực thể sử dụng một trung tâm truyền khóa (Điều 6.2). Phần 2 của bộ tiêu chuẩn này đưa ra các cơ chế truyền khóa khác nhau để kiến tạo một khóa giữa các thực thể. Phần 3 của bộ tiêu chuẩn này đưa ra các cơ chế về thỏa thuận khóa mật cũng như các cơ chế truyền khóa mật và khóa công khai.

5.1.5 Cài đặt khóa

Dịch vụ cài đặt khóa luôn cần phải thực hiện trước khi sử dụng một khóa. Cài đặt khóa nghĩa là thiết lập khóa vào trong một phương tiện quản lý khóa theo cách có thể bảo vệ để khóa không bị tổn thương.

5.1.6 Cất giữ khóa

Dịch vụ cất giữ khóa cung cấp một nơi chứa khóa để sử dụng ngay hoặc dự kiến sử dụng trong một thời gian ngắn hoặc cho mục đích sao lưu. Thông thường, cất giữ khóa theo phương thức tách biệt vật lý sẽ có lợi hơn. Chẳng hạn, điều này sẽ đảm bảo tính bí mật và toàn vẹn cho dữ liệu khóa hoặc tính toàn vẹn cho khóa công khai. Việc cất giữ khóa có thể xẩy ra trong tất cả trạng thái (Chờ kích hoạt, Đang hoạt động và Sau hoạt động) của một vòng đời khóa. Phụ thuộc vào tầm quan trọng của khóa mà các khóa có thể được bảo vệ bằng một trong các cơ chế sau:

- An toàn về mặt vật lý (ví dụ, bằng cách cất giữ khóa vào thiết bị chống được sự can thiệp hoặc lưu vào các phương tiện bên ngoài như đĩa mềm hay thẻ nhớ),
- Mã hóa bằng các khóa được lưu an toàn về mặt vật lý,
- Bảo vệ truy cập bằng mật khẩu hoặc PIN (Số định danh cá nhân).

Đối với tất cả dữ liệu khóa nên có khả năng phát hiện bất cứ cố gắng gây tổn thương nào.

5.1.7 Dẫn xuất khóa

Dịch vụ dẫn xuất khóa dựa trên một số lượng lớn khóa có thể sử dụng một khóa bí mật ban đầu gọi là khóa gốc, dữ liệu thay đổi không mật và một tiến trình biến đổi (cũng không cần giữ bí mật). Kết quả của quá trình này là tìm ra khóa gốc. Khóa gốc cần phải được bảo vệ theo cách đặc biệt. Tiến trình tìm khóa gốc đảm bảo có tính không đảo ngược và không thể đoán biết trước để đảm bảo rằng khi một khóa gốc bị tổn thương thì không làm tiết lộ nguồn gốc khóa và những thành phần khác của khóa gốc.

5.1.8 Cất giữ khóa

Cất giữ khóa là một tiến trình cất giữ dài hạn và an toàn các khóa sau khi sử dụng xong. Việc **cất giữ** khóa có thể sử dụng một dịch vụ **cất giữ** khóa nhưng lại tuân theo một cách thực hiện khác chẳng hạn cất giữ độc lập (off-line). Việc **cất giữ** khóa có thể cần để gọi dùng lại vào một thời gian sau đó nhằm

chứng minh hoặc bác bỏ một đòi hỏi nào đó sau khi khóa không còn sử dụng theo cách thông thường nữa.

5.1.9 Thu hồi khóa

Khi phát hiện hoặc nghi ngờ một khóa bị tổn thương thì dịch vụ **thu hồi khóa** được sử dụng để đảm bảo việc Vô hiệu hóa khóa một cách an toàn. Dịch vụ này rất cần thiết để nắm bắt thời gian hết hạn của khóa. Một khóa có thể được thu hồi khi có sự thay đổi về chủ sở hữu khóa. Sau khi khóa bị thu hồi có thể khóa đó chỉ được dùng cho việc giải mã và kiểm tra chữ ký mà thôi. Dịch vụ thu hồi khóa không thích hợp khi dùng trong một lược đồ dựa trên chứng chỉ bởi khi đó chù kỳ sống của khóa được điều khiển bằng hạn dùng trên chứng chỉ.

CHÚ Ý: Một số ứng dụng dùng khái niệm **xóa bỏ khóa** thay cho khái niệm **thu hồi khóa**.

5.1.10 Bỏ đăng ký khóa

Dịch vụ **bỏ đăng ký khóa** là một thủ tục cung cấp bởi tổ chức đăng ký có thẩm quyền khóa để loại bỏ sự kết hợp giữa khóa và thực thể (xem điều 5.1.11 về Hủy bỏ khóa). Khi một thực thể muốn **bỏ đăng ký** khóa thì anh ta phải liên hệ với tổ chức đăng ký có thẩm quyền khóa.

5.1.11 Hủy bỏ khóa

Dịch vụ hủy bỏ khóa tạo ra một tiến trình hủy bỏ an toàn những khóa từ lâu không còn cần đến nữa. Hủy bỏ một khóa là loại bỏ tất cả bản ghi của đối tượng thông tin quản lý khóa sao cho không thể tìm được bất cứ thông tin còn lại nào sau khi thực hiện hủy bỏ khóa dù là bằng bất cứ phương tiện khôi phục nào. Điều này đồng nghĩa với việc hủy bỏ tất cả các bảo sao dự phòng của khóa. Tuy nhiên, trước khi các bản sao dự phòng của khóa bị hủy bỏ phải đảm bảo rằng không có bất kỳ thông tin nào trong dữ liệu khóa cất giữ còn cần đến trong tương lai.

CHÚ THÍCH: Một vài dạng khóa có thể được lưu ở bên ngoài thiết bị điện tử vì thế để hủy bỏ các khóa này có thể cần đến một số thiết bị quản trị bổ sung.

5.2 Các dịch vụ hỗ trợ

Một số dịch vụ khác có thể cần đến để hỗ trợ cho việc quản lý khóa.

5.2.1 Các dịch vụ phương tiện quản lý khóa

Các dịch vụ quản lý khóa có thể sử dụng một số dịch vụ khác có liên quan đến an toàn. Các dịch vụ này bao gồm:

- **Điều khiển truy cập**: Dịch vụ này có thể được sử dụng để đảm bảo rằng tài nguyên của một hệ thống quản lý khóa chỉ được truy cập bởi các thực thể có thẩm quyền theo cách có ủy quyền.

- **Kiểm toán**: Là việc theo dõi các sự kiện liên quan đến an toàn xuất hiện trong một hệ thống quản lý khóa. Các dấu vết kiểm toán có thể giúp ích trong vấn đền xác định điểm yếu và rủi ro về an toàn.
- **Xác thực**: Dịch vụ này nên sử dụng để xác thực rằng một thực thể là một thành viên được ủy quyền của một miền an toàn nào đó.
- **Dịch vụ mật mã**: Các dịch vụ mật mã nên được sử dụng bởi các dịch vụ quản lý khóa để cung cấp tính toàn vẹn, bí mật, xác thực và không chối bỏ.
- **Dịch vụ thời gian**: Dịch vụ này cần thiết để tạo ra các tham số biến thiên theo thời gian như khoảng thời gian tồn tại hợp lệ.

5.2.2 Các dịch vụ hướng người dùng

Các hệ thống và thiết bị mật mã có thể đòi hỏi phải có các dịch vụ khác cần thiết cho các tính năng tương ứng, chẳng hạn dịch vụ **đăng ký người dùng**,…Việc thực thi cụ thể các dịch vụ này nằm ngoài phạm vi đề cập của tiêu chuẩn này.

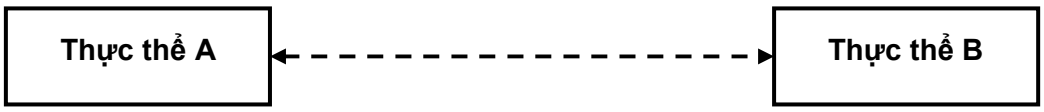
6 Các mô hình mang tính quan niệm về Phân phối khóa

Việc phân phối khóa giữa các thực thể là tương đối phức tạp. Nó có thể bị chi phối bởi điều kiện tự nhiên của các liên kết truyền thông, các mối quan hệ tin cậy liên quan và kỹ thuật mật mã được sử dụng. Các thực thể có thể truyền thông trực tiếp hoặc gián tiếp, có thể thuộc cùng một miền an toàn hoặc ở các miền an toàn khác nhau và có thể sử dụng hoặc không sử dụng các dịch vụ của một thực thể được tin cậy. Các mô hình mang tính quan điểm sau minh họa về các trường hợp khác nhau chi phối việc phân phối khóa và thông tin.

6.1 Phân phối khóa giữa các thực thể truyền thông

Truyền thông giữa các thực thể chịu ảnh hưởng bởi mối liên kết giữa các thực thể đó và sự tin cậy giữa chúng cũng như kỹ thuật mật mã được sử dụng.

Giả sử tồn tại mối kết nối giữa thực thể A và thực thể B là những thành phần đang muốn sử dụng kỹ thuật mật mã để trao đổi thông tin với nhau. Mối kết nối truyền thông này minh họa bởi Hình 3. Nói chung, việc phân phối khóa phải thực hiện qua một kênh an toàn và phải khác biệt về mặt logic với kênh truyền dữ liệu.



Hình 3 – Liên kết truyền thông giữa hai thực thể

Các trường hợp thực hiện khi các thực thể truyền thông trực tiếp với nhau là thỏa thuận khóa, điều khiển khóa và xác nhận khóa. Chi tiết về các vấn đề này sẽ được để cập ở Phần 2 (ISO/IEC 11770-2 : 1996, *Kỹ thuật mật mã - Quản lý khóa - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng*) và Phần 3 (TCVN 7817-3 : 2007, *Kỹ thuật mật mã - Quản lý khóa - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng*) của bộ TCVN đa thành phần này.

6.2 Phân phối khóa trong một miền

Mô hình sau dựa trên khái niệm về miền an toàn của bên có thẩm quyền an toàn theo ISO/IEC 10181-1. Cơ quan có thẩm quyền này có thể đưa ra các dịch vụ quản lý khóa chẳng hạn như trao đổi khóa. Khi một thực thể sử dụng kỹ thuật phi đối xứng để truyền thông tin mật thì có thể xẩy ra các trường hợp sau:

- Đối với trường hợp yêu cầu tính toàn vẹn dữ liệu hoặc xác thực nguồn gốc dữ liệu thì bên nhận phải có chứng chỉ khóa công khai tương ứng của bên gửi.
- Đối với trường hợp yêu cầu tính tin cậy thì bên gửi phải có chứng chỉ khóa công khai hợp lệ của bên nhận.
- Đối với trường hợp yêu cầu cả xác thực, tin cậy và toàn vẹn thì mỗi bên phải có chứng chỉ khóa công khai của bên kia. Điều này cung cấp cả khả năng chống chối bỏ.

Mỗi thực thể có thể muốn liên hệ với bên có thẩm quyền của nó để nhận được các chứng chỉ khóa công khai phù hợp. Nếu các đối tác truyền thông tin tưởng lẫn nhau và có thể xác thực chứng chỉ khóa công khai của nhau thì có thể không cần đến bên có thẩm quyền nữa.

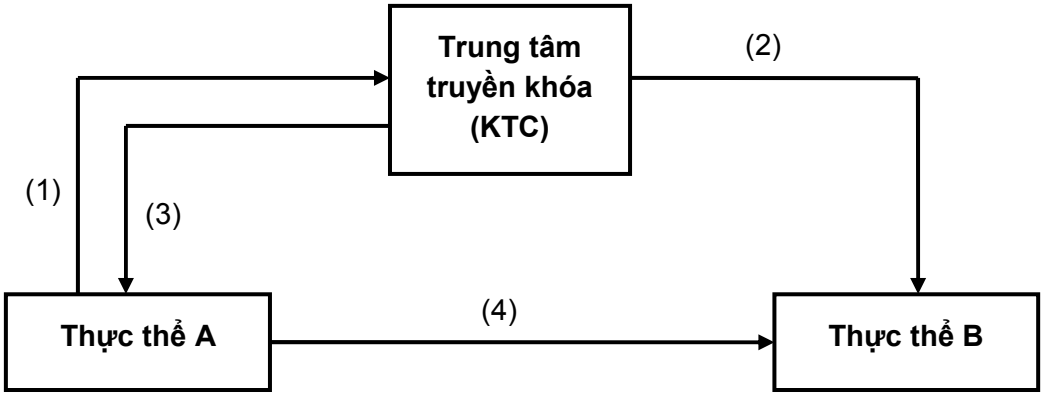
CHÚ THÍCH: Vẫn tồn tại các ứng dụng mật mã không cần đến các bên có thẩm quyền. Trong trường hợp này, mỗi đối tác truyền thông có thể chỉ trao đổi một cách an toàn thông tin công khai đặc biệt thay vì trao đổi chứng chỉ khóa công khai.

Khi sử dụng mật mã đối xứng giữa hai bên truyền thông thì quá trình sinh khóa được khởi tạo theo một trong hai cách sau:

1. Một thực thể tạo ra khóa và gửi nó cho Trung tâm truyền khóa (KTC);
2. Một thực thể yêu cầu Trung tâm phân phối khóa (KDC) tạo ra một khóa cho việc phân phối khóa tiếp theo.

Nếu thủ tục sinh khóa được thực hiện bởi một trong các thực thể thì việc phân phối an toàn khóa có thể được điều khiển bởi Trung tâm truyền khóa như minh họa ở Hình 4. Quá trình trao đổi khóa có thể diễn ra theo một số bước. KTC nhận một khóa đã được mã hóa từ thực thể A (1) rồi tiến hành giải mã nó sau đó lại mã tiếp bằng một khóa dùng chung giữa nó và thực thể B. Đến bước này KTC có thể thực hiện một trong hai cách sau:

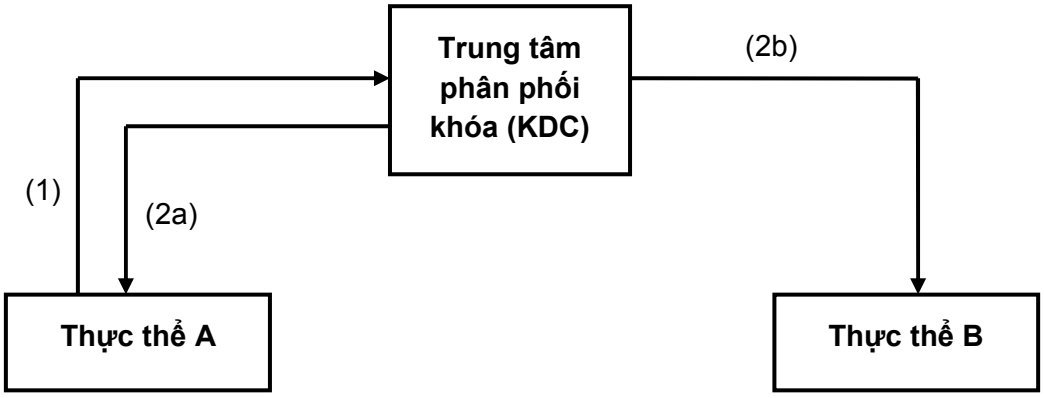
- Chuyển tiếp khóa được mã hóa đó đến thực thể B (2); hoặc
- Gửi khóa đó trở lại cho thực thể A để thực thể A gửi nó đến B (4).



Hình 4 – Trung tâm truyền khóa

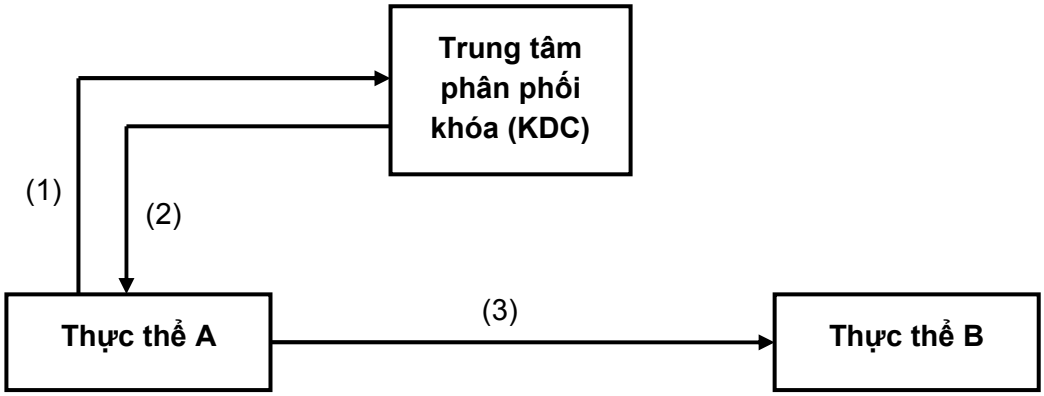
Nếu việc sinh khóa được thực hiện bởi bên thứ ba tin cậy thì có hai lựa chọn cho phân phối khóa tiếp theo giữa hai đối tác truyền thông đó là trường hợp minh họa ở Hình 5 – Mô hình mang tính khái niệm của Trung tâm phân phối khóa và Hình 6 – Phân phối khóa bằng cách chuyển tiếp một khóa từ thực thể A đến thực thể B.

Hình 5 minh họa về trường hợp một Trung tâm phân phối khóa có thể kết nối an toàn với cả hai thực thể. Trong trường hợp này, một khóa được sinh ra khi có yêu cầu của một trong hai thực thể, Trung tâm phân phối khóa sẽ có trách nhiệm phân phối an toàn khóa đến cả hai thực thể. Yêu cầu về một khóa dùng chung được trình bày bởi (1) và việc phân phối khóa đến hai thực thể truyền thông được thể hiện bởi (2a) và (2b).



Hình 5 – Mô hình mang tính khái niệm về Trung tâm phân phối khóa

Khi chỉ có thực thể A yêu cầu về một khóa dùng chung giữa A và B thì bên có thẩm quyền có thể hành động theo hai cách khác nhau. KTC có thể kết nối an toàn đến cả hai thực thể và phân phối an toàn một khóa mật cho cả hai thực thể như đã đề cập ở trên. Nhưng nếu bên có thẩm quyền chỉ kết nối được với A thì sao? Khi đó A sẽ chịu trách nhiệm phân phối khóa cho B. Hình 6 minh họa dạng phân phối khóa này. Yêu cầu về một khóa dùng chung thể hiện bởi (1), việc phân phối khóa cho A thể hiện bởi (2), chuyển tiếp khóa từ a đến b thể hiện bởi (3).



Hình 6 – Phân phối khóa bằng cách chuyển tiếp khóa từ A đến B

6.3 Phân phối khóa giữa nhiều miền

Mô hình thể hiện giữa hai thực thể có tên là A và B thuộc hai miền an toàn khác nhau cùng chia sẻ ít nhất một kỹ thuật mật mã (đối xứng hoặc phi đối xứng). Mỗi miền an toàn có một cơ quan có thẩm quyền về an toàn kết hợp với chúng, một bên được A tin cậy và một bên được B tin cậy. Nếu A và B tin cậy lẫn nhau thì khóa có thể được phân phối theo điều 6.1 và 6.2.

Có hai trường hợp phân biệt để thiết lập khóa giữa A và B:

- Dựa trên chứng chỉ khóa công khai của B (nếu có);
- Dựa trên sự thiết lập một khóa mật chia sẻ giữa A và B.

Các mối quan hệ về khóa khác nhau có thể xẩy ra giữa các thành phần này. Các quan hệ khóa này phản ánh một cách tự nhiên về sự tin cậy giữa các thành phần.

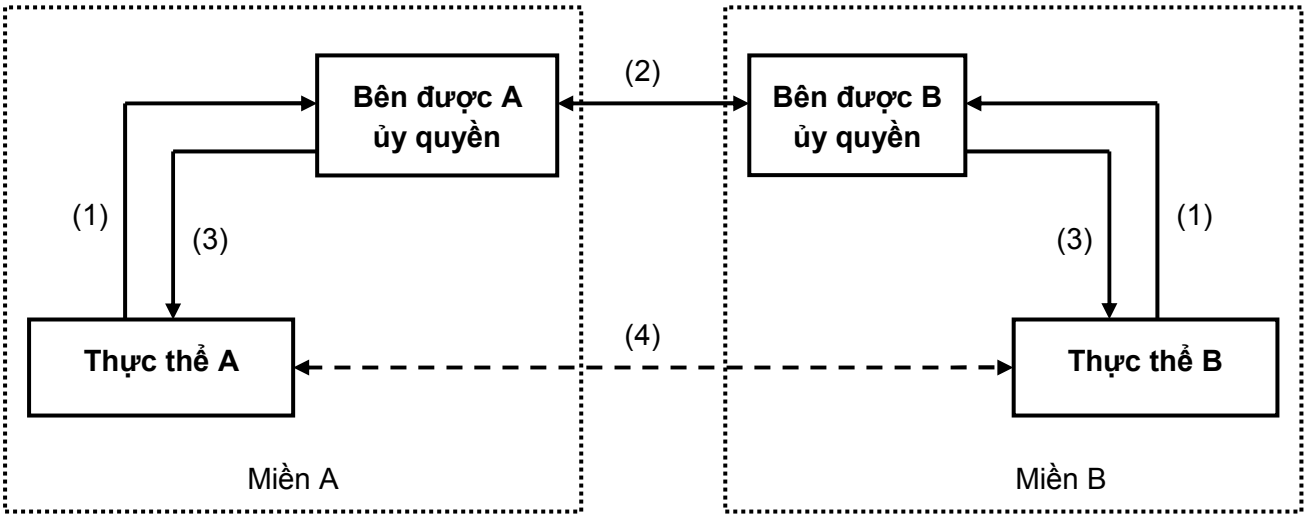
Khi các thực thể sử dụng một kỹ thuật phi đối xứng cho việc trao đổi thông tin và không truy cập đến một dịch vụ thư mục chung dùng để cất giữ các chứng chỉ khóa công khai thì mỗi bên có thể liên hệ với bên có thẩm quyền tương ứng của bên đó để nhận được chứng chỉ khóa công khai của đối tác (xem Hình 7 (1)). Bên có thẩm quyền của A và B thực hiện trao đổi chứng chỉ khóa công khai của A và B (2) rồi chuyển tiếp chúng đến cho A và B (3). Sau đó thì A và B có thể liên lạc bí mật và trực tiếp với nhau.

Một cách tiếp cận khác cho vấn đề trao đổi chứng chỉ khóa công khai là xác thực chéo (xem Phụ lục D).

Khi các thực thể liên lạc với nhau bằng kỹ thuật đối xứng thì mỗi thực thể đều liên hệ với bên có thẩm quyền an toàn tương ứng của mình (1) để nhận được một khóa mật cho phép chúng thực hiện truyền thông. Các bên có thẩm quyền sẽ thỏa thuận với nhau về một khóa mật (2) sử dụng bởi cả hai thực thể. Mỗi bên có thẩm quyền đều phân phối khóa bí mật đến cả hai thực thể bằng cách sử dụng bên có thẩm quyền còn lại như là một trung tâm phân phối. Bên có thẩm quyền thực hiện sau có thể sẽ phải thực hiện việc truyền khóa ((2) và (3)).

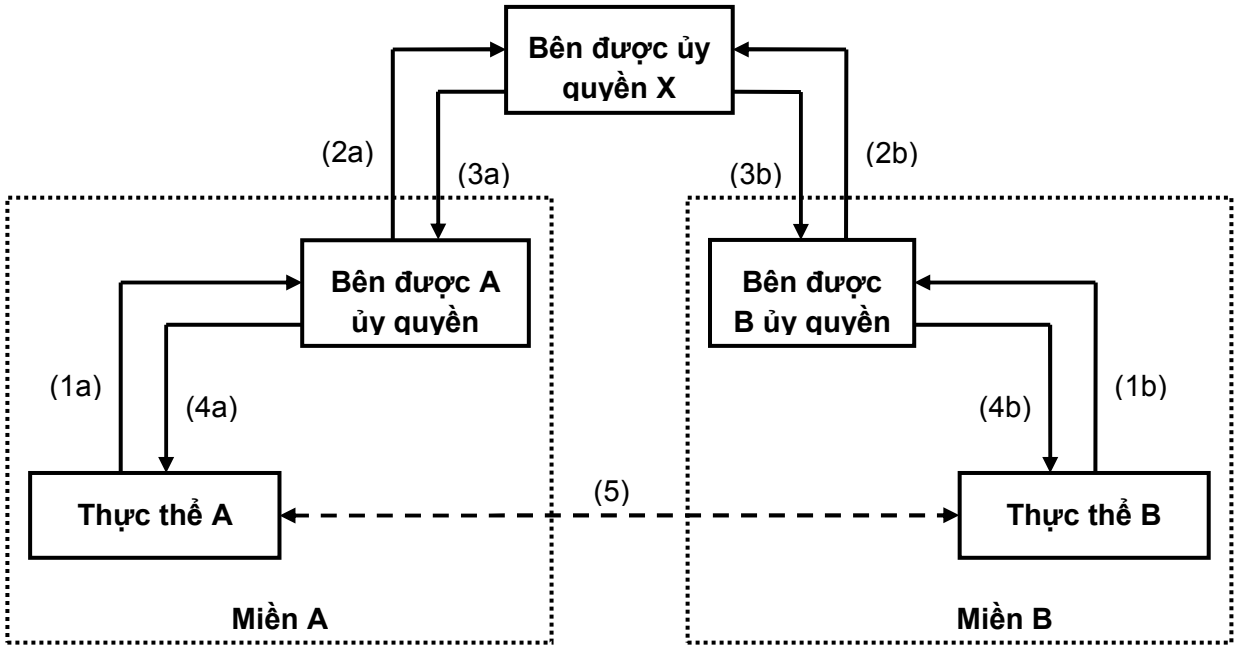
Khi A yêu cầu một khóa bí mật để truyền thông với B thì bên có thẩm quyền của A có thể hành động theo hai cách. Nếu nó có thể liên lạc với cả hai thực thể thì nó có thể phân phối một khóa mật cho cả

hai bên như đã mô tả ở phần trên. Nếu bên có thẩm quyền chỉ liên lạc được bởi một bên thì bên này sẽ nhận được khóa mật và có trách nhiệm chuyển tiếp cho bên còn lại.



Hình 7 – Phân phối khóa giữa hai miền

Đôi khi cả bên có thẩm quyền của A và bên có thẩm quyền của B không có quan hệ tin cậy lẫn nhau và cũng không liên lạc trực tiếp với nhau. Khi đó sẽ cần đến một bên có thẩm quyền X là bên được cả hai bên có thẩm quyền của A và B cùng tin cậy. Trường hợp này được minh họa ở Hình 8 (xem (2a) và (2b)). Bên có thẩm quyền X có thể sinh ra một khóa và phân phối nó cho bên có thẩm quyền của A và B (xem (3a) và (3b) ở Hình 8). Tương tự, bên được tin cậy X có thể chuyển tiếp một khóa mật hoặc một chứng chỉ khóa công khai nhận được (chẳng hạn ở (2a)) từ bên được A tin cậy đến bên được B tin cậy (3(b)). Các bên được tin cậy này sau đó lại chuyển tiếp khóa nhận được đến các thực thể tương ứng ((4a) và (4b) trong Hình 8) là những thành phần đang muốn trao dổi thông tin mật (5). Có thể cần phải tìm kiếm lần lượt các thực thể cho đến khi một chuỗi tin cậy được thiết lập.



Hình 8 – Chuỗi tin cậy giữa các bên được ủy quyền

7 Các nhà cung cấp dịch vụ chuyên dụng

Một số dịch vụ yêu cầu bởi một hệ thống quản lý khóa có thể được cung cấp bởi các nhà cung cấp dịch vụ ở bên ngoài. Các nhà cung cấp dịch vụ có thể là:

- Cơ quan chứng thực (CA) hoặc Cơ quan có thẩm quyền đăng ký khóa.
- Trung tâm phân phối khóa đề cập ở ISO/IEC 8732.
- Trung tâm truyền khóa đề cập ở ISO/IEC 8732.

Phụ lục A
(tham khảo)

Các nguy cơ đe dọa đối với Quản lý khóa

Việc quản lý khóa có thể nhạy cảm trước một số đe dọa sau đây:

- **Tiết lộ vật liệu khóa**: Vật liệu khóa ở dạng rõ hoặc không được bảo vệ có thể bị truy cập, thậm chí được mã hóa nhưng có thể bị giải mã.
- **Sửa đổi vật liệu khóa**: Thay đổi dữ liệu khóa làm cho nó hoạt động không như mong muốn.
- **Xóa bỏ trái phép vật liệu khóa**: Xóa bỏ khóa và thông tin liên quan đến khóa.
- **Không hủy bỏ hoàn toàn vật liệu khóa**: Có thể dẫn đến làm lộ khóa hiện tại hoặc sau này.
- **Thu hồi trái phép**: Loại bỏ trực tiếp hoặc gián tiếp khóa hoặc dữ liệu khóa đang sử dụng.
- **Giả mạo**: Mạo danh một thực thể hoặc người có thẩm quyền.
- **Chậm trễ thực thi các chức năng quản lý khóa**: Điều này có thể dẫn đến việc sinh khóa, phân phối, thu hồi hoặc đăng ký sai khóa, cập nhật khóa vào nơi chứa theo thời gian bị sai lạc, duy trì mức thẩm quyền của người dùng không đúng, … Nguy cơ đe dọa về chậm trễ có thể là kết quả từ bất kỳ các đe dọa nào đã đề cập trước đây hoặc từ các sai sót về mặt vật lý của thiết bị liên quan đến khóa.
- **Sử dụng khóa không đúng**:
    - Sử dụng khóa cho một mục đích mà nó không được ủy quyền, chẳng hạn sử dụng khóa dùng mã hóa khóa để mã hóa dữ liệu.
    - Sử dụng phương tiện quản lý khóa cho mục đích mà nó không được ủy quyền, chẳng hạn mã hóa hoặc giải mã dữ liệu không được phép.
    - Sử dụng các khóa đã hết hạn
    - Sử dụng khóa thái quá (nhiều lần).
    - Cung cấp khóa cho người nhận không có thẩm quyền.

Phụ lục B

(tham khảo)

Các đối tượng thông tin quản lý khóa

Một đối tượng thông tin quản lý khóa bao gồm một hoặc nhiều khóa và có thể kết hợp với một số thông tin điều khiển về cách sử dụng khóa. Thông tin điều khiển khóa thường ở dạng mặc nhiên hơn là chỉ ra chính xác về các quy ước điều khiển cách sử dụng đối tượng thông tin quản lý khóa. (Lấy ví dụ: việc sử dụng một khóa trong cặp khóa phi đối xứng của một bên được điều khiển bởi sự đồng ý của bên kia, một thành phần sử dụng cho mã hóa và một thành phần sử dụng cho giải mã).

Các thông tin điều khiển có thể là:

- Kiểu của đối tượng mà khóa được sử dụng để bảo vệ (là dữ liệu hoặc đối tượng thông tin quản lý khóa);
- Các thao tác hợp lệ (ví dụ: mã hóa, giải mã);
- Người dùng được phép;
- Môi trường nơi khóa được sử dụng;
- Các khía cạnh cụ thể khác tùy thuộc vào kỹ thuật điều khiển hoặc ứng dụng cụ thể sử dụng đối tượng thông tin quản lý khóa.

Việc tối ưu hóa đối tượng thông tin quản lý khóa có thể được thực hiện trên một phần hoặc toàn bộ một tiến trình sinh khóa.

Một ví dụ cụ thể về đối tượng thông tin quản lý khóa là một chứng chỉ. Nó bao gồm ít nhất các thành phần sau được ký bởi cơ quan chứng thực (CA):

- Vật liệu khóa;
- Định danh của người dùng có thể sử dụng đối tượng thông tin quản lý khóa tương ứng này;
- Các thao tác tương ứng với các thực thi của đối tượng thông tin quản lý khóa (có thể ở dạng ẩn);
- Thời gian hiệu lực;
- Định danh của cơ quan chứng thực (CA).

Một quy định về ASN.1 sau đây sẽ là ví dụ về một đối tượng thông tin quản lý khóa ở dạng một chứng chỉ. Tuy nhiên, một đối tượng thông tin quản lý khóa có thể bao gồm thêm một số thông tin hoặc các tham số thực thi cụ thể khác:

```
Key         ::= PROTECTED {KeyContents, protectionType};

KeyContents ::= SEQUENCE {

                keyID           [0]   Key_Identity,

                keyValue        [1]   Key_Value,

                checkValue      [2]   Check_Value,

                cryptoMethod    [3]   Cryptography_Method,

                timeStamp       [4]   Time_Stamp,

                generAuthority  [5]   Generating_Authority,

                certiAuthority  [6]   Certification_Authority,

                issuer          [7]   Issuer,

                validity        [8]   Validity_of_Key};
```

Chứng chỉ này bao gồm các tham số `Key_Identity` (một thẻ định danh cụ thể), `Key_Value` (giá trị của khóa) và `Check_Value` (giá trị kiểm tra tổng để đảm bảo về tính toàn vẹn của khóa) nhưng chỉ có `Key_Value` là giá trị bắt buộc phải có. Các tham số `Cryptography_Method`, `Issuer` và `Validity_of_Key` được sử dụng để giới hạn về thuật toán sử dụng, thời gian tối đa và người dùng cụ thể. Các tham số này tương đối quan trọng để điều khiển việc sử dụng khóa nhưng chúng là tùy chọn. Các tham số `Generating_Authority`, `Certification_Authority` và `Time_Stamp` cũng quan trọng, chúng dùng để minh chứng về nguồn gốc của khóa cũng như thời gian khóa đã sống tuy nhiên chúng cũng là tùy chọn. Đối với một chứng chỉ khóa thì tham số `Issuer` là bắt buộc..

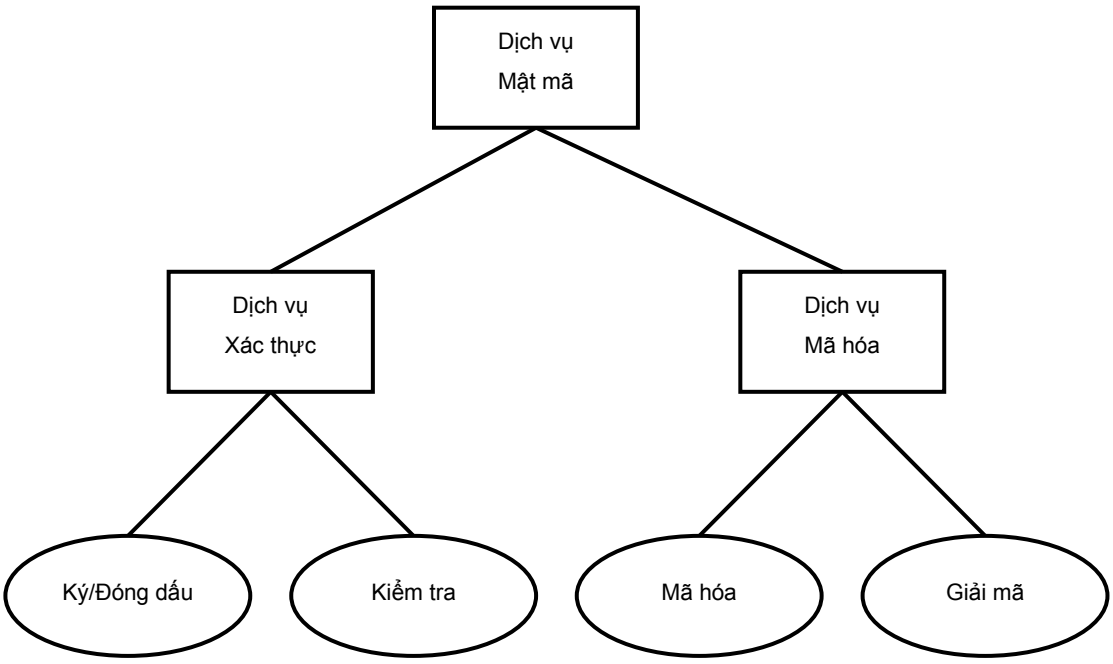
Phụ lục C

(tham khảo)

Phân lớp các ứng dụng mật mã

Cách phân lớp các hệ thống mật mã thường dựa vào hai kỹ thuật mật mã chính được sử dụng là đối xứng và phi đối xứng. Do công tác quản lý khóa phải đáp ứng cho cả hai kỹ thuật này có các hướng tiếp cận khác nhau cho nên việc phân lớp các hệ thống mật mã phải tuân theo tính năng cung cấp bởi từng kỹ thuật.

Nói chung, một hệ thống mật mã cung cấp hai loại hình dịch vụ khác nhau là các dịch vụ xác thực và các dịch vụ mã hóa. Các dịch vụ mã hóa được sử dụng để bảo vệ thông tin bằng mật mã, chẳng hạn như chúng có thể cung cấp tính bí mật cho dữ liệu. Các dịch vụ xác thực chủ yếu được sử dụng để xác thực thực thể, xác thực nguồn gốc, toàn vẹn dữ liệu và chống chối bỏ. Các loại hình hệ thống mật mã và thao tác tương ứng được minh họa trong Hình C-1.



Hình C-1 – Các dịch vụ mật mã và các cơ chế tương ứng

C.1 Khóa và các dịch vụ xác thực

Các dịch vụ xác thực cung cấp tính xác thực cho các thực thể truyền thông (xác thực thực thể), tính xác thực về nguồn của dữ liệu (xác thực nguồn gốc dữ liệu), tính không chối bỏ và toàn vẹn dữ liệu. Dịch vụ này có thể được sử dụng theo các cơ chế sau:

- **Đóng dấu một đơn vị dữ liệu**: Tạo ra một giá trị kiểm tra mật mã của dữ liệu cho mục đích toàn vẹn dữ liệu, chẳng hạn như tạo ra một mã xác thực thông điệp (MAC) bằng thuật toán đối xứng.
- **Ký một đơn vị dữ liệu**: Tạo ra một chữ ký số cho dữ liệu nhằm mục đích xác thực nguồn gốc dữ liệu, chống chối bỏ và/hoặc toàn vẹn dữ liệu.
- **Kiểm tra dấu được đóng đối với một đơn vị dữ liệu**: Tính toán về giá trị kiểm tra mật mã của dữ liệu và so sánh với giá trị kiểm tra tương ứng (chứng minh về tính toàn vẹn của dữ liệu).
- **Kiểm tra một đơn vị dữ liệu đã được ký**: Kiểm tra về chữ ký số để xác định xem là nó có được tạo ra bởi bên gửi hợp lệ hay không và/hoặc chứng minh cho tính toàn vẹn dữ liệu.

Trong một dịch vụ xác thực thì tiến trình ký và đóng dấu sử dụng thông tin bí mật (duy nhất và bí mật) của bên gửi hoặc chỉ được biết bởi bên gửi và bên nhận. Tiến trình kiểm tra sử dụng các thủ tục và thông tin công khai, tuy nhiên từ những thông tin này không thể suy luận ra thông tin bí mật của bên gửi hoặc thông tin bí mật được chia sẻ giữa bên gửi và bên nhận. Đặc điểm cơ bản của việc ký là chữ ký chỉ có thể được tạo ra với sự sử dụng thông tin bí mật của bên gửi gọi là *khóa bí mật*. Do đó khi một chữ ký được kiểm tra bằng cách sử dụng khóa công khai của bên gửi thì sau đó nó có thể được công nhận bởi bên thứ ba (chẳng hạn bên có tư cách pháp nhân) rằng bên duy nhất nắm giữ thông tin mật mới có thể tạo ra chữ ký.

Một dịch vụ xác thực sử dụng hai trong ba kiểu khóa sau:

- **Khóa dùng để đóng dấu**: Một khóa *bí mật*, chia sẻ.
- **Khóa dùng để ký**: Một khóa *bí mật*, duy nhất kết hợp với bên ký.
- **Khóa dùng để kiểm tra**: có thể là một khóa *công khai* hoặc một khóa *bí mật*.

Đối với kỹ thuật đối xứng thì dịch vụ xác thực sử dụng khóa để đóng dấu và khóa để kiểm tra là một khóa bí mật giống nhau. Đối với kỹ thuật phi đối xứng, sử dụng một khóa để ký và một khóa kiểm tra là một cặp khóa bao gồm một khóa bí mật và một khóa công khai.

C.2 Các dịch vụ mã hóa và Khóa

Các dịch vụ mã hóa chủ yếu cung cấp tính bí mật cho thông tin cũng như tính toàn vẹn của dữ liệu. Tùy thuộc vào kỹ thuật được sử dụng cho các dịch vụ an toàn mà tính xác thực và chống chối bỏ có thể cũng được sử dụng. Có hai cơ chế cơ bản sau đây:

- **Mã hóa**: Tạo ra các bản mã từ bản rõ đã cho;
- **Giải mã**: Tái tạo lại bản rõ từ bản mã tương ứng.

Một dịch vụ mã hóa có thể đặc trưng bởi kỹ thuật mật mã được sử dụng là đối xứng hay phi đối xứng. Khi sử dụng kỹ thuật đối xứng thì thao tác mã hóa và giải mã đều sử dụng chung một khóa (gọi là khóa chia sẻ). Khi sử dụng kỹ thuật phi đối xứng thì thao tác mã hóa và giải mã sử dụng hai khóa khác nhau nhưng có liên quan đến nhau là khóa công khai và khóa bí mật.

Phụ lục D
(tham khảo)

Quản lý vòng đời của chứng chỉ

Thông tin ở phụ lục này mô tả về các yêu cầu và thủ tục áp dụng cho việc quản lý vòng đời của một chứng chỉ khóa công khai.

D.1 Bên có thẩm quyền chứng thực

Một CA "được tin cậy" bởi các bên đăng ký với nó. Sự tin cậy này dựa trên việc sử dụng các cơ chế và thiết bị mật mã thích hợp đồng thời cũng dựa trên tính chuyên nghiệp trong quản lý và thực tế hoạt động. Tính tin cậy ở đây nên được xác nhận bởi một phương pháp kiểm toán (bên trong, bên ngoài hoặc cả hai) độc lập để đưa lại các kết quả kiểm toán luôn sẵn có đối với các bên đăng ký.

CA sẽ có trách nhiệm về các vấn đề:

1. Định danh các thực thể kết hợp với thông tin khóa công khai trong một chứng chỉ.
2. Đảm bảo chất lượng các cặp khóa phi đối xứng sử dụng để tạo ra chứng chỉ khóa công khai.
3. Bảo mật các tiến trình cấp chứng chỉ và khóa bí mật được sử dụng để ký thông tin khóa công khai.
4. Quản lý dữ liệu của một hệ thống cụ thể bao gồm trong thông tin khóa công khai như số serial của chứng chỉ khóa công khai, định danh nhà cung cấp chứng chỉ,…
5. Đưa ra và kiểm tra về khoảng thời gian sống cho phép.
6. Đưa ra thông báo cho thực thể được định danh trong thông tin khóa công khai rằng chứng chỉ khóa công khai đã được ban hành. Phương tiện để chuyển tải thông báo này phải độc lập với phương tiện sử dụng để chuyển tải thông tin khóa công khai đến CA.
7. Đảm bảo rằng hai thực thể khác nhau không được chỉ định cùng một định danh, nghĩa là phải hoàn toàn được phân biệt được hai thực thể khác nhau trong hệ thống.
8. Duy trì và ban hành các danh sách chứng chỉ đã bị thu hồi.
9. Ghi nhật ký về tất cả sự kiện liên quan đến quá trình tạo chứng chỉ khóa công khai.

Một CA có thể chứng thực thông tin khóa công khai của một CA khác để cung cấp một chứng chỉ khóa công khai. Do đó, việc xác thực có thể được thực hiện qua một chuỗi các chứng chỉ khóa công khai. Chứng chỉ khóa công khai đầu tiên của chuỗi sẽ nhận được và được xác thực bằng một số phương tiện khác ngoài các chứng chỉ khóa công khai.

D.1.1 Cặp khóa phi đối xứng của CA

CA sẽ có các phương tiện quản lý khóa an toàn để có thể tạo ra các cặp khóa phi đối xứng sử dụng bởi chính nó. Tiến trình sinh khóa này phải đảm bảo rằng dữ liệu khóa không thể bị đoán biết trước. Không có đối thủ nào có thể khai thác được lợi ích từ việc biết được tiến trình sinh khóa.

Khóa bí mật của CA được sử dụng để ký thông tin khóa công khai của các thực thể. Do đó có thể xẩy ra trường hợp một đối thủ sẽ mạo danh CA để tạo ra một chứng chỉ khóa công khai giả, vì thế khóa bí mật này luôn được bảo vệ ở mức cao. Khóa bí mật của CA phải được bảo vệ tốt khi sử dụng trong các phương tiện quản lý khóa. Nó nên được bảo vệ ở bên trong hoặc đưa cách ly khỏi các phương tiện quản lý khóa theo cách nào đó và phải được điều khiển bởi chính CA.

Tính toàn vẹn đối với khóa kiểm tra công khai của CA là nhân tố cơ bản về an toàn trong một hệ thống chứng chỉ khóa công khai. Nếu một khóa công khai của CA không được bao gồm trong chứng chỉ khóa công khai thì một sự đề phòng đặc biệt sẽ được thực hiện để đảm bảo rằng nó được phân phối có xác thực. Ở phía người dùng nên có sự đảm bảo về tính xác thực về bản sao khóa công khai của CA.

Khóa kiểm tra công khai của CA được sử dụng để xác minh các chứng chỉ khóa công khai đối với người dùng khác. Trước khi sử dụng khóa công khai của CA, mỗi người dùng nên chắc chắn rằng khóa kiểm tra còn hiệu lực.

D.2 Quy trình cấp chứng chỉ

Mục này mô tả về các yêu cầu và thủ tục áp dụng cho các tiến trình cấp chứng chỉ.

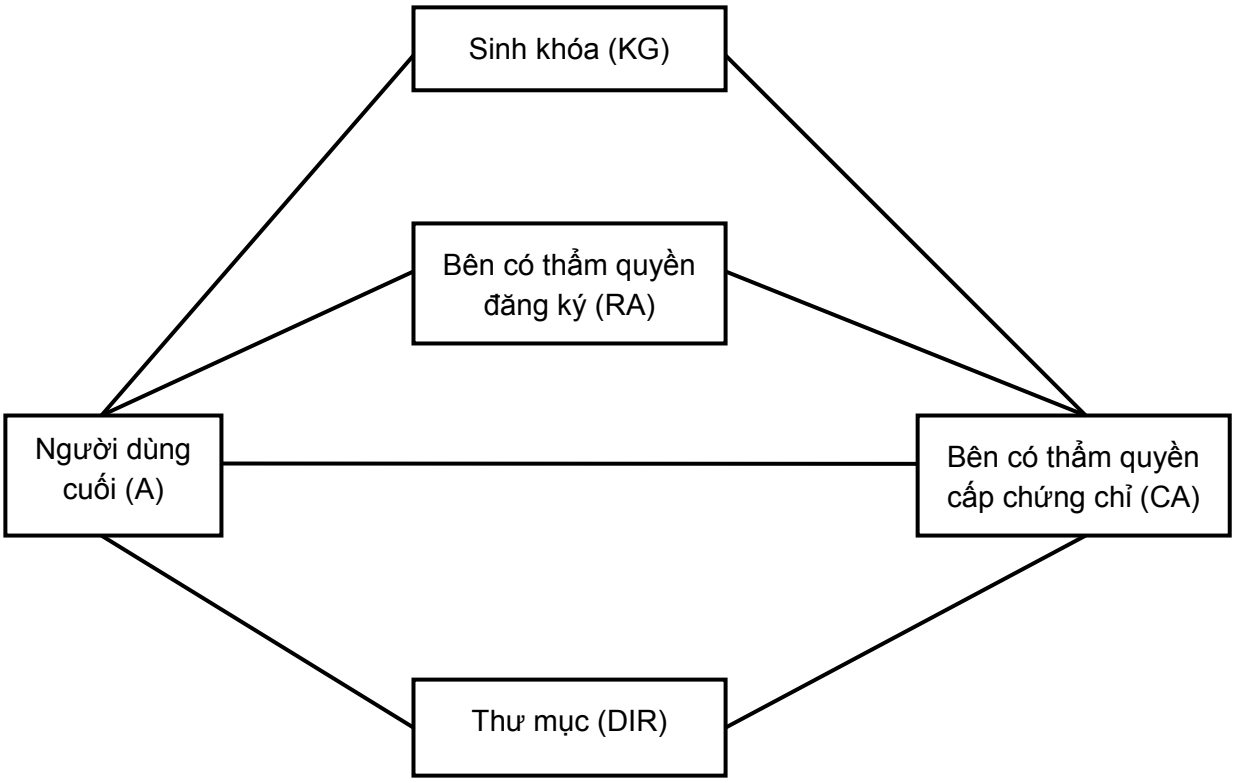
D.2.1. Mô hình chứng chỉ khóa công khai

Mục này đưa ra một mô hình tổng quát về việc chứng thực các khóa công khai. Mô hình này tách các chức năng chính thành các thực thể logic sau (xem Hình D-1):

1. Cơ quan chứng thực (CA): Là thực thể có trách nhiệm chứng thực thông tin khóa công khai của một thực thể người dùng cuối.
2. Thư mục (DIR): Là thực thể có trách nhiệm đưa các chứng chỉ khóa công khai trực tuyến để chúng luôn khả dụng đối với người dùng cuối.
3. Trình sinh khóa (KG): Thực thể có trách nhiệm tạo ra một cặp khóa phi đối xứng.
4. Bên có thẩm quyền đăng ký (RA): Thực thể có trách nhiệm cung cấp định danh người dùng cho CA.
5. Người dùng cuối (A).

Các mối quan hệ giữa các thực thể logic trong mô hình cũng như các yêu cầu an toàn trong các mối quan hệ này sẽ được thảo luận ở phần tiếp sau. Các thực thể logic có thể được kết hợp với nhau. Chẳng hạn, A và KG có thể chỉ là một thực thể khi người dùng tự tạo ra cặp khóa phi đối xứng, CA và KG có thể là một thực thể nếu CA tạo ra các cặp khóa nhân danh người dùng cuối.

CHÚ THÍCH: Trường hợp một chứng chỉ được tạo ra bởi một CA và RA là một thực thể kết hợp thì cũng tương tự như chứng chỉ được tạo ra bởi một CA và RA tách biệt nhau.



Hình D-1 – Mô hình cơ bản về Chứng chỉ khóa công khai

D.2.1.1 Các mối quan hệ trong việc cấp chứng chỉ

Mục này mô tả về một số mối quan hệ trong việc cấp chứng chỉ của mô hình cơ bản và các yêu cầu an toàn tương ứng. Trong một thực thi hệ thống thực tế không cần thiết phải có tất cả các mối quan hệ này. Chẳng hạn, các tác vụ của RA, CA và KG có thể được kết hợp làm một.

- **A – KG**: Khi thực thể A yêu cầu trình tạo khóa KG tạo ra cho nó một cặp khóa phi đối xứng. Khi đó, KG được tin cậy để tạo ra cặp khóa phi đối xứng có chất lượng cao. Trước hết, KG tạo ra một cặp khóa là (s_A,v_A) với s_A là khóa để ký và v_A là khóa để kiểm tra rồi gửi đến A. Việc truyền cặp khóa này có thể được thực hiện theo cách nào đó sao cho đảm bảo được sự bảo mật và xác thực. KG và A hoàn toàn chắc chắn rằng sẽ không có bên thứ ba nào có thể sửa đổi hoặc đọc được giá trị của cặp khóa phi đối xứng trong quá trình truyền.
- **A – RA:** Khi thực thể A yêu cầu một sự đăng ký từ Bên có thẩm quyền đăng ký RA thì A sẽ đệ trình thông tin định danh của nó cho RA. RA kiểm tra tính xác thực thông tin của A và có thể đưa thông tin này vào dữ liệu hệ thống của nó. Tiếp đó thông tin này được chuyển tiếp đến CA theo một cách an toàn.

- **A – CA:** Khi thực thể A yêu cầu Cơ quan chứng thực CA cấp một thông tin khóa công khai (hoặc một tập con của thông tin này) bao gồm khóa công khai và tên phân biệt của A thì thông tin về khóa công khai sẽ được gửi đến CA theo cách nào đó đảm bảo rằng có thể tin cậy và xác thực. CA kiểm tra tính xác thực về thông tin khóa công khai của A và có thể bổ sung thêm một số dữ liệu hệ thống rồi ký thông tin khóa công khai hoàn chỉnh này để tạo nên một chứng chỉ khóa công khai. Chứng chỉ khóa công khai này sau đó có thể được truyền đến cho A.

  Dựa vào chứng chỉ khóa công khai nhận được, A kiểm tra tính đúng đắn bằng cách dùng khóa kiểm tra công khai v_{CA} của CA. Khóa kiểm tra công khai v_{CA} của CA này được bố trí sao cho luôn khả dụng đối với A theo một cách có xác thực nào đó. Từ đây khóa công khai của A có thể được phân phối ở dạng một chứng chỉ khóa công khai và có thể được dùng bởi bất cứ ai có quyền truy cập vào khóa kiểm tra công khai của CA.

  Nếu CA yêu cầu KG tạo ra một cặp khóa phi đối xứng nhân danh A thì cặp khóa được tạo ra cho A sẽ được gửi từ KG đến A theo con đường bí mật, toàn vẹn và có xác thực. Ngoài ra, CA còn được tin cậy để duy trì tính bí mật, tin cậy và xác thực cho tất cả các cặp khóa phi đối xứng trong suốt quá trình xử lý và cất giữ. Cuối cùng, CA sẽ truyền khóa bí mật của A đến cho A theo cách nào đó đảm bảo rằng không bất cứ bên thứ ba nào có thể sửa đổi và đọc được dữ liệu được truyền.

- **A – DIR**: Thực thể A truyền chứng chỉ khóa công khai của nó đến Thư mục DIR và đăng ký chứng chỉ này vào danh mục. Khi đăng ký chứng chỉ vào thư mục các chứng chỉ phải đảm bảo được tính xác thực thực thể và điều khiển truy cập. Có thể cần phải có sự thỏa thuận giữa A và DIR rằng ai là người có quyền quản lý mục chứng chỉ này trên thư mục. Trong một số ứng dụng, DIR quản lý tất cả các mục thuộc thư mục chứng chỉ nhưng trong một số ứng dụng khác thì mỗi thực thể X sẽ chịu trách nhiệm quản lý chứng chỉ của mình trên thư mục.

- **RA - CA:** RA yêu cầu CA chứng thực về thông tin khóa công khai của A. Thông tin khóa công khai của A được truyền từ RA đến CA theo đường truyền có xác thực. CA kiểm tra tính xác thực của A và có thể thêm vào một số dữ liệu hệ thống rồi ký thông tin khóa công khai hoàn chỉnh này để tạo ra một chứng chỉ khóa công khai cho A. CA thông báo cho RA biết về quá trình chứng thực này.

- **CA – KG:** Trong trường hợp CA yêu cầu KG tạo ra một cặp khóa phi đối xứng nhân danh thực thể A. Khi đó, KG được tin cậy để tạo ra các cặp khóa phi đối xứng có chất lượng cao. KG sẽ thực hiện tạo ra một cặp khóa phi đối xứng rồi gửi đến cho CA theo cách có bảo mật và xác thực. KG và CA hoàn toàn chắc chắn rằng sẽ không có bất cứ bên thứ ba nào có thể sửa đổi hoặc đọc được dữ liệu trong quá trình truyền. CA đảm bảo tính bí mật và xác thực hoàn toàn cho tất cả các cặp khóa phi đối xứng trong suốt quá trình xử lý và cất giữ.

- **CA – DIR:** CA truyền các chứng chỉ khóa công khai được tạo ra trực tiếp đến cho Thư mục DIR và đăng ký chúng vào thư mục. Xác thực thực thể và điều khiển truy cập là hai yêu cầu cần đảm bảo cho việc đăng ký các chứng chỉ khóa công khai vào thư mục.

D.2.2 Đăng ký

Tiến trình đăng ký khóa của một thực thể là việc yêu cầu đệ trình chứng chỉ của thực thể đó cùng với sự xem xét của RA và CA. Các mục sau đây minh họa về các yêu cầu áp dụng cho việc đệ trình một yêu cầu chứng chỉ của một thực thể. Yêu cầu chứng chỉ có thể có hoặc không bao gồm giá trị khóa công khai.

D.2.2.1 Đệ trình một yêu cầu xin cấp chứng chỉ cho cá nhân

Đối với các ứng dụng có độ rủi ro thấp, việc chấp nhận một yêu cầu cấp chứng chỉ nên dựa trên định danh duy nhất áp dụng cho một chứng chỉ khóa công khai. Các yêu cầu cấp chứng chỉ không cần phải trình bày thông tin về nhân thân nhưng phải có các thông tin về thực tế công việc hợp lý để có thể sử dụng cho việc định danh duy nhất.

Đối với các ứng dụng có độ rủi ro cao, việc chấp nhận một yêu cầu cấp chứng chỉ nên dựa trên sự hiện diện của người muốn có (hoặc người được ủy quyền) duy nhất chứng chỉ khóa công khai và sựa trên việc sử dụng các tiêu chuẩn thương mại hợp lý để định danh người dùng (và cơ quan mà người đó công tác nếu được yêu cầu). Có thể thực hiện việc kiểm tra định danh này bằng một thực thể thứ ba được tin cậy.

D.2.2.2 Đệ trình một yêu cầu xin cấp chứng chỉ cho thực thể có tư cách pháp nhân

Việc chấp nhận một yêu cầu xin cấp chứng chỉ trong trường hợp này nên dựa trên sự chuyển giao trực tiếp thông tin yêu cầu chứng chỉ của ít nhất một đại diện thuộc thực thể có yêu cầu và:

1. Ký hoặc đóng dấu (nếu cần) của người đứng đầu tổ chức cho phép áp dụng một chứng chỉ khóa công khai,
2. Sử dụng các thông lệ thương mại hợp lý để định danh chữ ký hoặc con dấu (nếu thích hợp) của thực thể.
3. Sử dụng thông lệ thương mại hợp lý để định danh cho đại diện nhận thông tin yêu cầu xin cấp chứng chỉ.

D.2.3 Các mối quan hệ giữa các thực thể có tư cách pháp nhân

Có một yêu cầu đối với các thực thể có tư cách pháp nhân trong quan hệ hợp đồng với các thực thể có tư cách pháp nhân khác. Điều này có thể tùy thuộc vào các trường hợp nhau sau đây:

1. Nhân viên của công ty có các cặp khóa phi đối xứng dành cho cá nhân. Thực thể có tư cách pháp nhân hoạt động như một CA đối với các nhân viên thuộc công ty. Các giao tác được ủy quyền bởi các cá thể sử dụng các khóa cá nhân đã được chứng thực bởi CA của công ty. Bên nhận sẽ kiểm tra xem bên gửi có được chứng thực bởi công ty hay không, khóa công khai của CA tại công ty lại được chứng thực bởi CA cao hơn.
2. Nhân viên công ty không có cặp khóa phi đối xứng dành cho cá nhân. Chỉ có thực thể có tư cách pháp nhân mới có một hoặc một số cặp khóa phi đối xứng. Bên nhận sẽ kiểm tra xem các

thao tác chuyển trạng thái có phù hợp với khóa công khai của công ty hay không. Bên nhận không cần phải bận tâm đến các chính sách và đặc quyền được chỉ định của công ty gửi đến.

D.2.4 Tạo chứng chỉ

Tiến trình tạo chứng chỉ khóa công khai sẽ xẩy ra trước bất cứ thao tác sử dụng cặp khóa phi đối xứng nào.

Một tiến trình tạo chứng chỉ khóa công khai cần thực hiện mấy bước sau:

1. Kiểm tra phát hiện lỗi đối với thông tin khóa công khai.
2. Chấp nhận thông tin khóa công khai: Các yêu cầu chấp nhận thông tin khóa công khai đã được đưa ra trong phần đăng ký khóa ở trên.
3. Chuẩn bị và bổ sung dữ liệu được yêu cầu dùng cho quản lý chứng chỉ khóa công khai. Tùy trường hợp, CA có thể tạo ra một hoặc một số cặp khóa phi đối xứng cho thực thể.
4. Tính toán và ký chứng chỉ khóa công khai. Điều này có thể thực hiện bằng hàm băm.
5. Kiểm toán các mục nhật ký. Các hành động của CA trong quá trình tạo chứng chỉ khóa công khai nên được ghi lại.

Đối với các ứng dụng có độ rủi ro cao thì yêu cầu (1) có thể đòi hỏi có nhiều chữ ký lên chứng chỉ khóa công khai bởi CA, các chữ ký thực hiện trong các phương tiện độc lập nhau (đối với các khóa bí mật khác nhau) hoặc (2) yêu cầu nhiều chữ ký trên thông tin khóa công khai bởi các CA khác nhau.

D.2.5 Làm mới/Thời gian sống

Một chứng chỉ khóa công khai có vòng đời là thời gian sống hợp lệ được bắt đầu trong chứng chỉ khóa công khai hoặc được đưa ra bởi sự quản lý của CA.

D.3 Phân phối và sử dụng chứng chỉ khóa công khai

Mục này mô tả về các yêu cầu và thủ tục áp dụng để phân phối và sử dụng các chứng chỉ khóa công khai.

D.3.1 Phân phối và cất giữ chứng chỉ khóa công khai

Khi một chứng chỉ khóa công khai được tạo ra thì không có phương pháp đo lường đặc biệt nào có thể đảm bảo được tính bí mật hoặc toàn vẹn dữ liệu của chứng chỉ đó. Các chứng chỉ khóa công khai có thể được cất giữ ở một thư mục công khai để tạo điều kiện dễ dàng trong truy cập đối với người dùng.

D.3.2 Kiểm tra chứng chỉ khóa công khai

Để kiểm tra một chứng chỉ khóa công khai, thực thể tiến hành kiểm tra B sẽ thực hiện ít nhất một phép kiểm tra chữ ký của CA trên chứng chỉ khóa công khai. Nếu chứng chỉ khóa công khai này hợp lệ thì B sẽ được đảm bảo rằng thông tin khóa công khai của thực thể A là vẫn còn hợp lệ (xem phần D.5 – Thu

hồi chứng chỉ). Để kiểm tra chứng chỉ khóa công khai, bên kiểm tra sẽ sở hữu một bản sao của khóa kiểm tra chứng chỉ cung cấp bởi CA.

D.4 Đường dẫn chứng chỉ

Tất cả CA không cần phải biết nhau và chứng thực lẫn nhau và cũng không cần có một sự phân cấp rõ ràng nào về các CA. Điều này tương tự như việc các CA chứng thực lẫn nhau (chứng thực chéo) để cho phép sự mềm dẻo khi sử dụng và trao đổi các chứng chỉ khóa công khai. Quá trình chứng thực chéo nên được thực hiện dựa trên các mức đảm bảo cao và mã thực hành cẩn trọng. Khi một mạng tồn tại các chứng chỉ chứng thực chéo thì các đường dẫn để kiểm tra các chứng chỉ khóa công khai có thể được tạo ra. Một người dùng chỉ cần có sự tin cậy vào sự hợp lệ của khóa cung cấp bởi một CA. Sự tin cậy này sau đó được mở rộng thông qua đường dẫn chứng thực để ban hành một khóa công khai của đối tác bằng một CA chưa biết.

D.5 Thu hồi chứng chỉ

Các chứng chỉ có thể bị thu hồi trước thời gian tới hạn bởi bên ban hành CA. Điều này có thể xẩy ra bởi một số lý do sau đây:

1. Khóa bí mật của một thực thể bị tổn thương,
2. Một thực thể yêu cầu hủy bỏ chứng chỉ,
3. Có sự thay đổi sát nhập của một thực thể,
4. Một thực thể chấm dứt hoạt động,
5. Định danh sai về một thực thể,
6. Khóa bí mật của CA bị tổn thương,
7. CA ngừng cung cấp dịch vụ.

Tùy theo từng trường hợp mà các thủ tục và phương tiện truyền thông nhanh chóng sẽ được thực hiện để hủy bỏ theo cách an toàn và có xác thực:

1. Một hoặc một số chứng chỉ khóa công khai của một hoặc một số thực thể,
2. Một tập bao gồm tất cả chứng chỉ đã được phát hành bởi một CA dựa trên một cặp khóa phi đối xứng sử dụng cho CA để ký các thông tin khóa công khai,
3. Tất cả chứng chỉ khóa công khai phát hành bởi một CA mà không quan tâm đến phương thức cặp khóa phi đối xứng được sử dụng.

Trường hợp (2) và (3) cung cấp phương tiện để hủy bỏ các chứng chỉ khóa công khai khi có sự tổn thương hoặc nghi ngờ bị tổn thương khóa bí mật của CA hoặc khi cặp khóa phi đối xứng dùng để ký các chứng chỉ khóa công khai bị thay đổi. Khi các chứng chỉ khóa công khai hết hạn hoặc bị hủy bỏ thì một bản sao của chứng chỉ khóa công khai cũ sẽ được tiến hành bởi một bên thứ ba tin cậy trong một thời gian nhất định nhằm đảm bảo tính cẩn trọng cho thực tế công việc, pháp luật và quy định.

Khi một khóa bí mật của một thực thể hoặc một CA bị hủy bỏ vì bất cứ lý do gì thì CA sẽ phát hành ngay lập tức một chứng chỉ khóa công khai mới thay thế và báo cho tất cả thực thể trong hệ thống về tất cả các chứng chỉ khóa công khai tương ứng vừa bị hủy bỏ. Điều này có thể thực hiện bằng các cách: CA gửi một thông điệp có xác thực đến tất cả thực thể; nhờ một CA khác gửi một thông điệp có xác thực đến tất cả thực thể; duy trì một danh sách trực tuyến về tất cả chứng chỉ khóa công khai đã bị thu hồi bởi một bên thứ ba tin cậy; phát hành một danh sách các chứng chỉ khóa công khai đã bị thu hồi hoặc còn hiệu lực.

Khi một chứng chỉ khóa công khai bị thu hồi do tổn thương hoặc nghi ngờ bị tổn thương khóa bí mật thì khóa bí mật này không được dùng tiếp nữa. Khóa công khai trong trường hợp này chỉ được sử dụng cho mục đích kiểm tra và cũng chỉ để kiểm tra dữ liệu được ký trước thời điểm bị thu hồi. Sau đó bất cứ dữ liệu khóa nào được mã hóa bằng chứng chỉ khóa công khai này (dưới bất cứ hình thức nào) đều nên ngừng sử dụng ngay lập tức.

Khi một chứng chỉ khóa công khai hết hạn hoặc bị thu hồi vì lý do khác với lý do bị tổn thương hoặc nghi tổn thương khóa bí mật thì khóa bí mật cũng không được sử dụng tiếp nữa. Khóa công khai tương ứng trong trường hợp này cũng chỉ dùng cho mục đích kiểm tra hoặc giải mã. Tất cả dữ liệu khóa được gửi và được bảo vệ bởi chứng chỉ khóa công khai này (dưới bất cứ hình thức nào) đều nên được thay thế càng sớm càng tốt.

D.5.1 Danh sách thu hồi

Một danh sách thu hồi bao gồm một danh sách được đánh dấu về thời gian của một loạt định danh chứng chỉ khóa công khai cho biết các chứng chỉ khóa công khai đó đã bị thu hồi bởi CA. Có hai dạng gắn tem thời gian có thể sử dụng trong danh sách thu hồi:

1. Ngày tháng và thời gian mà CA ban hành lệnh thu hồi,
2. Ngày tháng và thời gian phát hiện hoặc nghi ngờ bị tổn thương.

Giá trị ngày tháng dễ dàng được đưa ra theo dấu kiểm toán của thông điệp bị nghi ngờ. Chứng chỉ khóa công khai được giữ lại trong danh sách thu hồi ít nhất cho đến khi nó hết hạn dùng. Tem thời gian là một mốc thời gian nào đó, nó cho biết về thời điểm mà chứng chỉ khóa công khai của một thực thể bị thu hồi.

Trong trường hợp xẩy ra thu hồi khi phát hiện hoặc nghi ngờ bị tổn thương thì thông tin được ký sử dụng khóa bí mật kết hợp sẽ không được thừa nhận là còn hợp lệ nếu chữ ký được thực hiện sau thời gian nghi ngờ bị tổn thương hoặc nếu thời gian ký thật sự không xác định được. Thông tin sẽ không thể mã hóa bằng cách sử dụng một khóa công khai đã được thu hồi.

Một danh sách thu hồi sẽ:

1. Được gắn ngày tháng và ký bởi CA vì thế các thực thể có thể kiểm tra tính toàn vẹn của danh sách và ngày tháng ban hành,
2. Ban hành bởi CA trong thời gian quy định kể cả khi không có bất cứ sự thay đổi nào xẩy ra kể từ thời điểm ban hành gần nhất,

3. Tất cả thực thể đều có thể truy cập trừ trường hợp có sự hạn chế của phát luật, quy định hoặc của tòa án,…

Một số cơ chế phân phối khác có thể thực hiện cho danh sách thu hồi như:

- Gửi đến mỗi người dùng một thông điệp/thao tác chuyển trạng thái bởi bên thứ ba tin cậy,
- Người dùng yêu cầu bên thứ ba tin cậy cho biết trạng thái hiện tại của một chứng chỉ khóa công khai,
- Truy vấn CA về danh sách thu hồi hiện tại của nó.

CA sẽ công bố và phân phối một danh sách thu hồi theo định kỳ.

Phụ lục E
(tham khảo)

Tài liệu tham khảo

1. ISO 8732:1998, *Banking – Key management (wholesale)* (*Ngân hàng - Quản lý khóa (dùng cho quy mô lớn)).*

2. ISO/IEC 9594:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework (Công nghệ thông tin – Liên kết các hệ thống mở - Thư mục - Phần 8: Khung xác thực).*

3. ISO/IEC 10116:1991, *Information technology – Modes of operation fot an n-bit block cipher algorithm (Công nghệ thông tin – Các chế độ hoạt động của thuật toán mã khối n bít).*

4. ISO 11166-1:1994, *Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats (Ngân hàng - Quản lý khóa bằng phương tiện thuật toán phi đối xứng - Phần 1: Nguyên lý, thủ tục và định dạng).*

5. ISO 11568-1: 1994, *Banking – Key management (retail) – Part 1: Introduction to key management (Ngân hàng - Quản lý khóa (dùng cho quy mô nhỏ) - Phần 1: Giới thiệu về quản lý khóa).*

6. ISO 11568-2: 1994, *Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers (Ngân hàng - Quản lý khóa (dùng cho quy mô nhỏ) - Phần 2: Các kỹ thuật quản lý khóa dùng cho hệ mật đối xứng)*.

7. ISO 11568-3: 1994, *Banking – Key management (retail) – Part 3: Key life cycle for symmetric ciphers (Ngân hàng - Quản lý khóa (dùng cho quy mô nhỏ) - Phần 3: Vòng đời khóa của hệ mật đối xứng).*

8. ISO 11568-4, *Banking – Key management (retail) – Part 4: Key management techniques for public key cryptosystems (Ngân hàng - Quản lý khóa (dùng cho quy mô nhỏ) - Phần 4: Các kỹ thuật quản lý khóa cho hệ thống khóa công khai).*

9. ISO 11568-5, *Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems (Ngân hàng - Quản lý khóa (dùng cho quy mô nhỏ) - Phần 5: Vòng đời khóa của hệ thống khóa công khai).*

10. ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques (Công nghệ thông tin – Kỹ thuật mật mã -*

Quản lý khóa - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng).

11. ISO/IEC 11770-3, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques (Công nghệ thông tin – Kỹ thuật mật mã - Quản lý khóa - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng).*

12. ISO/IEC 13888, *Information technology – Security requirements – Non-repudiation (all parts) (Công nghệ thông tin – Các yêu cầu an toàn - Chống chối bỏ (tất cả các phần)).*