TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 11393-1:2016
ISO/IEC 13888-1:2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - CHỐNG CHỐI BỎ - PHẦN 1: TỔNG QUAN

Information technology - Security techniques - Non-repudiation - Part 1: General

HÀ NỘI - 2016

Mục lục

Lời nói đầu

TCVN 11393-1:2016 hoàn toàn tương đương tiêu chuẩn ISO/IEC 13888-1:2009.

TCVN 11393-1:2016 do Trung tâm Ứng cứu Khẩn cấp máy tính Việt Nam và Học viện Công nghệ Bưu chính Viễn thông biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11393 gồm 03 phần:

- TCVN 11393-1:2016, Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan
- TCVN 11393-2:2016, Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng
- TCVN 11393-3:2016, Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.

Lời giới thiệu

Mục đích của một dịch vụ chống chối bỏ là tạo ra, thu thập, duy trì, sẵn sàng cung cấp và xác minh bằng chứng liên quan đến một sự kiện hay hành động đã yêu cầu nhằm giải quyết tranh chấp về sự xuất hiện hay không xuất hiện của sự kiện hay hành động. Phần này của bộ tiêu chuẩn TCVN 11393 (ISO/IEC 13888) xác định một mô hình cho các cơ chế chống chối bỏ cung cấp bằng chứng dựa trên các giá trị kiểm tra mật mã đã tạo ra bằng các kỹ thuật mật mã đối xứng và phi đối xứng.

Các dịch vụ chống chối bỏ thiết lập bằng chứng; bằng chứng thiết lập trách nhiệm liên quan đến một sự kiện hay hành động cụ thể. Thực thể chịu trách nhiệm về hành động, hay liên quan đến sự kiện mà bằng chứng được tạo ra liên quan đến nó, được coi là chủ thể bằng chứng.

Các cơ chế chống chối bỏ cung cấp các giao thức cho việc trao đổi các thẻ chống chối bỏ đặc trưng cho mỗi dịch vụ chống chối bỏ. Các thẻ chống chối bỏ bao gồm các vỏ bọc bảo vệ và/hoặc chữ ký số và có thể cả dữ liệu bổ sung:

- Các vỏ bọc bảo vệ được tạo ra bởi một tổ chức tạo ra chứng cứ bằng các kỹ thuật mật mã đối xứng.
- Các chữ ký số được tạo ra bởi một bộ tạo bằng chứng hoặc một tổ chức tạo ra chứng cứ bằng các kỹ thuật mật mã phi đối xứng.

Các thẻ chống chối bỏ có thể được lưu ở dạng thông tin chống chối bỏ, có thể sử dụng tiếp đó bởi các bên tranh chấp hay bởi một tòa án nhằm phân xử trong tranh chấp.

Tùy thuộc vào chính sách chống chối bỏ hiện hành cho một ứng dụng cụ thể và môi trường pháp lý trong đó ứng dụng hoạt động, thông tin bổ sung có thể được yêu cầu để hoàn thiện thông tin chống chối bỏ, ví dụ:

- Bằng chứng bao gồm tem thời gian tin cậy được cung cấp bởi một tổ chức cấp tem thời gian,
- Bằng chứng được cung cấp bởi một công chứng viên, đưa ra một sự bảo đảm về dữ liệu đã được tạo ra hay một hành động hoặc sự kiện đã được thực thi bởi một hoặc nhiều thực thể.

Chống chối bỏ có thể chỉ được đưa ra trong ngữ cảnh một chính sách an toàn thông tin đã xác định rõ cho một ứng dụng cụ thể và môi trường pháp lý của nó. Các chính sách chống chối bỏ được mô tả trong ISO/IEC 10181-4.

Các cơ chế chống chối bỏ chung cho các dịch vụ chống chối bỏ khác nhau trước hết được mô tả, sau đó được áp dụng cho một phần các dịch vụ chống chối bỏ như:

- chống chối bỏ nguồn gốc,
- chống chối bỏ việc chuyển phát,
- chống chối bỏ việc đệ trình,
- chống chối bỏ việc vận chuyển.

Các dịch vụ chống chối bỏ bổ sung đã đề cập trong phần này của bộ tiêu chuẩn này gồm:

- chống chối bỏ việc tạo lập,
- chống chối bỏ việc nhận,
- chống chối bỏ sự hiểu biết,
- chống chối bỏ việc gửi.

Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan

Information technology - Security techniques - Non-repudiation - Part 1: General

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra một mô hình chung cho các phần tiếp theo của bộ tiêu chuẩn TCVN 11393 đặc tả các cơ chế chống chối bỏ sử dụng các kỹ thuật mật mã. Bộ tiêu chuẩn TCVN 11393 cung cấp các cơ chế chống chối bỏ cho các giai đoạn chống chối bỏ sau đây:

- Tạo bằng chứng;
- Chuyển giao, lưu trữ và thu hồi bằng chứng;
- Xác minh bằng chứng.

Việc phân xử tranh chấp về bằng chứng nằm ngoài phạm vi của bộ tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có).

ISO/IEC 10181-4:1997 Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework *(Công nghệ thông tin - Liên kết hệ thống mở - Bộ khung an toàn cho các hệ thống mở: Bộ khung chống chối bỏ).*

TCVN 7818 (tất cả các phần) (ISO/IEC 18014) Công nghệ thông tin - Kỹ thuật mật mã – Dịch vụ tem thời gian.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau.

3.1

Trách nhiệm giải trình (accountability)

Thuộc tính bảo đảm rằng các hành động của một thực thể có thể được truy vết duy nhất tới thực thể đó.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.2

Chứng thư (certificate)

Dữ liệu của thực thể được trao nộp không thể giả mạo với khóa riêng hoặc khóa bí mật của một tổ chức chứng thực.

3.3

Tổ chức chứng thực (certification authority)

Tổ chức được tin cậy bởi một hay nhiều người sử dụng để tạo ra và cấp chứng thư.

CHÚ THÍCH 1: Trích chọn từ ISO/IEC 9594-8:2011, 3.3.17.

CHÚ THÍCH 2: Theo tùy chọn, tổ chức chứng thực có thể tạo các khóa của người dùng.

3.4

Hàm kiểm tra mật mã (cryptographic check function)

Phép biến đổi mật mã nhận đầu vào là một khoá bí mật và một chuỗi tuỳ ý, cho đầu ra là một giá trị kiểm tra mật mã.

3.5

Tính toàn vẹn dữ liệu (data integrity)

Thuộc tính đảm bảo dữ liệu không bị thay đổi hoặc phá hủy một cách trái phép.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.6

Sự xác thực nguồn gốc dữ liệu (data origin authentication)

Sự chứng thực rằng nguồn của dữ liệu đã nhận được đúng như đã khẳng định.

3.7

Thiết bị lưu dữ liệu (data storage)

Phương tiện lưu trữ thông tin mà từ đó dữ liệu được đưa ra để chuyển phát, hoặc nơi dữ liệu được lưu vào bởi một tổ chức chuyển phát.

3.8

Tổ chức chuyển phát (delivery authority)

Tổ chức được tin cậy bởi bên gửi để chuyển phát dữ liệu từ bên gửi tới bên nhận, và để cung cấp cho người gửi bằng chứng về việc cấp và vận chuyển dữ liệu theo yêu cầu.

3.9

Chữ ký số (digital signature)

Dữ liệu được gắn thêm vào, hoặc một chuyển đổi mật mã của khối dữ liệu cho phép bên nhận khối dữ liệu xác minh nguồn gốc và tính toàn vẹn của khối dữ liệu và bảo vệ chống lại sự giả mạo, ví dụ bởi bên nhận.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.10

Định danh phân biệt (distinguishing identifier)

Thông tin để phân biệt rõ ràng một thực thể trong quá trình chống chối bỏ.

3.11

Bằng chứng (evidence)

Thông tin được sử dụng, hoặc bởi bản thân thông tin hoặc khi kết hợp với thông tin khác, để thiết lập chứng cớ về một sự kiện hoặc hành động.

CHÚ THÍCH: Bằng chứng không cần thiết phải minh chứng cho sự thật hoặc sự tồn tại của một điều gì đó (xem thêm minh chứng), song có thể góp phần vào việc thiết lập minh chứng đó.

3.12

Bên tạo bằng chứng (evidence generator)

Thực thể cung cấp bằng chứng chống chối bỏ.

[ISO/IEC 10181-4]

3.13

Bên sử dụng bằng chứng (evidence user)

Thực thể sử dụng bằng chứng chống chối bỏ.

[ISO/IEC 10181-4]

3.14

Bên xác minh bằng chứng (evidence verifier)

Thực thể xác minh bằng chứng chống chối bỏ.

[ISO/IEC 10181-4]

3.15

Bên yêu cầu bằng chứng (evidence requester)

Thực thể yêu cầu bằng chứng cần được tạo ra bởi thực thể khác hoặc bởi bên thứ ba tin cậy.

3.16

Chủ thể bằng chứng (evidence subject)

Thực thể chịu trách nhiệm cho hành động hoặc kết hợp với sự kiện, liên quan đến bằng chứng đã

được tạo ra.

3.17

Mã băm (hash-code)

Chuỗi bit đầu ra của một hàm băm.

[ISO/IEC 10118-1]

3.18

Hàm băm (hash function)

Hàm thực hiện việc ánh xạ các chuỗi bít thành các chuỗi bit có chiều dài cố định, thỏa mãn hai thuộc tính sau:

- Đối với một đầu ra cho trước, không thể tính toán để tìm ra một đầu vào có ánh xạ đến đầu ra đó.
- Đối với một đầu vào cho trước, không thể tính toán để tìm ra một đầu vào thứ hai có ánh xạ đến cùng đầu ra.

[ISO/IEC 10118-1]

3.19

Dấu vết (imprint)

Chuỗi bit, hoặc mã băm của chuỗi dữ liệu hoặc là bản thân chuỗi dữ liệu.

3.20

Khóa (key)

Dãy các ký hiệu dùng cho kiểm soát hoạt động chuyển đổi mật mã (ví dụ mật mã hóa, giải mật mã, tính toán hàm kiểm tra mật mã, tính toán chữ ký, hoặc xác minh chữ ký).

[ISO/IEC 11770-3]

3.21

Tổ chức giám sát (monitoring authority)

Bên thứ ba tin cậy thực hiện giám sát các hành động và sự kiện, và được tin cậy để cung cấp bằng chứng về những gì đã được giám sát.

3.22

Mã xác thực thông điệp (Message Authentication Code - MAC)

Chuỗi bit đầu ra của thuật toán MAC.

[ISO/IEC 9797-1]

CHÚ THÍCH: Một MAC đôi khi còn được gọi là giá trị kiểm tra mật mã (xem ví dụ TCVN 9696-2:2013 (ISO 7498-2:1989)).

3.23

Thuật toán mã xác thực thông điệp (Message Authentication Code algorithm - MAC algorithm)

Thuật toán để tính toán hàm ánh xạ các chuỗi bit và một khóa bí mật vào các chuỗi bit có chiều dài cố định, thỏa mãn hai thuộc tính sau:

- Cho một khóa bất kỳ và chuỗi đầu vào bất kỳ, hàm có thể tính toán một cách hiệu quả.
- Cho bất kỳ một khóa cố định, khi không biết trước về khóa, không thể tính toán giá trị hàm trên cho bất kỳ chuỗi đầu vào mới nào, ngay cả khi biết về tập các chuỗi đầu vào và các giá trị hàm tương ứng, trong đó giá trị chuỗi đầu vào thứ i có thể đã được chọn sau khi quan sát giá trị của các giá trị hàm thứ i - 1 đầu tiên.

CHÚ THÍCH 1: Thuật toán MAC đôi khi còn gọi là hàm kiểm tra mật mã (xem ví dụ TCVN 9696-2:2013 (ISO 7498-2:1989))

CHÚ THÍCH 2: Tính khả thi của việc tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể của người dùng.

[ISO/IEC 9797-1]

3.24

Chống chối bỏ việc tạo lập (non-repudiation of creation)

Dịch vụ nhằm mục đích bảo vệ chống lại sự từ chối sai trái của một thực thể trong việc đã tạo ra nội dung của một thông điệp (nghĩa là phải chịu trách nhiệm về nội dung của một thông điệp).

3.25

Chống chối bỏ việc chuyển phát (non-repudiation of delivery)

Dịch vụ nhằm mục đích bảo vệ chống lại từ chối sai trái của bên nhận về việc đã nhận một thông điệp và thừa nhận nội dung của một thông điệp.

3.26

Thẻ chống chối bỏ việc chuyển phát (non-repudiation of delivery token)

Phần dữ liệu cho phép nguồn phát thiết lập việc chống chối bỏ chuyển phát đối với một thông điệp.

3.27

Giao dịch chống chối bỏ (non-repudiation exchange)

Chuỗi của một hoặc nhiều chuyển giao thông tin chống chối bỏ (NRI) cho mục đích chống chối bỏ.

3.28

Thông tin chống chối bỏ (non-repudiation information)

Tập hợp thông tin, có thể chứa thông tin về một sự kiện hoặc hành động mà bằng chứng cần được tạo ra và xác minh cho chúng, cũng như bản thân bằng chứng và chính sách chống chối bỏ hiện hành.

3.29

Chống chối bỏ sự hiểu biết (non-repudiation of knowledge)

Dịch vụ nhằm mục đích bảo vệ chống lại sự chối bỏ sai trái của bên nhận về việc đã quan tâm đến nội dung của một thông điệp đã nhận.

3.30

Chống chối bỏ nguồn gốc (non-repudiation of origin)

Dịch vụ nhằm mục đích bảo vệ chống lại sự chối bỏ sai trái của nguồn phát về việc đã tạo ra nội dung thông điệp và đã gửi thông điệp.

3.31

Thẻ chống chối bỏ nguồn gốc (non-repudiation of origin token)

Phần dữ liệu cho phép bên nhận thiết lập sự chống chối bỏ nguồn gốc đối với thông điệp.

3.32

Chính sách chống chối bỏ (non-repudiation policy)

Tập các tiêu chí cho việc cung cấp các dịch vụ chống chối bỏ.

CHÚ THÍCH: Cụ thể hơn, một tập các quy tắc cần được áp dụng cho việc tạo ra và xác minh bằng chứng và cho việc phân xử.

3.33

Chống chối bỏ việc nhận (non-repudiation of receipt)

Dịch vụ nhằm mục đích bảo vệ chống lại sự chối bỏ sai của bên nhận về việc đã nhận một thông điệp.

3.34

Chống chối bỏ việc gửi (non-repudiation of sending)

Dịch vụ nhằm mục đích bảo vệ chống lại sự chối bỏ sai của bên gửi về việc đã gửi một thông điệp.

3.35

Bên yêu cầu dịch vụ chống chối bỏ (non-repudiation service requester)

Thực thể có yêu cầu bằng chứng chống chối bỏ cần được tạo ra cho một sự kiện hoặc hành động cụ thể.

3.36

Chống chối bỏ việc đệ trình (non-repudiation of submission)

Dịch vụ nhằm mục đích cung cấp bằng chứng về việc tổ chức chuyển phát đã chấp nhận một thông điệp để truyền đi.

3.37

Thẻ chống chối bỏ việc đệ trình (non-repudiation of submission token)

Phần dữ liệu cho phép nguồn phát (bên gửi) hoặc tổ chức chuyển phát thiết lập sự chống chối bỏ việc đệ trình cho một thông điệp đã được đệ trình để truyền đi.

3.38

Thẻ chống chối bỏ (non-repudiation token)

Một loại thẻ an toàn đặc biệt được định nghĩa trong ISO/IEC 10181-1, bao gồm bằng chứng và dữ liệu bổ sung (tùy theo yêu cầu).

3.39

Chống chối bỏ việc vận chuyển (non-repudiation of transport)

Dịch vụ nhằm mục đích cung cấp bằng chứng cho nguồn phát thông điệp về việc tổ chức chuyển phát đã chuyển phát một thông điệp tới bên nhận dự định.

3.40

Thẻ chống chối bỏ việc vận chuyển (non-repudiation of transport token)

Phần dữ liệu cho phép nguồn phát hoặc tổ chức chuyển phát thiết lập sự chống chối bỏ vận chuyển cho một thông điệp.

3.41

Tổ chức công chứng (notary authority)

Bên thứ ba tin cậy được tin cậy để cung cấp bằng chứng về thuộc tính của các thực thể liên quan và của dữ liệu đã lưu trữ hoặc trao đổi, hoặc để mở rộng thời gian hiệu lực của một thẻ đang tồn tại sau khi nó hết hiệu lực hoặc sau thu hồi kế tiếp.

3.42

Việc công chứng (notarization)

Sự cung cấp bằng chứng bởi một công chứng viên về thuộc tính của các thực thể liên quan trong một hành động hoặc sự kiện và của dữ liệu đã lưu trữ hoặc đã trao đổi.

3.43

Thẻ công chứng (notarization token)

Thẻ chống chối bỏ được tạo bởi một công chứng viên.

3.44

Nguồn phát (originator)

Thực thể thực hiện gửi một thông điệp tới bên nhận hoặc tạo ra tính sẵn sàng cho một thông điệp mà các dịch vụ chống chối bỏ cần được cung cấp cho nó.

3.45

Khóa riêng (private key)

Khóa của một cặp khóa phi đối xứng cho một thực thể, chỉ có thể được sử dụng bởi thực thể này.

[ISO/IEC 11770-3]

CHÚ THÍCH: Trong hệ thống chữ ký phi đối xứng, khóa riêng xác định phép chuyển đổi chữ ký. Trong hệ mật mã phi đối xứng, khóa riêng xác định phép biến đổi giải mật mã.

3.46

Minh chứng (proof)

Sự chứng thực về việc bằng chứng có giá trị phù hợp với chính sách chống chối bỏ hiện hành.

Chú ý: Minh chứng là bằng chứng để chứng minh sự thật hoặc sự tồn tại của một cái gì đó.

3.47

Khóa công khai (public key)

Khóa của một cặp khóa phi đối xứng cho một thực thể, có thể đưa ra công khai.

[ISO/IEC 11770-3]

CHÚ THÍCH: Trong trường hợp lược đồ chữ ký phi đối xứng, khóa công khai xác định phép biến đổi kiểm chứng. Trong hệ mật mã phi đối xứng, khóa công khai xác định phép biến đổi mật mã hóa. Một khóa được coi là "biết công khai" không nhất thiết phải là sẵn dùng rộng rãi. Khóa có thể chỉ sẵn dùng cho tất cả các thành viên của một nhóm xác định trước.

3.48

Chứng thư khóa công khai (public key certificate)

Thông tin khóa công khai của một thực thể được ký bởi tổ chức chứng thực và vì vậy không thể giả mạo.

[ISO/IEC 11770-3]

3.49

Bên nhận (recipient)

Thực thể thực hiện việc thu (nhận hoặc đón) một thông điệp mà các dịch vụ chống chối bỏ cần được cung cấp cho nó.

3.50

Khóa bí mật (secret key)

Khóa được sử dụng với các kỹ thuật mật mã đối xứng và chỉ có thể sử dụng được bởi tập các thực thể xác định trước.

CHÚ THÍCH: Trích chọn từ ISO/IEC 11770-3:1999, 3.35.

3.51

Tổ chức an toàn thông tin (security authority)

Thực thể chịu trách nhiệm định nghĩa hoặc thực thi chính sách an toàn.

CHÚ THÍCH: Trích chọn từ ISO/IEC 10181-1, 3.3.17

3.52

Chứng thư an toàn (security certificate)

Tập dữ liệu liên quan đến an toàn được phát hành bởi một tổ chức an toàn thông tin hoặc bên thứ ba tin cậy, kèm theo thông tin an toàn được sử dụng để cung cấp tính toàn vẹn và xác thực nguồn gốc dữ liệu.

CHÚ THÍCH: Trích chọn từ ISO/IEC 10181-1, 3.3.18.

3.53

Vỏ bọc bảo vệ (secure envelope - SENV)

Tập các phần dữ liệu được xây dựng bởi một thực thể theo cách mà một thực thể bất kỳ nào đó giữ khóa bí mật có thể xác minh tính toàn vẹn và nguồn gốc của chúng.

CHÚ THÍCH: Với mục đích tạo ra bằng chứng, vỏ bọc bảo vệ SENV được xây dựng và xác minh bởi một bên thứ ba tin cậy (TTP) với một khóa bí mật chỉ có bên thứ ba tin cậy này (TTP) biết.

3.54

Chính sách an toàn (security policy)

Tập các tiêu chí dùng cho việc cung cấp dịch vụ an toàn.

[TCVN 9696-2:2013 (ISO 7498-2:1989)]

3.55

Thẻ an toàn (security token)

Tập dữ liệu liên quan đến an toàn thông tin được bảo vệ về tính toàn vẹn và xác thực nguồn gốc dữ liệu từ một nguồn không phải là tổ chức an toàn thông tin.

CHÚ THÍCH: Trích chọn từ ISO/IEC 10181-1, 3.3.26.

3.56

Bên ký (signer)

Thực thể tạo ra chữ ký số.

3.57

Tem thời gian (time-stamp)

Tham số biến đổi theo thời gian biểu thị một thời điểm liên quan đến một tham chiếu thời gian chung.

[TCVN 7818-1 (ISO/IEC 18014-1)]

3.58

Tổ chức cấp tem thời gian (time-stamping authority)

Bên thứ ba tin cậy cung cấp dịch vụ cấp tem thời gian.

[TCVN 7818-1 (ISO/IEC 18014-1)]

3.59

Tin cậy (trust)

Mối quan hệ giữa hai phần tử, một tập các hành động và một chính sách an toàn, trong đó phần tử *x* tin cậy phần tử *y* khi và chỉ khi *x* có sự tin cậy rằng *y* sẽ hành động theo cách được xác định rõ (ứng với các hành động) mà không vi phạm chính sách an toàn đã được đưa ra.

CHÚ THÍCH: Trích chọn từ TCVN 7818-1 (ISO/IEC 18014-1)

3.60

Bên thứ ba tin cậy (trusted third party)

Tổ chức an toàn thông tin hoặc đại diện của của tổ chức này được tin cậy bởi các thực thể khác tương ứng với các hành động liên quan đến bảo đảm an toàn.

CHÚ THÍCH 1: Trích chọn từ TCVN 7818-1 (ISO/IEC 18014-1), 3.3.30

CHÚ THÍCH 2: Trong phạm vi của bộ tiêu chuẩn này, bên thứ ba tin cậy được tin cậy bởi nguồn phát, bên nhận, và/hoặc tổ chức chuyển phát cho các mục đích chống chối bỏ, và bởi bên khác ví dụ như một quan tòa.

3.61

Tem thời gian tin cậy (trusted time-stamp)

Tem thời gian được bảo đảm bởi một tổ chức cấp tem thời gian.

3.62

Khóa xác minh (verification key)

Giá trị yêu cầu để xác minh một MAC.

3.63

Bên xác minh (verifier)

Thực thể thực hiện xác minh bằng chứng.

4 Ký hiệu và chữ viết tắt

A, B	Định danh phân biệt cho hai thực thể *A* và *B*
CA	Tổ chức chứng thực
$CHK_X(y)$	Giá trị kiểm tra mật mã được tính trên dữ liệu y sử dụng khóa của thực thể *X*
DA	Định danh phân biệt của tổ chức chuyển phát
GNRT	Thẻ chống chối bỏ chung

Q	Dữ liệu tùy chọn cần được bảo vệ tính toàn vẹn / nguồn phát
Imp(y)	Dấu vết của chuỗi dữ liệu y, là (1) mã băm của chuỗi dữ liệu *y*, hoặc (2) chuỗi dữ liệu *y*
m	Một thông điệp mà bằng chứng được tạo ra cho nó
MAC	Mã xác thực thông điệp
NA	Tổ chức công chứng
NRDT	Thẻ chống chối bỏ chuyển phát
NRI	Thông tin chống chối bỏ
NROT	Thẻ chống chối bỏ nguồn gốc
NRST	Thẻ chống chối bỏ việc đệ trình
NRTT	Thẻ chống chối bỏ vận chuyển
NT	Thẻ công chứng
OSI	Liên kết hệ thống mở
Pol	Định danh phân biệt của chính sách chống chối bỏ (hoặc các chính sách) áp dụng cho bằng chứng.
SENV	Vỏ bọc bảo vệ (Secure envelope).
$SENV_X(y)$	Vỏ bọc bảo vệ được tính trên dữ liệu y sử dụng khóa bí mật của thực thể *X*.
SIG	Thông điệp đã ký.
$SIG_X(y)$	Thông điệp đã ký được tạo từ dữ liệu y bởi thực thể X sử dụng khóa riêng của nó.
$S_X(y)$	Chữ ký được tính trên dữ liệu y sử dụng thuật toán chữ ký và khóa riêng của thực thể *X*.
text	Phần dữ liệu tạo nên một phần của thẻ có thể chứa thông tin bổ sung, ví dụ một định danh khóa và/hoặc định danh thông điệp.
T_g	Ngày giờ cho bằng chứng được tạo ra.
T_i	Ngày giờ cho sự kiện hoặc hành động xảy ra.
TSA	Định danh phân biệt của tổ chức cấp tem thời gian tin cậy.
TST	Thẻ tem thời gian được tạo ra bởi TSA.
TTP	Định danh phân biệt của bên thứ ba tin cậy.
$V_X(y)$	Hoạt động xác thực áp dụng cho dữ liệu y (vỏ bọc bảo vệ hoặc chữ ký số) bằng cách sử dụng một thuật toán xác minh và khóa xác minh của thực thể *X*.
(y,z)	Kết quả của phép ghép nối theo thứ tự của *y* và z.

5 Tổ chức phần còn lại của tiêu chuẩn

Các dịch vụ chống chối bỏ được mô hình hóa trước hết bằng việc xác định các yêu cầu cơ bản nêu trong Điều 6, tiếp đó mô tả như nêu ở Điều 7 về vai trò của các thực thể liên quan tới việc cung cấp và xác minh bằng chứng. Sự tham gia của các bên thứ ba tin cậy trong các giai đoạn chống chối bỏ khác nhau, cụ thể là việc cung cấp và xác minh bằng chứng được mô tả trong Điều 8. Các cơ chế tạo ra và xác minh bằng chứng được mô tả trong Điều 9 liên quan đến việc tạo ra các vỏ bọc bảo vệ và các chữ ký số dựa trên các kỹ thuật mật mã đối xứng và phi đối xứng. Các hàm kiểm tra mật mã chung cho cả hai cơ chế cơ bản được rút ra nhằm biểu diễn rõ hơn các thẻ chống chối bỏ. Trong Điều 10, ba loại thẻ được định nghĩa: thứ nhất là thẻ chống chối bỏ chung phù hợp cho nhiều dịch vụ chống chối bỏ, thứ hai là thẻ tem thời gian được tạo ra bởi tổ chức cấp tem thời gian tin cậy và thứ ba là thẻ công chứng được tạo ra bởi công chứng viên để cung cấp bằng chứng về các thuộc tính của các thực thể liên quan cũng như của dữ liệu đã lưu trữ hoặc trao đổi. Các dịch vụ chống chối bỏ cụ thể và các thẻ chống chối bỏ được mô tả trong Điều 11. Điều 12 nêu một ví dụ về việc sử dụng các thẻ chống chối bỏ trong môi trường truyền thông điệp.

6 Các yêu cầu

Phụ thuộc vào việc rút ra giá trị kiểm tra mật mã dùng để tạo ra vỏ bọc bảo vệ và chữ ký số và độc lập với dịch vụ chống chối bỏ được hỗ trợ bởi các cơ chế chống chối bỏ, các yêu cầu sau đây được đặt ra cho các thực thể liên quan trong giao dịch chống chối bỏ:

- Các thực thể của một giao dịch chống chối bỏ sẽ tin cậy bất kỳ bên thứ ba tin cậy nào tham gia vào giao dịch.

  CHÚ THÍCH: Khi sử dụng các thuật toán mật mã đối xứng, luôn luôn yêu cầu một TTP. Khi sử dụng các thuật toán mật mã phi đối xứng, một TTP luôn luôn được yêu cầu để tạo ra chứng thư khóa công khai hoặc tạo ra chữ ký số cho bằng chứng.

- Trước khi tạo ra bằng chứng, bên tạo bằng chứng phải biết chính sách chống chối bỏ nào có thể được chấp nhận đối với bên (hoặc các bên) xác minh, loại bằng chứng được yêu cầu và tập các cơ chế có thể được chấp nhận đối với bên (hoặc các bên) xác minh.

- Các cơ chế để tạo ra hoặc xác minh bằng chứng sẽ sẵn dùng cho các thực thể của một giao dịch chống chối bỏ cụ thể, hoặc một tổ chức tin cậy phải sẵn sàng cung cấp các cơ chế và thực hiện các chức năng cần thiết thay mặt cho bên yêu cầu bằng chứng.

- Các khóa phù hợp với các cơ chế đang được sử dụng (ví dụ: khóa riêng dùng cho cơ chế phi đối xứng, khóa bí mật dùng cho cơ chế đối xứng) sẽ được nắm giữ (và nếu cần thiết sẽ được chia sẻ) bởi các thực thể liên quan.

- Người dùng bằng chứng và tòa án được yêu cầu về khả năng có thể xác minh bằng chứng.

- Nếu một tem thời gian tin cậy được yêu cầu, hoặc đồng hồ được cung cấp bởi bên tạo ra bằng chứng

không thể tin cậy, thì khi đó một tổ chức cấp tem thời gian cần được kết nối truy cập bởi bên tạo ra bằng chứng hoặc bên xác minh bằng chứng.

7 Các dịch vụ chống chối bỏ chung

7.1 Các thực thể tham gia vào việc cung cấp và xác minh bằng chứng

Một số thực thể riêng biệt có thể liên quan đến việc cung cấp một dịch vụ chống chối bỏ.

Ba thực thể liên quan tới giai đoạn tạo ra bằng chứng gồm:

- Bên yêu cầu bằng chứng mong muốn thu được bằng chứng.
- Chủ thể bằng chứng thực hiện một hành động hoặc được tham gia vào một sự kiện.
- Bên tạo ra bằng chứng thực hiện việc tạo ra bằng chứng.

Hai thực thể liên quan tới giai đoạn xác minh bằng chứng gồm:

- Người dùng bằng chứng, có thể hoặc không thể xác minh trực tiếp.
- Bên xác minh bằng chứng có thể xác minh bằng chứng theo yêu cầu của người dùng bằng chứng.

Trong giai đoạn tạo ra bằng chứng, sự kiện hoặc hành động có sự liên quan tới chủ thể bằng chứng. Bằng chứng có thể được cung cấp theo yêu cầu từ bên yêu cầu bằng chứng hoặc bởi chính chủ thể bằng chứng.

Trong một số trường hợp chỉ có hai thực thể (chủ thể bằng chứng và bên yêu cầu bằng chứng) cần thiết để cung cấp bằng chứng, tuy nhiên, trong một số trường hợp khác, một bên thứ ba cũng cần thiết để cung cấp bằng chứng. Bằng chứng sau đó được trả lại hoặc sẵn sàng cung cấp cho bên yêu cầu bằng chứng: bằng chứng có thể khi đó sẽ được chuyển tiếp hoặc sẵn sàng cung cấp cho các thực thể khác.

Trong giai đoạn xác minh bằng chứng, một người dùng bằng chứng mong muốn xác minh xem bằng chứng có đúng không. Nếu người dùng bằng chứng không thể xác minh bằng chứng trực tiếp thì bằng chứng sẽ được xác minh bởi bên xác minh bằng chứng theo yêu cầu của người dùng bằng chứng.

7.2 Các dịch vụ chống chối bỏ

Chống chối bỏ bao gồm việc tạo ra bằng chứng có thể sử dụng để minh chứng về một sự kiện hoặc hành động đã xảy ra. Bằng chứng được tạo ra ở dạng dữ liệu có thể xác minh, mô tả các hành động hoặc sự kiện. Dữ liệu và bằng chứng được lưu trữ (môi trường không phải kiểu OSI) hoặc được trao đổi trong một giao dịch chống chối bỏ giữa các bên liên quan. Bằng chứng được truyền đi trong các thẻ chống chối bỏ như một phần của các giao thức chống chối bỏ.

Một số dịch vụ chống chối bỏ có thể được cung cấp bằng cách nhóm các dịch vụ khác; ví dụ: dịch vụ chống chối bỏ nguồn phát có thể được cung cấp bằng cách kết hợp chống chối bỏ việc tạo ra và chống

chối bỏ việc gửi đi, chống chối bỏ chuyển phát có thể được cung cấp bằng cách kết hợp chống chối bỏ việc nhận và chống chối bỏ sự hiểu biết.

8 Sự tham gia của bên thứ ba tin cậy

8.1 Tổng quan

Bên thứ ba tin cậy có thể được tham gia vào việc cung cấp các dịch vụ chống chối bỏ, tùy thuộc vào các cơ chế được sử dụng hoặc chính sách chống chối bỏ hiện hành. Việc sử dụng các kỹ thuật mật mã phi đối xứng yêu cầu các khóa công khai đích thực có thể được đảm bảo bởi các chứng thư được phát hành bởi các bên thứ ba, ví dụ bởi các tổ chức chứng thực. Việc sử dụng các kỹ thuật mật mã đối xứng yêu cầu sự tham gia trực tuyến của một bên thứ ba tin cậy để tạo ra và xác minh vỏ bọc bảo vệ (SENV). Chính sách chống chối bỏ hiện hành có thể yêu cầu bằng chứng được tạo ra từng phần hoặc toàn bộ bởi bên thứ ba tin cậy.

Chính sách chống chối bỏ hiện hành cũng có thể yêu cầu:

- Một tem thời gian tin cậy được cung cấp bởi tổ chức cấp tem thời gian tin cậy;
- Một công chứng viên cần được tham gia vào xác minh dữ liệu của một hoặc nhiều bên và trả lại dữ liệu cho các bên với chữ ký điện tử;
- Một tổ chức giám sát cần được tham gia để cung cấp bằng chứng về các thuộc tính của các thực thể có liên quan và của dữ liệu đã lưu trữ hoặc trao đổi.

Các bên thứ ba tin cậy có thể tham gia với các mức độ khác nhau trong các giai đoạn chống chối bỏ. Khi trao đổi bằng chứng, các bên hoặc sẽ được biết, được thông báo, hoặc thỏa thuận về chính sách chống chối bỏ nào cần áp dụng được cho bằng chứng.

Có thể có một số bên thứ ba tin cậy tham gia đóng các vai trò khác nhau (ví dụ: công chứng, cấp tem thời gian, giám sát, chứng thực khóa, sinh chữ ký, xác minh chữ ký, sinh vỏ bọc bảo vệ, xác minh vỏ bọc bảo vệ, sinh thẻ, hoặc các vai trò chuyển phát), như đã chỉ ra trong chính sách chống chối bỏ. Một bên thứ ba tin cậy đơn lẻ có thể đóng trong một hoặc nhiều vai trò này.

8.2 Giai đoạn tạo ra bằng chứng

Bằng chứng là thông tin có thể được sử dụng để giải quyết tranh chấp và được tạo ra bởi bên tạo ra bằng chứng đại diện cho một chủ thể bằng chứng, một bên thứ ba tin cậy, hoặc theo yêu cầu của bên yêu cầu bằng chứng. Một TTP có thể tham gia vào giai đoạn tạo bằng chứng theo các cách sau (xem định nghĩa về tổ chức trực tuyến, nội tuyến, ngoại tuyến trong ISO/IEC TR 14516):

- Trực tiếp:

- Khi hoạt động như một tổ chức trực tuyến (on-line) chủ động tham gia vào mọi trường hợp của dịch vụ chống chối bỏ, một mình bên thứ ba tin cậy tạo ra bằng chứng với tư cách đại diện cho chủ thể bằng chứng. Việc tạo trực tuyến các giá trị kiểm tra mật mã và các thẻ chống chối bỏ có thể được yêu cầu khi các kỹ thuật mật mã đối xứng được sử dụng để cung cấp bằng chứng, Ví dụ: để tạo ra vỏ bọc bảo vệ như đã định nghĩa trong TCVN 11393-2 (ISO/IEC 13888-2)
- Khi hoạt động như một tổ chức tạo bằng chứng nội tuyến (in-line), tự bản thân bên thứ ba tin cậy tạo ra bằng chứng, ví dụ: như tổ chức chuyển phát.

- Gián tiếp:
  - Khi hoạt động như một tổ chức ngoại tuyến (off-line) không tham gia vào tất cả các trường hợp của dịch vụ chống chối bỏ, bên thứ ba tin cậy cung cấp chứng thư khóa công khai ngoại tuyến liên quan tới các thực thể tạo bằng chứng dựa trên các chữ ký.
  - Khi hoạt động như một tổ chức tạo ra thẻ, bên thứ ba tin cậy xây dựng bất kỳ loại thẻ chống chối bỏ nào, bao gồm một hoặc nhiều thẻ chống chối bỏ được cung cấp bởi chủ thể bằng chứng hoặc bởi một hoặc nhiều tổ chức tin cậy.
  - Khi hoạt động như một tổ chức tạo ra chữ ký số, bên thứ ba tin cậy đại diện cho chủ thể bằng chứng hoặc người yêu cầu bằng chứng tạo ra chữ ký số.
  - Khi hoạt động như một tổ chức cấp tem thời gian, bên thứ ba tin cậy được tin cậy để cung cấp bằng chứng bao gồm thời điểm khi thẻ tem thời gian được tạo ra.
  - Khi hoạt động như một tổ chức công chứng (công chứng viên), bên thứ ba tin cậy được tin cậy trong cung cấp bằng chứng về các thuộc tính của thực thể liên quan và của dữ liệu đã lưu trữ hoặc trao đổi giữa các thực thể. Công chứng viên được tin cậy trong việc kéo dài thời gian hiệu lực của các thẻ đang tồn tại khi chúng hết hạn sử dụng hoặc bị thu hồi sau đó.
  - Khi hoạt động như một tổ chức giám sát, bên thứ ba tin cậy giám sát các hoạt động và các sự kiện, và được tin cậy trong cung cấp bằng chứng về những gì đã được giám sát.

8.3 Giai đoạn chuyển giao, lưu trữ và thu hồi bằng chứng

Trong giai đoạn này, bằng chứng được truyền tải giữa các bên, hoặc đến và đi từ thiết bị lưu trữ. Tùy thuộc vào chính sách chống chối bỏ hiện hành, các hoạt động của giai đoạn này có thể không luôn luôn xảy ra trong tất cả các trường hợp của dịch vụ chống chối bỏ. Các hoạt động của giai đoạn này có thể được thực hiện bởi bên thứ ba tin cậy hoặc các bên khác.

- Khi hoạt động như một tổ chức chuyển phát, bên thứ ba tin cậy sẽ phù hợp cho chống chối bỏ việc đệ trình và chống chối bỏ việc vận chuyển.

- Khi hoạt động như một tổ chức giữ hồ sơ bằng chứng, bên thứ ba tin cậy ghi lại bằng chứng để sau này người dùng bằng chứng hay quan tòa có thể lấy lại.

8.4 Giai đoạn xác minh bằng chứng

Khi hoạt động như tổ chức xác minh bằng chứng, bên thứ ba tin cậy hoạt động như một tổ chức trực tuyến, được tin cậy bởi người dùng bằng chứng để xác minh từng loại thông tin chống chối bỏ được cung cấp trong thẻ chống chối bỏ. Khi bằng chứng được tạo ra sử dụng kỹ thuật mật mã đối xứng, nó chỉ có thể được xác minh bởi một bên thứ ba tin cậy, nếu không thì sự tham gia của một bên thứ ba tin cậy có thể là tùy ý.

Cách thức sử dụng để xác minh thẻ chống chối bỏ phụ thuộc vào các kỹ thuật dùng để tạo ra nó như sau:

- Vỏ bọc bảo vệ chỉ có thể được xác minh bởi bên thứ ba tin cậy.
- Chữ ký số có thể được xác minh bằng sử dụng một hoặc nhiều chứng thư khóa công khai và danh sách chứng thư thu hồi khi tất cả vẫn còn hợp lệ tại thời điểm tạo ra bằng chứng.
- Chứng thư khóa công khai hợp lệ tại thời điểm bằng chứng được tạo ra phải được xác minh cho thời điểm khi bằng chứng được tạo ra. Trong trường hợp chứng thư khóa công khai hết hạn hoặc bị thu hồi ở thời điểm bằng chứng được đưa ra, có thể hoàn tất bằng cách xác minh chứng thư khóa công khai cho thời gian đã xác nhận trong một thẻ tem thời gian hoặc một thẻ công chứng có trong bằng chứng, tương ứng với chính sách chống chối bỏ hiện hành.
- Danh sách thu hồi chứng thư (khóa công khai) hợp lệ tại thời điểm bằng chứng được tạo ra phải được xác minh ở thời điểm bằng chứng được đưa ra. Trong một số trường hợp, có thể là sau nhiều năm.
- Trường hợp việc chống chối bỏ yêu cầu sử dụng tổ chức cấp tem thời gian để cung cấp bằng chứng, thì nó sẽ được thể hiện theo cách sau. Giá trị thời gian có trong bằng chứng (nghĩa là trong thẻ tem thời gian) phải được so sánh với giá trị thời gian có trong bằng chứng được tạo ra bởi thực thể tạo ra nó, bên thứ ba tin cậy hoặc bên yêu cầu bằng chứng. Khi các giá trị thời gian này được xác minh là hợp lệ theo chính sách an toàn, thì bằng chứng việc tạo ra chúng bởi thực thể tạo ra bằng chứng, một bên thứ ba tin cậy hoặc bên yêu cầu bằng chứng có thể được chấp nhận.
- Các thẻ chống chối bỏ bổ sung (ví dụ thẻ công chứng) được xác minh theo các kỹ thuật được sử dụng để tạo ra.

9 Các cơ chế tạo và xác minh bằng chứng

9.1 Tổng quan

Trong các giai đoạn này, bằng chứng được biểu diễn bằng các thẻ chống chối bỏ bao gồm các vỏ bọc bảo vệ (SENV) hoặc các chữ ký số (SIG). Cả hai dựa vào các giá trị kiểm tra mật mã (CHK) được sinh ra hoặc bởi các kỹ thuật mật mã phi đối xứng hoặc đối xứng tương ứng. Khi sử dụng các chữ ký dựa trên chứng thư, thẻ chống chối bỏ về cơ bản gồm thông điệp đã được ký (bao gồm cả thông điệp và chữ ký) và (các) chứng thư khóa công khai của nó. Nếu chứng thư khóa công khai không được cung cấp cùng với chữ ký số, thì nó phải sẵn dùng cho các bên thích hợp. Khi sử dụng chữ ký dựa trên định danh (xem ISO/IEC 14888-2), thẻ chống chối bỏ gồm thông điệp đã được ký, dữ liệu nhận dạng của thực thể ký và định danh (nghĩa là định danh phân biệt) của tổ chức cung cấp một hoặc cả hai khóa cho bên ký.

9.2 Vỏ bọc bảo vệ

Để một vỏ bọc bảo vệ trở thành bằng chứng hợp lệ, nó phải được tạo ra bởi bên thứ ba tin cậy sử dụng một khóa bí mật chỉ bên thứ ba tin cậy đó biết.

CHÚ THÍCH: SENV có thể được sử dụng cho bảo vệ nguồn gốc / tính toàn vẹn giữa bên yêu cầu bằng chứng của một giao dịch chống chối bỏ và một TTP. Trong trường hợp đó, SENV được tạo ra và xác minh với một khóa được biết bởi cả thực thể liên quan và TTP.

Một vỏ bọc bảo vệ được tạo ra thông qua việc sử dụng các kỹ thuật toàn vẹn đối xứng trên dữ liệu *y*, sử dụng khóa bí mật của thực thể *X* để cung cấp giá trị kiểm tra mật mã $CHK_X(y)$ được gắn thêm vào dữ liệu *y* như sau:

$$SENV_X(y) = (y, CHK_X(y)).$$

Hàm $CHK_X(y)$ có thể được biểu diễn bởi các cơ chế toàn vẹn dữ liệu khác nhau, ví dụ như MAC.

CHÚ THÍCH: Một MAC có thể là một mã xác thực thông điệp như chỉ ra trong ISO/IEC 9797.

Các cơ chế khác có thể được chỉ ra trong các phần cụ thể của bộ tiêu chuẩn TCVN 11393.

9.3 Chữ ký số

Một thực thể *X* có thể ký thông điệp y sử dụng phép toán chữ ký số và khóa riêng của nó. Kết quả nhận lại là thông điệp đã được ký, được ký hiệu là $SIG_X(y)$. Sự hợp lệ của thông điệp đã được ký $SIG_X(y)$ có thể được xác minh bởi bất kỳ ai có bản sao đích thực của khóa công khai của thực thể *X*.

Nếu phép toán chữ ký số không cho phép khôi phục lại thông điệp, thông điệp đã ký được tạo thành bằng cách gắn thêm chữ ký $S_X(y)$ vào thông điệp *y*.

$$SIG_X(y) = (y, S_X(y))$$

Nếu phép toán chữ ký số cho phép khôi phục lại thông điệp, một phần hoặc tất cả thông điệp *y* có thể được khôi phục từ $S_X(y)$, thì thông điệp đã ký $SIG_X(y)$ có thể được tạo thành bằng cách gắn thêm $S_X(y)$ vào phần của *y* mà không thể khôi phục từ chữ ký $S_X(y)$.

CHÚ THÍCH 1: Các chữ ký số cho phép khôi phục lại thông điệp được chỉ ra trong ISO/IEC 9796.

CHÚ THÍCH 2: Các chữ ký số cùng với phụ lục được chỉ ra trong ISO/IEC 14888.

9.4 Cơ chế xác minh bằng chứng

Các vỏ bọc bảo vệ (SENV) hoặc các chữ ký số (SIG) được xác minh bằng cách áp dụng phép toán xác minh $V_X(SENV)$ hoặc $V_X(SIG)$ tương ứng sử dụng khóa xác minh của thực thể tạo ra bằng chứng X. Kết quả của phép toán xác minh là đúng hoặc sai.

Các vỏ bọc bảo vệ chỉ có thể được xác minh bởi bên thứ ba tin cậy nắm giữ khóa bí mật đã được dùng để tạo ra vỏ bọc bảo vệ.

CHÚ THÍCH: Nếu SENV được tạo ra cho truyền thông bảo vệ nguồn gốc / tính toàn vẹn, thì nó có thể được xác minh bởi bất kỳ thực thể nào có giữ khóa bí mật phù hợp.

Chữ ký số có thể được xác minh bởi thực thể bất kỳ có giữ khóa công khai của bên ký. Việc cung cấp khóa xác minh công khai cho bên xác minh phụ thuộc vào kiểu của lược đồ chữ ký đã được áp dụng để tạo ra chữ ký số.

- Chữ ký dựa trên chứng thư được xác minh bằng khóa công khai của bên ký có sẵn trong chứng thư khóa công khai được phát hành bởi tổ chức chứng thực.
- Chữ ký dựa trên định danh được xác minh bởi bất kỳ thực thể nào có giữ dữ liệu định danh thực thể ký và các tham số hệ thống công khai nhận được từ tổ chức tin cậy cung cấp các khóa riêng dựa trên định danh cho người ký.

Khi sử dụng chữ ký số, một chuỗi các chứng thư khóa công khai hoặc các định danh cũng có thể phải được xác minh để đạt được sự bảo đảm cần thiết.

10 Thẻ chống chối bỏ

10.1 Tổng quan

Một dịch vụ chống chối bỏ được dàn xếp bởi thông tin chống chối bỏ. Thông tin chống chối bỏ được tổng hợp từ một hoặc nhiều thẻ chống chối bỏ. Bên tạo bằng chứng phải cung cấp ít nhất một thẻ chống chối bỏ được rút ra từ thẻ chống chối bỏ chung. Các thẻ bổ sung thường được yêu cầu để xác minh bằng chứng. Các thẻ bổ sung có thể được hoặc không được cung cấp cho bên xác minh. Khi chúng không được cung cấp, bên xác minh cần phải hoặc tự lấy (ví dụ các chứng thư khóa công khai và/hoặc các danh sách thu hồi chứng thư), hoặc yêu cầu chúng (ví dụ cấp tem thời gian từ các tổ chức cấp tem thời gian). Ba thẻ chung được mô tả trong tiêu chuẩn này, có tên là Thẻ chống chối bỏ chung, Thẻ tem thời gian, và Thẻ công chứng. Các thẻ rút ra từ thẻ chống chối bỏ chung được tạo ra bởi bên tạo bằng chứng, trong khi các thẻ khác được tạo bởi bên thứ ba tin cậy: thẻ tem thời gian được tạo bởi một tổ chức cấp tem thời gian, thẻ công chứng được tạo bởi một tổ chức công chứng.

Các dịch vụ chống chối bỏ chỉ có thể được cung cấp trong một khoảng thời gian xác định. Có thể cần phải thay đổi thời gian hiệu lực của thẻ sau khi thẻ đã được phát hành, ví dụ giảm thời gian hiệu lực nếu thấy có tấn công vào một lược đồ chữ ký cụ thể. Mặt khác, nếu thẻ chống chối bỏ vẫn được xem là an toàn (về mặt mật mã) sau khi hết thời gian hiệu lực, khi đó chính sách chống chối bỏ có thể cho phép kéo dài thời gian hiệu lực của thẻ (ví dụ: bằng cách đính kèm một thẻ công chứng từ tổ chức công chứng vào thẻ đó).

10.2 Thẻ chống chối bỏ chung (GNRT)

Thẻ chống chối bỏ chung được định nghĩa như sau:

$$GNRT = (text, z, CHK_X(z))$$

với: $z = (Pol, f, A, B, C, D, E, T_g, T_l, Q, Imp(m))$

Trường dữ liệu z bao gồm các thành phần dữ liệu sau:

Pol Chính sách (hay các chính sách) chống chối bỏ áp dụng cho bằng chứng,

f Kiểu dịch vụ chống chối bỏ đang được cung cấp,

A Định danh phân biệt của chủ thể bằng chứng,

B Định danh phân biệt của bên tạo bằng chứng mà khác với chủ thể bằng chứng,

C Định danh phân biệt của thực thể tương tác với chủ thể bằng chứng (ví dụ bên gửi thông điệp, bên dự kiến nhận thông điệp hoặc tổ chức chuyển phát),

D Định danh phân biệt của bên yêu cầu bằng chứng nếu khác với chủ thể bằng chứng,

E Các định danh phân biệt của các thực thể khác liên quan đến hành động (ví dụ các bên dự kiến nhận một thông điệp),

T_g Ngày giờ bằng chứng đã được tạo ra,

T_l Ngày giờ xảy ra sự kiện hoặc hành động,

Q Dữ liệu tùy chọn cần được bảo vệ nguồn gốc / tính toàn vẹn,

Imp(m) Dấu vết của thông điệp liên quan tới một sự kiện hoặc hành động.

CHÚ THÍCH: Tùy thuộc vào chính sách chống chối bỏ hiện hành, một số phần dữ liệu có thể là tùy chọn.

Định danh phân biệt *A* luôn luôn cần có mặt. Tất cả các định danh phân biệt khác là *B, C, D, E* có thể không cần có mặt. Định danh phân biệt *B* của bên tạo bằng chứng cần thiết khi bằng chứng được tạo ra bởi tổ chức đại diện cho chủ thể bằng chứng. Định danh phân biệt *C* cần thiết trong trường hợp truyền tải thông điệp. Định danh phân biệt *D* của bên yêu cầu bằng chứng cần thiết cho trường hợp bên yêu cầu bằng chứng khác với chủ thể bằng chứng. (Các) định danh phân biệt *E* của (các) thực thể khác tham gia trong hành động bao gồm trường hợp chống chối bỏ việc đệ trình tới tổ chức chuyển phát và chống chối bỏ vận chuyển bởi tổ chức chuyển phát.

Trường *"text"* bao gồm dữ liệu bổ sung mà không cần thiết được bảo vệ bằng mật mã. Thông tin phụ thuộc vào kỹ thuật đang được sử dụng, cụ thể là:

- Với chữ ký dựa trên chứng thư, trường *"text"* có thể chứa một hoặc nhiều chứng thư khoá công khai hoặc đơn giản là định danh phân biệt của tổ chức chứng thực cùng với số hiệu của chứng thư được gán cho chứng thư khóa công khai.
- Với chữ ký dựa trên định danh, trường *"text"* có thể chứa định danh phân biệt của tổ chức cung cấp một hoặc cả hai khóa cho bên ký.

10.3 Thẻ tem thời gian

Nếu một tem thời gian tin cậy được yêu cầu hoặc đồng hồ được cung cấp bởi bên tạo ra thẻ chống chối bỏ không thể được tin cậy, thì cần phải dựa vào một bên thứ ba tin cậy, một tổ chức cấp tem thời gian (TSA). Vai trò của TSA là thiết lập thêm bằng chứng biểu thị thời điểm thẻ đã được tạo ra.

Thẻ tem thời gian được cung cấp bởi tổ chức cấp tem thời gian sẽ được tạo bằng cách sử dụng phương pháp bất kỳ từ TCVN 7818 (ISO/IEC 18014)

10.4 Thẻ công chứng

Dịch vụ công chứng được sử dụng để cung cấp bằng chứng bởi tổ chức công chứng về các thuộc tính của các thực thể liên quan và của dữ liệu đã biểu thị, hoặc để kéo dài thời gian hiệu lực của một thẻ chống chối bỏ đang tồn tại sau khi hết hạn hoặc sau việc thu hồi kế tiếp.

Dữ liệu *y* được cung cấp bởi thực thể yêu cầu dịch vụ.

CHÚ THÍCH: Dữ liệu y có thể là một thông điệp, một thẻ chống chối bỏ, một mã băm của thông điệp, mã băm của một thẻ, hoặc bất kỳ dữ liệu nào mà bên yêu cầu dịch vụ muốn được chứng nhận bởi công chứng viên.

Thẻ công chứng (Notarization Token - NT) được định nghĩa như sau:

$$NT = (text, w, CHK_{NA}(w))$$

với $w = (Pol, f, A, NA, T_g, Q, Imp(y))$

Phần tử dữ liệu *w* gồm các thành phần dữ liệu sau:

Pol	Chính sách (hoặc các chính sách) áp dụng cho bằng chứng,
f	Cờ chỉ ra đây là dịch vụ công chứng,
A	Định danh phân biệt của thực thể *X* yêu cầu dịch vụ công chứng *f*,
NA	Định danh phân biệt của tổ chức công chứng,
T_g	Ngày giờ thực hiện công chứng,
Imp(y)	Dấu vết của dữ liệu *y* mà dịch vụ công chứng được cung cấp cho nó.

Thẻ tương tự có thể được sử dụng bởi tổ chức giám sát để tạo ra bằng chứng trên dữ liệu *y* được cung cấp bởi chủ thể bằng chứng và/hoặc được tạo ra bởi chính tổ chức giám sát.

11 Các dịch vụ chống chối bỏ cụ thể

11.1 Tổng quan

Phần sau đây xác định tập hợp cụ thể các hành động, tất cả đều liên quan tới việc vận chuyển thông điệp giữa thực thể *A* và thực thể *B*. Các thành phần trung gian như tổ chức chuyển phát cũng có liên quan.

Thực thể *A* tạo ra một thông điệp *m* và thiết lập chống chối bỏ nguồn gốc theo ý muốn của mình hoặc theo như được yêu cầu bởi chính sách chống chối bỏ hiện hành hoặc bởi thực thể khác (ví dụ bởi một bên nhận). Chống chối bỏ nguồn gốc được cung cấp bởi bên tạo bằng chứng, đó có thể chính là nguồn phát hoặc một bên thứ ba tin cậy.

Thực thể *A* gửi thông điệp *m* cùng với bằng chứng được chứa trong một thẻ chống chối bỏ nguồn gốc NROT tới thực thể B là bên nhận (xem Hình 1).

Trong một số trường hợp, một hoặc nhiều bên thứ ba tin cậy có thể thực hiện chức năng của tổ chức chuyển phát. Trường hợp có một tổ chức chuyển phát, tất cả các dịch vụ chống chối bỏ được mô tả trong Điều này có thể được cung cấp.

Trong các trường hợp khác có thể không có tổ chức chuyển phát. Khi không có tổ chức chuyển phát, chỉ một số dịch vụ chống chối bỏ đã được mô tả trong Điều này có thể được cung cấp; nghĩa là chỉ có thể cung cấp các dịch vụ chống chối bỏ nguồn gốc và chống chối bỏ việc chuyển phát.

Tùy thuộc vào ứng dụng cụ thể và chính sách chống chối bỏ hiện hành, hệ thống chuyển phát được tin cậy để tạo ra bằng chứng về việc:

- đã nhận thông điệp *m* với thẻ chống chối bỏ NROT từ thực thể *A* để truyền tải tới thực thể *B* bằng cách tạo ra một thẻ chống chối bỏ việc đệ trình NRST,
- đã chuyển phát thông điệp *m* với thẻ chống chối bỏ NROT tới thiết bị lưu dữ liệu của thực thể *B*, tới bên nhận dự kiến, bằng cách tạo ra một thẻ chống chối bỏ vận chuyển NRTT.

Tùy thuộc vào chính sách chống chối bỏ hiện hành, có thể cần phải có thẻ tem thời gian (TST) hoặc thẻ công chứng (NT) được cung cấp như bằng chứng (bổ sung) cho thẻ chống chối bỏ đang tồn tại.

CHÚ THÍCH: Từ chối việc gửi hoặc nhận thông điệp bao gồm khả năng một bên gửi (hoặc bên nhận), trong khi không thể từ chối việc một thông điệp đã được gửi (hoặc được nhận), có thể chối bỏ thời điểm đã gửi (hoặc đã nhận) thông điệp đó.

11.2 Chống chối bỏ nguồn gốc

Dịch vụ chống chối bỏ nguồn gốc dùng cho trường hợp bên gửi thông điệp vừa tạo ra vừa gửi thông điệp đó.

Dịch vụ này được thiết kế để bảo vệ chống lại việc chối bỏ sai trái của bên gửi về việc vừa là bên tạo ra thông điệp (tác giả của nội dung) vừa là bên gửi thông điệp đó.

Dịch vụ này có thể được cung cấp bởi chính bên gửi hoặc tổ chức đại diện cho bên gửi.

11.3 Chống chối bỏ việc chuyển phát

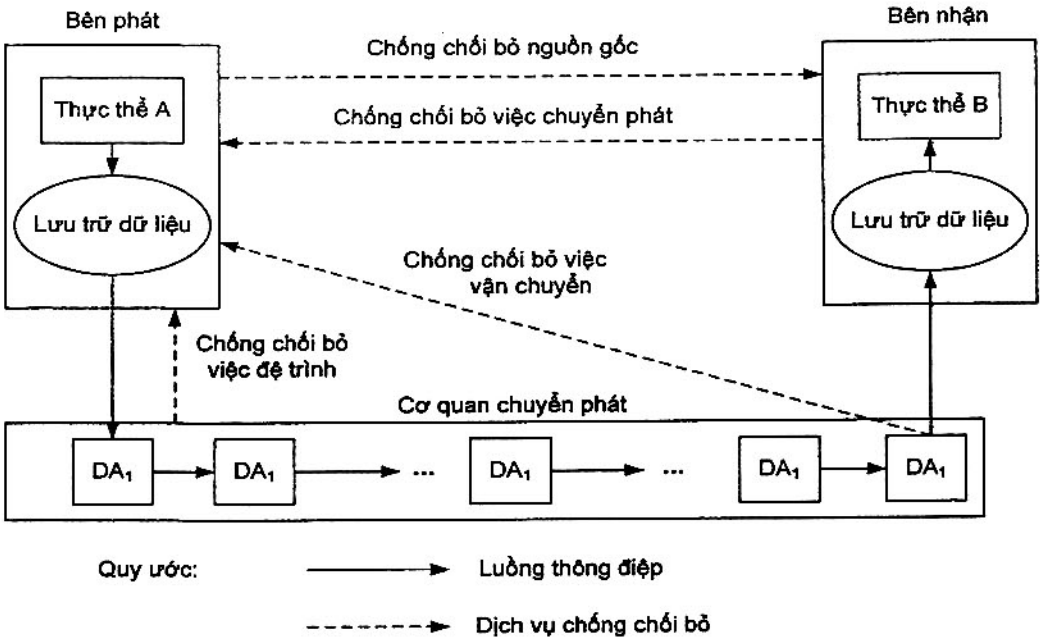
Dịch vụ chống chối bỏ việc chuyển phát bao gồm trường hợp bên nhận thừa nhận thực tế là nó vừa nhận thông điệp vừa quan tâm về nội dung của thông điệp.

11.4 Chống chối bỏ việc đệ trình

Dịch vụ này yêu cầu có sự xuất hiện của tổ chức chuyển phát tham gia vào việc vận chuyển thông điệp giữa một bên gửi và một hoặc nhiều bên nhận. Tổ chức chuyển phát được tin cậy bởi bên gửi để chấp nhận một thông điệp từ nó và tiếp đó nó nỗ lực cố gắng để chuyển phát thông điệp này. Khi chấp nhận thông điệp, tổ chức chuyển phát cung cấp bằng chứng về việc đệ trình thông điệp bởi bên gửi. Tổ chức chuyển phát công nhận thực tế rằng thông điệp đã được đệ trình song không quan tâm đến nội dung thông điệp là gì.

11.5 Chống chối bỏ việc vận chuyển

Dịch vụ này yêu cầu sự tồn tại của tổ chức chuyển phát tham gia vào việc vận chuyển thông điệp giữa một bên gửi và một bên nhận. Tổ chức chuyển phát được tin cậy bởi bên gửi để chuyển phát một thông điệp tới nơi mà nó sẵn sàng để dùng cho bên nhận. Trong khi chuyển phát thông điệp, tổ chức chuyển phát cung cấp bằng chứng về việc ký gửi thông điệp trong thiết bị lưu dữ liệu của bên nhận. Tổ chức chuyển phát công nhận thực tế là thông điệp đã được ký gửi nhưng không chịu trách nhiệm về nội dung của thông điệp. Tổ chức chuyển phát không thể đảm bảo rằng thông điệp được nhận một cách đầy đủ bởi bên nhận.



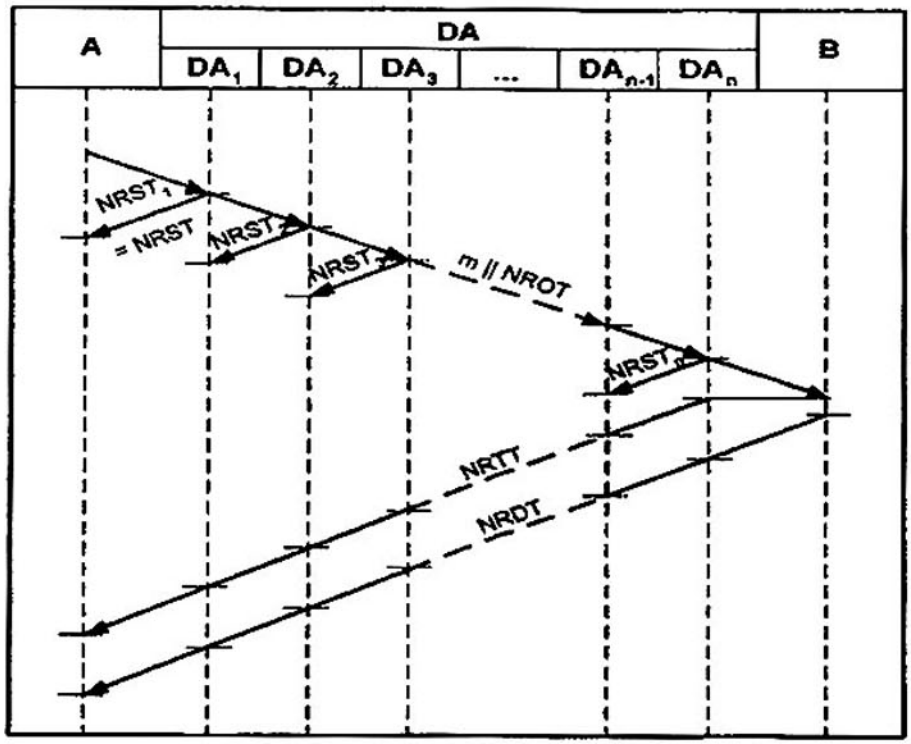
Hình 1 - Các dịch vụ chống chối bỏ cụ thể

12 Sử dụng các thẻ chống chối bỏ cụ thể trong môi trường chuyển thông điệp

Các thẻ chống chối bỏ (NROT, NRST, NRTT, NRDT) cho các dịch vụ chống chối bỏ cụ thể được thảo luận trong Điều nêu trên được định nghĩa trong các phần tiếp theo của tiêu chuẩn này sử dụng thẻ chống chối bỏ chung GNRT như đã trình bày ở Điều 10.1. Có bốn thẻ có thể được sử dụng theo cách thức sau, cụ thể là nếu hệ thống Tổ chức chuyển phát bao gồm một chuỗi của *n* tổ chức chuyển phát con DA_i, $i = 1... n$.

Mỗi tổ chức chuyển phát con DA_i tạo ra một thẻ chống chối bỏ việc đệ trình $NRST_i$ ở thời điểm nhận thông điệp từ thực thể đệ trình hoặc tổ chức chuyển phát trước đó. Điều này thiết lập một chuỗi các thẻ $NRST_i$ trung gian được lưu trữ như bằng chứng bởi bên nhận tương ứng của thẻ. Thẻ chống chối bỏ việc đệ trình đầu tiên $NRST_1$ được gửi tới bên gửi (nguồn phát) để giữ lại làm thẻ chống chối bỏ việc đệ trình *NRST*. Thẻ chống chối bỏ vận chuyển *NRTT* chỉ được tổ chức chuyển phát con cuối cùng DA_n tạo ra tại thời điểm cung cấp thông điệp tới thiết bị lưu dữ liệu của người nhận dự kiến (xem Hình 2).

Theo yêu cầu hoặc của chính sách chống chối bỏ hiện hành hoặc của nguồn phát, thực thể *B* thiết lập chống chối bỏ chuyển phát bằng cách tạo bằng chứng nhận về việc nhận thông điệp *m* và gửi lại thẻ chống chối bỏ chuyển phát *NRDT* về nguồn phát *A* để giữ lại làm bằng chứng trong trường hợp có tranh chấp.



Hình 2 - Các thủ tục dịch vụ chống chối bỏ (ví dụ)

Thư mục tài liệu tham khảo

[1] TCVN 9696-2:2013 *(ISO 7498-2:1989)* Công nghệ thông tin - Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 2: Kiến trúc an ninh.

[2] ISO/IEC 9594-8:2001, Information technology – Open Systems Interconnection – The Directory Public-Key and attribute certificate frameworks *(Công nghệ thông tin – Liên kết hệ thống mở – Bộ khung danh bạ khóa công khai và chứng thư thuộc tính).*

[3] ISO/IEC 9796 (all parts), Information technology – Security techniques – Digital signature schemes giving message recovery *(Công nghệ thông tin – Các kỹ thuật an toàn – Lược đồ chữ ký số cho khôi phục thông điệp).*

[4] ISO/IEC 9797 (all parts), Information technology – Security techniques - Message Authentication Codes MACs *(Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác thực thông điệp).*

[5] ISO/IEC 9798-1:1997, Information technology – Security techniques – Entity Authentication – Part 1: General *(Công nghệ thông tin - Các kỹ thuật an toàn – Xác thực cho thực thể - Phần 1: Tổng quan).*

[6] ISO/IEC 10118-1, Information technology – Security techniques - Hash-functions – Part 1: General *(Công nghệ thông tin – Các kỹ thuật an toàn – Các hàm băm – Phần 1: Tổng quan).*

[7] ISO/IEC 10181-1:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview *(Công nghệ thông tin – Liên kết hệ thống mở – Bộ khung an toàn cho các hệ thống mở: Tổng quan).*

[8] TCVN 7817-3:2007 (ISO/IEC 11770-3:1999) *Công nghệ thông tin – Kỹ thuật mật mã – Quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật phi đối xứng.*

[9] TCVN 11393-2:2016 (ISO/IEC 13888-2:2010) *Công nghệ thông tin – Các kỹ thuật an toàn – Chống chối bỏ – Phần 2: Các cơ chế sử dụng các kỹ thuật đối xứng*

[10] ISO/IEC TR 14516, Information technology – Security techniques – Guidelines for use and management of Trusted Third Party services *(Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn sử dụng và quản lý các dịch vụ của bên thứ ba tin cậy).*

[11] ISO/IEC 14888 (all parts), Information technology – Security techniques – Digital signatures with appendix *(Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số với phụ lục).*

[12] ISO/IEC 15496 (all parts), Information technology – Security techniques – Cryptographic techniques based on elliptic curves *(Công nghệ thông tin – Các kỹ thuật an toàn – Các kỹ thuật mật mã dựa trên đường cong elliptic).*