TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13722:2023
ISO/IEC 17922:2017

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – KHUNG XÁC THỰC VIỄN SINH TRẮC SỬ DỤNG MÔ-ĐUN AN TOÀN PHẦN CỨNG SINH TRẮC HỌC

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

HÀ NỘI – 2023

Mục lục

Lời nói đầu

TCVN 13722:2023 hoàn toàn tương đương với ISO/IEC 17922:2017.

TCVN 13722:2023 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố

TCVN 13722:2023 mô tả sơ đồ xác thực sinh trắc học từ xa sử dụng mô-đun an toàn phần cứng sinh trắc học (biometric hardware security module - BHSM) để xác thực viễn sinh trắc học dựa trên việc chứng minh chủ sở hữu chứng thư ITU-T X.509 đã đăng ký cá nhân tại thẩm quyền đăng ký (registration authority - RA).

Tiêu chuẩn này cung cấp các yêu cầu cho triển khai các mô-đun an toàn phần cứng sinh trắc học để vận hành an toàn xác thực từ xa trong môi trường PKI. Tập trung vào

Giới thiệu

Tiêu chuẩn này mô tả sơ đồ xác thực viễn sinh trắc, sử dụng mô-đun an toàn phần cứng sinh trắc học (BHSM) cho xác thực viễn sinh trắc của người xuất trình BHSM với tư cách là chủ sở hữu chứng thư ITU-T X.509 đã đăng ký với tổ chức chứng thực (CA) được nhúng trong BHSM đó. Tiêu chuẩn này cung cấp các yêu cầu để triển khai mô hình BHSM phục vụ cho việc xác thực từ xa đảm bảo an toàn trong môi trường cơ sở hạ tầng khóa công khai (PKI). Mô hình này cung cấp sự đảm bảo cho xác thực viễn sinh trắc bằng cách sử dụng nhận dạng sinh trắc học được tích hợp vào một mô-đun an toàn phần cứng. Đồng thời cung cấp các định dạng ASN.1 cho phép kết hợp xác thực sinh trắc học vào khung ITU-T X.509 để xác thực người dùng là chủ sở hữu của chứng thư ITU-T X.509.

Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viễn sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học

Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module

1 Phạm vi áp dụng

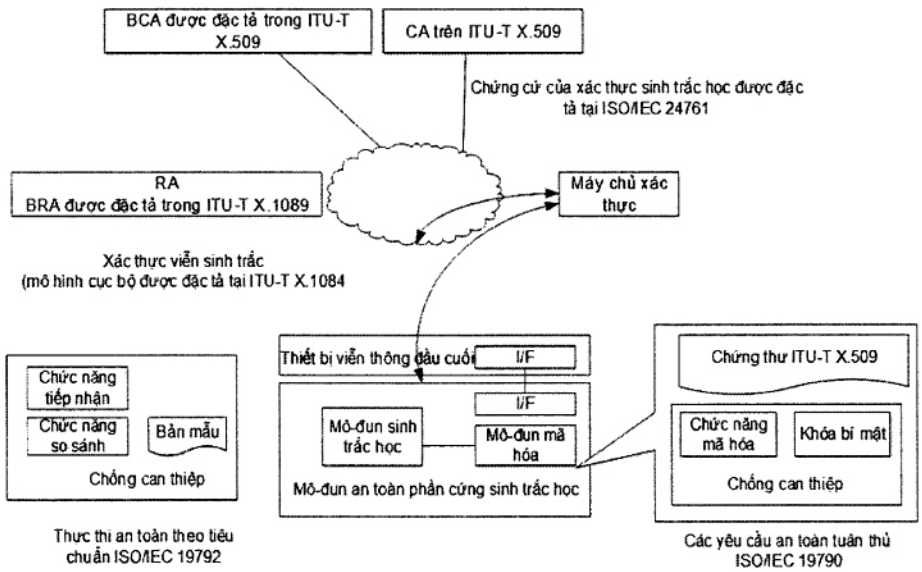
Để chứng minh quyền sở hữu, chứng thư ITU-T X.509 được đăng ký riêng lẻ với thẩm quyền đăng ký (RA), mô-đun an toàn phần cứng sinh trắc học được coi là nền tảng cung cấp xác thực sinh trắc học. Tiêu chuẩn này cung cấp một khung để xác thực viễn sinh trắc bằng BHSM.

Trong phạm vi của Tiêu chuẩn này, các vấn đề sau được đề cập:

- Cơ chế xác thực viễn sinh trắc sử dụng BHSM trong môi trường mạng viễn thông;
- Định dạng và giao thức của ASN.1 (abstract syntax notation one - Ký hiệu cú pháp trừu tượng 1).

Môi trường tiêu chuẩn liên quan được mô tả trong Hình 1. Vai trò chính của Tiêu chuẩn này là phù hợp với các tiêu chuẩn xác thực viễn sinh trắc và cơ sở hạ tầng khóa công khai (PKI) hiện có và thiết lập một tiêu chuẩn cơ chế sử dụng BHSM để xác minh quyền sở hữu chứng thư ITU-T X.509 trong môi trường viễn sinh trắc.

Chú thích – Trong Tiêu chuẩn này, chứng thư ITU-T X.509 nghĩa là chứng thư khóa công khai ITU-T X.509.



Hình 1 – Môi trường tiêu chuẩn cho BHSM.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. 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, bổ sung (nếu có).

2.1 Tương đồng với Khuyến nghị | Tiêu chuẩn Quốc tế

Khuyến nghị ITU-T X.509 (2016) | ISO/IEC 9594-8:2016, Công nghệ thông tin - Kết nối hệ thống mở - Thư mục: Khoá công khai và các khung chứng thư thuộc tính.

2.2 Kết hợp Khuyến nghị | Tiêu chuẩn quốc tế tương đương về nội dung kỹ thuật

Không.

2.3 Tài liệu tham khảo bổ sung

ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection *(Công nghệ thông tin – Các kỹ thuật an toàn – Bảo vệ thông tin sinh trắc học).*

TCVN 12042:2017 (ISO 24761:2009/ Cor 1:2013) về Công nghệ thông tin - Các kỹ thuật an toàn - Ngữ cảnh xác thực cho sinh trắc học.

TCVN 11295:2016 (ISO 19790:2012) về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã.

TCVN 11385:2016 (ISO/IEC 19792:2009) về Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học.

3 Thuật ngữ và định nghĩa

3.1 Các thuật ngữ được định nghĩa trong Tiêu chuẩn này

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1.1

Mô-đun an toàn phần cứng sinh trắc học (biometric hardware security module)

Mô-đun an toàn phần cứng kết hợp cảm biến sinh trắc học và nhận dạng sinh trắc học để xác thực người dùng.

CHÚ THÍCH - Trong trường hợp so sánh giữa các mô-đun an toàn phần cứng sinh trắc học, các mô-đun này thường ở dạng thẻ thông minh, nhưng thời gian gần đây có cả ở dạng thiết bị USB là token an toàn và có thể được gắn trực tiếp vào các máy tính đa năng.

3.1.2

Mô-đun an toàn phần cứng (hardware security module)

Phần cứng thực thi bộ xử lý mật mã an toàn, sử dụng chứng thư ITU-T X.509 và khóa bí mật để cung cấp xác thực an toàn.

3.1.3

Xác thực viễn sinh trắc (telebiometric authentication)

Xác thực sinh trắc học sử dụng giao tiếp dữ liệu bằng điện thoại, radio hoặc một công nghệ liên quan.

3.2 Các thuật ngữ được định nghĩa trong các tiêu chuẩn quốc tế khác

3.2.1 Các thuật ngữ sau được định nghĩa trong ISO/IEC 2382-37:

3.2.1.1

Tham chiếu sinh trắc học (biometric reference)**:**

Một hoặc nhiều mẫu sinh trắc học được lưu trữ, các mẫu sinh trắc học hoặc các mô hình sinh trắc học đặc trưng cho một chủ thể dữ liệu sinh trắc học và được sử dụng làm đối tượng so sánh sinh trắc học.

3.2.1.2

Mẫu sinh trắc học (biometric sample)**:**

Biểu diễn đặc tính sinh trắc học dưới dạng tương tự hoặc kỹ thuật số trước khi trích xuất sang đặc tính sinh trắc học.

3.2.2 Các thuật ngữ được định nghĩa trong ISO/IEC 9798-1:

3.2.2.1

Xác thực thực thể (entity authentication):

Chứng thực rằng thực thể này là một thực thể đã được khai báo.

3.2.3 Các thuật ngữ được định nghĩa trong ISO/IEC 24745:

3.2.3.1

Tham chiếu danh tính (identity reference):

Là một thuộc tính phi sinh trắc và là một định danh với giá trị giữ nguyên trong suốt thời gian tồn tại của thực thể trong một miền.

3.2.3.2

Biệt danh (pseudonymous identifier):

Một phần của tham chiếu sinh trắc học, có thể làm tham chiếu đại diện cho một cá nhân hoặc chủ thể dữ liệu trong một miền nhất định thông qua một danh tính được bảo vệ, có thể được xác minh bằng mẫu sinh trắc học thu được và dữ liệu bổ trợ (nếu có).

3.2.3.3

Làm mới (renewability)**:**

Thuộc tính của sự chuyển đổi hoặc quy trình để tạo nhiều tham chiếu sinh trắc học, được biến đổi độc lập có nguồn gốc từ một hoặc nhiều mẫu sinh trắc học thu được từ cùng một đối tượng dữ liệu và có thể được sử dụng để nhận ra cá nhân trong khi không tiết lộ thông tin về tham chiếu ban đầu.

3.2.3.4

Tham chiếu sinh trắc học làm mới (renewable biometric reference):
Định danh có thể được gỡ bỏ hoặc làm mới đại diện cho một cá nhân hoặc đối tượng dữ liệu trong một miền nhất định bằng danh tính nhị phân được bảo vệ và được xây dựng (lại) từ mẫu sinh trắc học đã thu thập được.

CHÚ THÍCH - Tham chiếu sinh trắc học làm mới bao gồm một số Biệt danh và các phần tử dữ liệu tùy chọn bổ sung cần thiết để xác minh hoặc nhận dạng sinh trắc học, chẳng hạn như dữ liệu phụ trợ.

3.2.3.5

Khả năng thu hồi (revocability):

Khả năng ngăn cản việc xác minh thành công trong tương lai của một tham chiếu sinh trắc học xác định và tham chiếu danh tính tương ứng.

4 Ký hiệu và thuật ngữ viết tắt

Vì mục đích của Tiêu chuẩn này, các từ viết tắt sau đây được áp dụng:

ACBio	Authentication Context for Biometrics	Ngữ cảnh xác thực cho sinh trắc học
ASN.1	Abstract Syntax Notation One	Ký hiệu cú pháp trừu tượng 1
BCA	Biometric Certificate Authority	Tổ chức có thẩm quyền chứng thực sinh trắc học
BHSM	Biometric Hardware Security Module	Mô-đun an toàn phần cứng sinh trắc học
BIR	Biometric Information Record	Bản ghi thông tin sinh trắc học
BRA	Biometric Registration Authority	Tổ chức có thẩm quyền đăng ký sinh trắc học
BRT	Biometric Reference Template	Mẫu tham chiếu sinh trắc học
BR	Biometric Reference	Tham chiếu sinh trắc học
CA	Certification Authority	Tổ chức có thẩm quyền chứng thực
CSR	Certificate Signing Request	Yêu cầu ký chứng thư
DN	Distinguished Name	Tên phân biệt
EPSID	Encrypted PSID	PSID được mã hóa
HSM	Hardware Security Module	Thiết bị an toàn phần cứng
I/F	Interface	Giao diện

IR	Identity Reference	Tham chiếu danh tính
OID	Object Identifier	Định danh đối tượng
PIN	Personal Identification Number	Số nhận dạng cá nhân
PKI	Public-Key Infrastructure	Cơ sở hạ tầng khóa công khai
PSID	Pseudonymous Identifier	Biệt danh
RA	Registration Authority	Tổ chức có thẩm quyền đăng ký
RBR	Renewable Biometric Reference	Tham chiếu sinh trắc học làm mới
USB	Universal Serial Bus	USB

CHÚ THÍCH 1 - trong Tiêu chuẩn này, biệt danh (PSID) chính là PI trong ISO/IEC 24745.

CHÚ THÍCH 2 - BRT chỉ được sử dụng trong chứng thư BRT.

5 Ký hiệu và định nghĩa

Vì mục đích của tiêu chuẩn này, các quy ước sau đây áp dụng cho các biểu thức toán học.

E Hàm mã hóa

H Hàm băm

P_k Khóa kiểm tra chữ ký số

R Chuỗi bit ngẫu nhiên

R_a Chuỗi bit ngẫu nhiên sử dụng để thực thi thử thách/phản hồi giữa CA và mô-đun an toàn phần cứng sinh trắc học (BHSM)

Sign Ký số

S_k Khóa tạo chữ ký số (khóa bí mật)

6 Mô-đun an toàn phần cứng sinh trắc học cho xác thực viễn sinh trắc

6.1 Tính năng bổ sung của BHSM cho HSM

Một mô-đun an toàn phần cứng (HSM) quản lý và bảo vệ các khóa bí mật quan trọng bằng cách sử dụng ký số nhằm mục đích cung cấp xác thực mạnh. Các HSM là các thiết bị vật lý thường ở dạng thẻ thông minh hoặc USB có khả năng chống can thiệp với sự xâm nhập và sửa đổi hoạt động nội bộ, hay chèn cơ chế tiếp cận chủ động hoặc thụ động để tiết lộ dữ liệu bí mật, cũng như thay đổi hoạt động của các thiết bị.

Phần lớn các tài nguyên mật mã được xử lý chính bởi HSM là các cặp khóa công khai/bí mật (và chứng thư) được sử dụng trong mật mã khóa công khai liên quan đến chứng thư ITU-T X.509 được sử dụng, ví dụ: mã hóa/giải mã và chữ ký số. Nếu khóa bí mật bị lộ, các chứng thư và chữ ký điện tử không còn tính tin cậy và các giao dịch sử dụng HSM có thể là gian lận với các tiềm ẩn có tác động bất lợi nghiêm trọng có thể xảy ra đối với chủ sở hữu khóa và các bên khác trong giao dịch. An toàn vật lý ở mức cao, khi HSM được đảm bảo thực thi đúng cách.

Tuy nhiên, an toàn vật lý chỉ là một nhân tố trong an toàn tổng thể cho quá trình xác thực. An toàn tổng thể là hạn chế cuối cùng với sự đảm bảo HSM đang được sử dụng bởi chủ sở hữu hợp pháp của nó. Thông thường, sự ràng buộc của HSM với chủ sở hữu được cung cấp bằng mã PIN hoặc mật khẩu mà chỉ chủ sở hữu hợp pháp mới biết. Độ mạnh của mật khẩu thường được coi là thấp vì mật khẩu có thể bị lộ do vô tình hoặc bất cẩn từ phía chủ sở hữu, do cố ý tiết lộ hoặc do các cuộc tấn công vật lý vào cơ sở dữ liệu mật khẩu. Việc sử dụng xác thực sinh trắc học để tăng cường hoặc thay thế mật khẩu hay mã PIN có thể cung cấp ràng buộc mạnh mẽ hơn và tăng cường tính xác thực.

Khi một HSM chứa khóa bí mật được sử dụng để xác thực dựa trên cơ sở hạ tầng khóa công khai (PKI), cá nhân người xác minh chỉ có thể kiểm tra xem chứng thư HSM có thuộc về chủ sở hữu hợp pháp đã biết hay không. Tuy nhiên, nó không thể xác nhận rằng người sử dụng HSM và tự xưng là chủ sở hữu của nó là chủ sở hữu hợp pháp. Nếu HSM thuộc quyền sở hữu của một người khác, trong trường hợp cố tình hay vô tình làm lộ mật khẩu như: được chuyển giao cho người khác; có sự thông đồng giữa các bên; bị tấn công và phát hiện, thì HSM có thể được sử dụng để thực hiện các giao dịch gian lận. Mô-đun an toàn phần cứng sinh trắc học là một HSM sử dụng sinh trắc học để xác thực người dùng cục bộ vào mô-đun nhằm cung cấp thêm sự đảm bảo cho các giao dịch.

6.2 Kịch bản chung để sử dụng BHSM

Việc sử dụng BHSM được giới hạn trong việc xác thực người sử dụng các dịch vụ đối với các nhà cung cấp dịch vụ. Vì vậy, nó trở thành một phần của hệ thống lớn hơn cho việc cung cấp các dịch vụ và người dùng truy cập vào các dịch vụ. Trong dạng tình huống này, người dùng tương tác với dịch vụ thông qua giao diện máy khách (I/F), ví dụ: máy tính cá nhân hoặc thiết bị di động. BHSM được kết nối với khách hàng và các tín hiệu điện chuyển giữa BHSM và người dùng, hay giữa dịch vụ chuyển qua khách hàng với tư cách là người trung gian.

Máy khách kết nối với dịch vụ thông qua liên kết hoặc mạng viễn thông, ví dụ: Internet. Phần mô tả và giao thức trong Tiêu chuẩn này giới thiệu đến dữ liệu và lệnh được trao đổi giữa người dùng và BHSM hoặc BHSM và dịch vụ, nó được hiểu là được định tuyến thông qua máy khách. Trong một số trường hợp, BHSM sẽ là một thiết bị vật lý riêng biệt kết nối với máy khách. Trong các trường hợp khác, BHSM có thể được nhúng vào máy khách (ví dụ: điện thoại di động) nhưng trong cả hai trường hợp, BHSM được coi là một phần riêng và là mô-đun riêng, tách biệt.

Có thể có các cơ chế tại chỗ để bảo vệ thông tin liên lạc giữa khách hàng và dịch vụ nhưng những cơ chế này không được Tiêu chuẩn này đề cập đến. Các biện pháp và giao thức an toàn được mô tả trong Tiêu chuẩn này chỉ quan tâm đến việc xác thực của người dùng đối với dịch vụ sử dụng BHSM. Điều này bao gồm các biện pháp để đảm bảo giao tiếp end-to-end an toàn giữa BHSM và dịch vụ sao cho, ví dụ, kẻ mạo danh không thể xác thực dịch vụ với tư cách là người dùng được ủy quyền bằng cách đánh cắp hay giả mạo BHSM hoặc khách hàng.

6.3 Xác thực viễn sinh trắc sử dụng BHSM

Xác thực viễn sinh trắc có thể cung cấp xác thực người dùng an toàn bằng cách sử dụng xác thực sinh trắc học qua mạng mở nhưng trong một số mô hình, thông tin sinh trắc học phải được truyền đến máy chủ xác thực thông qua mạng mở. Khi sử dụng sinh trắc học, cần phải cân nhắc đến tính an toàn và quyền riêng tư của thông tin sinh trắc học. Cuối cùng, việc tích hợp xác thực sinh trắc học với HSM có thể là một giải pháp vì thông tin sinh trắc học có thể vẫn nằm trong tầm kiểm soát của người dùng với một mô-đun chống can thiệp. Trong trường hợp này, các tham chiếu sinh trắc

học được lưu trữ duy nhất trong BHSM chứ không phải trên máy chủ xác thực và không bắt buộc phải chuyển qua mạng mở. Cần cân nhắc việc sử dụng các tham chiếu sinh trắc học làm mới (RBR) và biệt danh để nếu một tham chiếu sinh trắc học (BR) bị lộ, nó có thể bị hủy bỏ và cung cấp một tham chiếu mới cho người dùng cùng với một biệt danh mới. Việc sử dụng các tham chiếu sinh trắc học làm mới và các biệt danh đảm bảo chống lại việc dữ liệu sinh trắc học của các tham chiếu sinh trắc học đã bị thu hồi có thể được trích xuất từ biệt danh.

Sơ đồ xác thực viễn sinh trắc dựa trên BHSM được mô tả trong Tiêu chuẩn này dựa trên PKI hiện có và cần được tích hợp với nó một cách thích hợp. Tiêu chuẩn này hỗ trợ các cặp khóa phi đối xứng sử dụng hệ mật RSA hoặc các loại mật mã khác hỗ trợ mã hóa/giải mã. Tiêu chuẩn này mô tả phương pháp để ràng buộc thông tin sinh trắc học của người dùng đã đăng ký của BHSM với chứng thư ITU-T X.509.

Các giao thức hoạt động và giao dịch BHSM được mô tả trong Tiêu chuẩn này liên quan đến các vai trò sau:

- Một người dùng, một chủ sở hữu BHSM có chứng thư ITU-T X.509 và tham chiếu sinh trắc học được lưu trữ trong BHSM;

- Một máy chủ xác thực và một bên phụ thuộc có yêu cầu xác thực cho người dùng;

- Một tổ chức có thẩm quyền đăng ký cần đăng ký tham chiếu sinh trắc học của người dùng và cung cấp thông tin nhận dạng sinh trắc học được lưu trữ trong BHSM của người dùng;

- Một tổ chức chứng thực (CA) cấp chứng thư ITU-T X.509 của người dùng.

Trong Tiêu chuẩn này, các khuyến nghị sau đây được nêu ra.

- CA phải có khả năng cung cấp chứng thư ITU-T X.509 với PSID;

- CA không được sử dụng tham chiếu sinh trắc học gốc của người dùng ở bất kỳ đâu trong chứng thư khóa công khai, để tránh khả năng tiết lộ dữ liệu sinh trắc học riêng tư của người dùng;

- Để bảo vệ thông tin có thể nhận dạng cá nhân và quyền riêng tư của người dùng, dữ liệu sinh trắc học của người dùng không được rời khỏi BHSM. Trong quá trình đăng ký và xác thực sinh trắc học, chỉ PSID mới được rời khỏi BHSM.

7 Xác thực viễn sinh trắc với mô-đun an toàn phần cứng sinh trắc học

7.1. Quy định chung

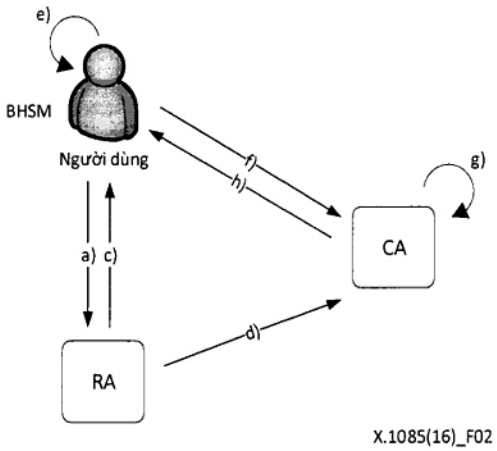
Tiêu chuẩn này mô tả hai phương pháp đăng ký thành viên và xác thực bằng BHSM. Đầu tiên là mô tả giao thức sử dụng phần mở rộng chứng thư ITU-T X.509 để chứa thông tin nhận dạng người dùng. Thứ hai là mô tả một giao thức đã sửa đổi sử dụng chứng thư ITU-T X.509 kết hợp với bối cảnh xác thực ISO/IEC 24761 đối với triển khai xác thực sinh trắc học (ACBio - authentication context for biometrics).

Tính toàn vẹn và sự đảm bảo của việc đăng ký thành viên phụ thuộc vào mối quan hệ tin cậy giữa RA và CA, cũng như các thủ tục để đăng ký thành viên được thực hiện hoàn toàn dưới sự giám sát liên tục của RA. RA trong PKI có vai trò hạn chế hơn nhiều so với RA được đặc tả trong Tiêu chuẩn này. Vì vậy, đây là một giả định trong các thủ tục đăng ký được mô tả trong 7.2.1 và 7.2.2. Lưu ý rằng nếu các điều kiện này không được thực hiện, tính toàn vẹn và đảm bảo của việc đăng ký thành viên có thể bị ảnh hưởng.

7.2.Các thủ tục để đăng ký thành viên

7.2.1 Thủ tục đăng ký thành viên sử dụng mở rộng chứng thư ITU-T X.509

Quy trình đăng ký thành viên để cấp một BHSM chứa chứng thư ITU-T X.509 được thể hiện trong Hình 2. Để đảm bảo an toàn, toàn bộ quy trình đăng ký thành viên được mô tả trong các bước từ a) tới h) dưới đây phải được đặt dưới sự kiểm soát của RA. Mô tả chi tiết về các chữ ký số chống chối bỏ, xem ISO/IEC 15945.



Hình 2 – Quy trình đăng ký thành viên với BHSM

a) Người dùng trực tiếp tới RA, tại đó định danh và quyền đăng nhập của họ đã được thiết lập. Các đặc điểm sinh trắc học của người dùng có liên quan được thu thập và tham chiếu sinh trắc học được tạo cho người dùng. RA cung cấp BHSM cho người dùng và lưu trữ tham chiếu sinh trắc học của người dùng trong BHSM;

b) RA tạo PSID – xem 8.1.2 để biết thêm thông tin về cách tạo PSID

c) RA lưu trữ PSID trong BHSM của người dùng;

d) RA gửi PSID đã tạo tới CA;

e) Sau khi người dùng thực hiện xác thực sinh trắc học thành công đối với BHSM, người dùng sẽ tạo khóa bí mật và khóa công khai của mình trong BHSM;

f) Người dùng tạo yêu cầu ký chứng thư (CSR - certificate signing request) tới CA yêu cầu chứng thư ITU-T X.509 sau khi xác thực sinh trắc học thành công bằng BHSM;

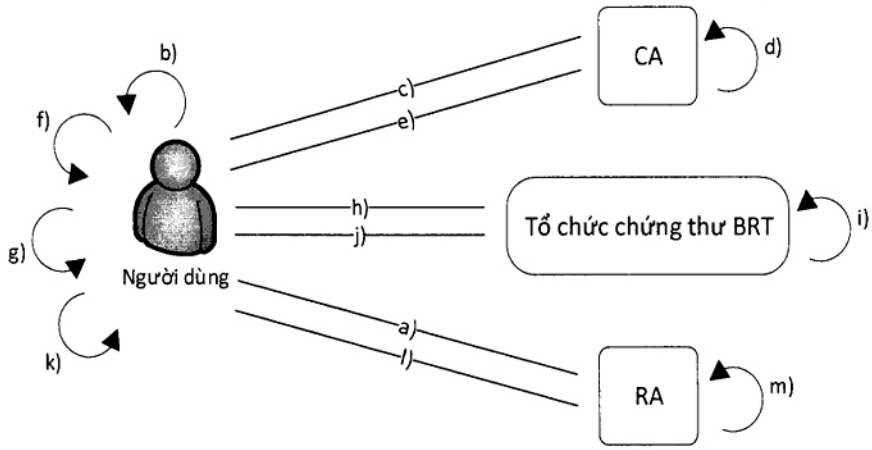
g) CA tạo chứng thư ITU-T X.509 của người dùng bao gồm PSID trong trường mở rộng subjectAltName có chứa directoryName;

h) CA gửi chứng thư ITU-T X.509 của người dùng, chứng thư này sau đó sẽ được lưu trữ an toàn trong BHSM của người dùng

CHÚ THÍCH - Trong Tiêu chuẩn này, vai trò của khóa công khai và khóa bí mật của người dùng không được mô tả chi tiết vì chúng sẽ được sử dụng cho các hệ thống mật mã khóa công khai thông thường như mã hóa/giải mã và chữ ký số. Ngoài ra, phương pháp ký và mật mã khóa công khai chính xác được sử dụng sẽ phụ thuộc vào hệ thống mật mã được chọn (ví dụ: RSA hay hệ mật trên Đường cong Elliptic).

7.2.2. Quy trình đăng ký thành viên áp dụng ISO/IEC 24761

Quy trình đăng ký thành viên để cấp chứng thư ITU-T X.509 và chứng thư mẫu tham chiếu sinh trắc học (BRT), được đặc tả trong ISO / IEC 24761, để sử dụng BHSM được mô tả trong Hình 3. Trong Hình 3, toàn bộ tập thủ tục của quy trình đăng ký được mô tả. Để đảm bảo an ninh, toàn bộ quá trình đăng ký phải được thực hiện dưới sự kiểm soát của RA



Hình 3 – Quy trình đăng ký thành viên với BHSM sử dụng ACBBio

a Người dùng trực tiếp tới RA, trên đó định danh và cấp quyền đăng nhập của họ đã được thiết lập;

b) Người dùng tạo cặp khóa công khai và khóa bí mật trong BHSM;

c) Người dùng gửi yêu cầu cấp chứng thư ITU-T X.509 tới CA;

d) CA tạo chứng thư ITU-T X.509 theo yêu cầu;

e) CA gửi chứng thư ITU-T X.509 tới người dùng;

f) Người dùng lưu trữ chứng thư ITU-T X.509 trong BHSM;

g) Người dùng tạo tham chiếu sinh trắc học và phiên bản ACBio để đăng ký thành viên;

h) Người dùng gửi yêu cầu cấp chứng thư BRT với các giá trị của serialNumber và tổ chức phát hành trong chứng thư ITU-T X.509 và phiên bản ACBio để đăng ký thành viên với tổ chức chứng thư BRT;

i) Tổ chức chứng thư BRT tạo chứng thư BRT, đặt giá trị của serialNumber vào trường pkiCertificateSerialNumber, giá trị của người cấp cho trường pkiCertificateIssuerName và phiên bản ACBio để đăng ký thành viên vào trường enrolmentACBioInstances tương ứng;

j) Tổ chức chứng thư BRT gửi chứng thư BRT tới người dùng;

k) Người dùng lưu trữ chứng thư BRT cũng như tham chiếu sinh trắc học trong BHSM;

l) Người dùng gửi chứng thư ITU-T X.509 và chứng thư BRT tới RA để đăng ký;

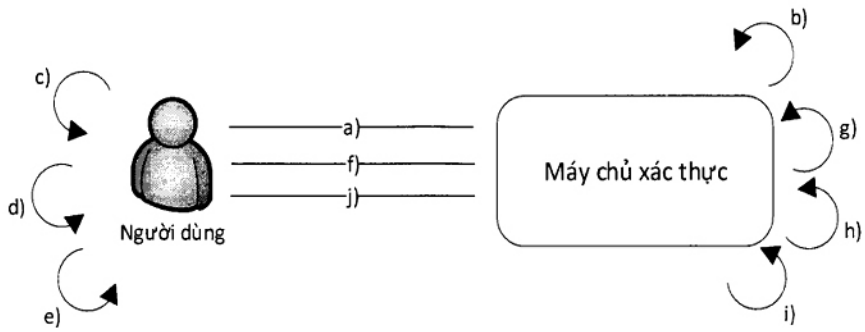
m) RA lưu trữ chứng thư ITU-T X.509 và chứng thư BRT trong cơ sở dữ liệu người dùng.

CHÚ THÍCH - Việc nhận dạng là cần thiết để cấp chứng thư ITU-T X.509 và chứng thư BRT nhưng quy trình nhận dạng bị bỏ qua trong phần mô tả ở trên.

7.3. Quá trình xác thực sinh trắc học

7.3.1. Quá trình xác thực sử dụng mở rộng của chứng thư ITU-T X.509

Quá trình viễn sinh trắc với BHSM có thể được mô tả như trong Hình 4, sơ đồ thông tin chi tiết hơn của BHSM và nhà cung cấp dịch vụ được mô tả trong Hình 5, thử thách phản hồi được thêm vào để bảo vệ cuộc tấn công phát lại



Hình 4 – Xác thực viễn sinh trắc với BHSM

a) Người dùng truy cập một dịch vụ tại máy chủ xác thực

b) Máy chủ xác thực tạo ra một số ngẫu nhiên R_a như một thử thách. Thử thách này được gửi đến hệ thống người dùng và đầu vào BHSM

c) Người dùng thực hiện xác thực sinh trắc học cục bộ sử dụng mô-đun sinh trắc học trong BHSM;

d) BHSM lấy PSID và thử thách R_a, đồng thời tính toán chữ ký số bằng cách ghép hai dữ liệu này sử dụng *sk,* khóa bí mật của BHSM;

e) Chữ ký số được tạo trong bước d) được mã hóa, sử dụng khóa công khai của máy chủ xác thực;

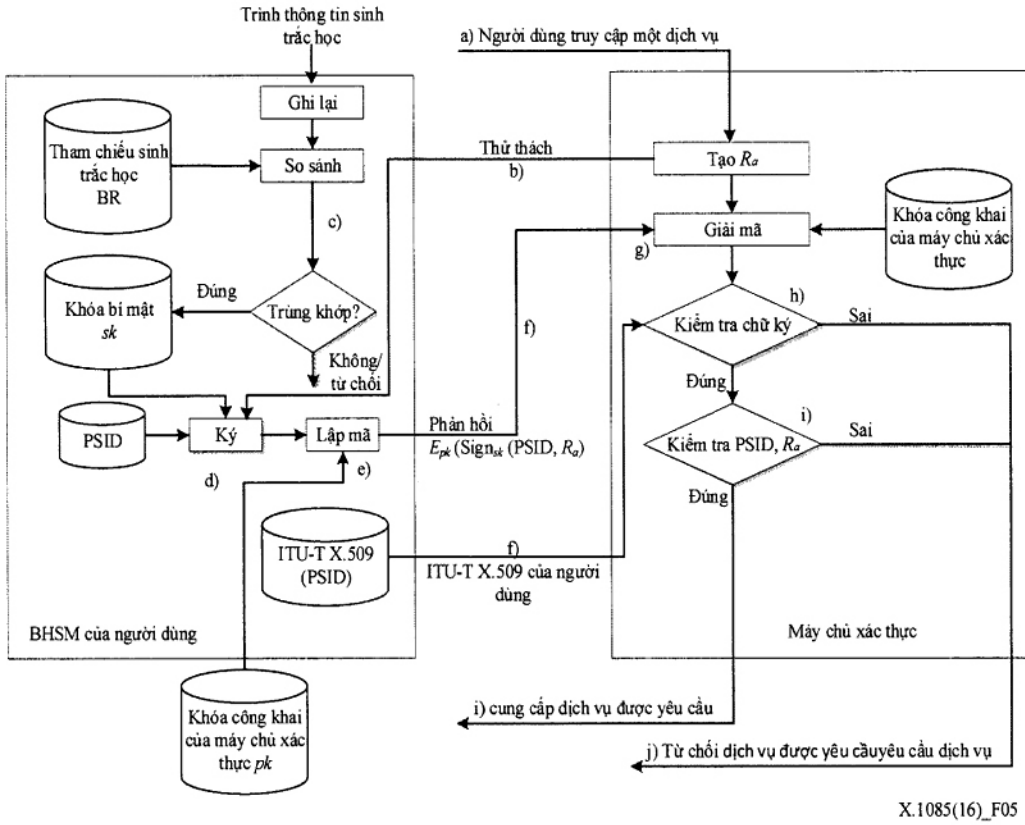
f) Sau khi người dùng xác thực thành công, BHSM gửi dữ liệu mã hóa đã ký số của R_a và PSID đã tạo ở bước d) và e) tới máy chủ xác thực. Chứng thư ITU-T X.509 cũng được gửi đi trong quá trình này;

g) Máy chủ xác thực sử dụng khóa bí mật của nó để giải mã thông điệp;

h) Máy chủ xác thực xác minh chữ ký với chứng thư ITU-T X.509 của BHSM sử dụng khóa công khai của nó;

i) Chủ sở hữu của chứng thư ITU-T X.509 được xác thực bởi máy chủ xác thực qua việc so sánh PSID trong chứng thư ITU-T X.509 và R_a được tạo ở bước b) với PSID được lấy ra và R_a trong bước g) tương ứng;

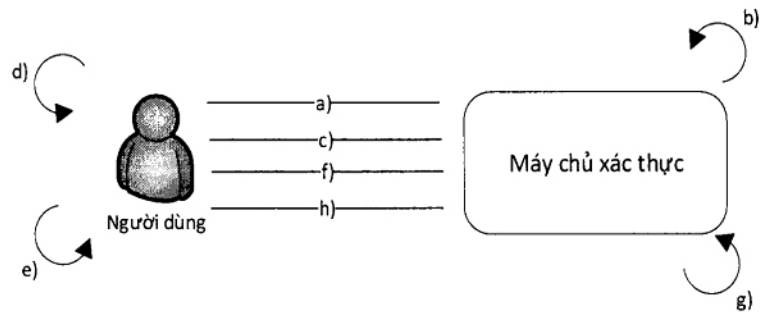
j) Nếu xác thực thành công, máy chủ xác thực sẽ cung cấp dịch vụ mà người dùng yêu cầu, ngược lại máy chủ xác thực sẽ từ chối dịch vụ được người dùng yêu cầu.



Hình 5 – Luồng thông tin trong xác thực viễn sinh trắc với BHSM

7.3.2. Quá trình xác thực áp dụng ISO/IEC 24761

Tiêu chuẩn này có thể áp dụng ISO/IEC 24761 để kiểm tra tính hợp lệ của kết quả của quá trình xác minh sinh trắc học được thực hiện trong BHSM. Quá trình xác thực viễn sinh trắc với BHSM sử dụng ACBio được mô tả trong Hình 6.



Hình 6 – Quy trình xác thực viễn sinh trắc với BHSM sử dụng ACBio

a) Người dùng truy cập tới một dịch vụ tại máy chủ xác thực;

b) Máy chủ xác thực tạo một số ngẫu nhiên R_a là một thử thách;

c) Máy chủ xác thực gửi thử thách tới người dùng;

d) Người dùng thực hiện xác thực sinh trắc học bằng BHSM và một thể hiện ACBio được tạo trong BHSM với thử thách được đặt trong trường controlValue nếu xác thực sinh trắc học thành công

e) Phản hồi là chữ ký số lên thử thách, được tạo trong BHSM với khóa bí mật của người dùng;

f) Phản hồi và một phiên bản ACBio được gửi tới máy chủ xác thực;

g) Máy chủ xác thực thực hiện xác thực phản hồi và phiên bản ACBio;

h) Dịch vụ được cung cấp cho người dùng từ máy chủ xác thực nếu cả hai quá trình xác minh và xác thực thành công

8. Quy trình xác thực viễn sinh trắc dựa trên BHSM.

8.1 Tạo PSID và chứng thư ITU-T X.509

8.1.1 Đăng ký tham chiếu sinh trắc học

Sau khi một người dùng được định danh đúng và xác thực thành công, các đặc điểm sinh trắc học có liên quan của họ sẽ được thu thập. Một tham chiếu sinh trắc học tương ứng được RA tạo ra và được lưu trữ trong BHSM để sử dụng sau này nhằm xác thực người dùng với BHSM. Tham chiếu sinh trắc học phải được bảo vệ theo các yêu cầu về tính an toàn, tính toàn vẹn, khả năng làm mới/thu hồi và yêu cầu riêng tư đối với ứng dụng. ISO/IEC 24745 cung cấp các hướng dẫn về quản lý và xử lý thông tin sinh trắc học an toàn và tuân thủ quyền riêng tư

8.1.2. Tạo PSID

8.1.2.1. Quy định chung

Cần có định danh người dùng để định danh người dùng được ủy quyền của BHSM. Định danh này sẽ được ràng buộc với chứng thư ITU-TX.509 của người dùng. Định danh phải là duy nhất trong miền ứng dụng của BHSM. Nó có thể được tạo ra dưới bất kỳ hình thức thích hợp nào tùy theo yêu cầu của ứng dụng. Đó có thể là thông tin nhận dạng cá nhân cho phép biết được danh tính thực sự của người dùng cần được biết; cách khác, nó có thể là một biệt danh và không được liên kết với danh tính thực của người dùng nhưng cho phép liên kết các giao dịch với những người dùng có biệt danh trong miền ứng dụng của BHSM.

PSID được sử dụng với BHSM là biệt danh của người dùng tuân theo các yêu cầu sau:

- PSID phải là duy nhất trong bối cảnh sử dụng BHSM;
- Quá trình đăng ký phải đảm bảo rằng giá trị PSID có trong chứng thư ITU-T X.509 là đúng giá trị PSID được lưu trữ trong BHSM.

8.1.2.2. Tạo PSID bằng cách sử dụng tham chiếu sinh trắc học của người dùng

Một phương pháp tạo PSID là dựa trên tham chiếu sinh trắc học của người dùng với dữ liệu bổ sung để cung cấp khả năng làm mới và xử lý nhằm bảo vệ dữ liệu cá nhân và sự riêng tư của người dùng. Việc triển khai được đặc tả trong Tiêu chuẩn này.

Một số ngẫu nhiên an toàn (ít nhất 160 bit) phải được tạo đúng cách và được sử dụng cùng với tham chiếu sinh trắc học để tạo PSID. RA sẽ tạo PSID để đưa vào chứng thư ITU-T X.509 như sau:

PSID =*h*(BR, *R*)

trong đó BR là tham chiếu sinh trắc học được trích xuất từ người dùng, *R* là số ngẫu nhiên và *h* là hàm băm phù hợp. Một ví dụ về kiểu Cú pháp ký hiệu trừu tượng một (ASN.1) cho PSID được mô tả trong Phụ lục A. Sau khi PSID được tạo ra, RA sẽ phải lưu trữ an toàn PSID trong BHSM của người dùng và cũng sẽ được chuyển một cách an toàn đến CA.

8.1.3. Yêu cầu và cấp phát chứng thư số

Dưới sự kiểm soát của RA, BHSM yêu cầu CA cấp chứng thư ITU-T X.509 cho người dùng. Các thông tin sau đi kèm với yêu cầu:

a) Mã hóa PSID (EPSID) (với khóa công khai của CA);

b) Tên phân biệt của người dùng

CHÚ THÍCH – Tên phân biệt của người dùng (DN- distinguished name) có thể là chính PSID

c) Khóa công khai của người dùng

d) Các chi tiết về thuật toán sinh khóa công khai / bí mật được sử dụng

e) Thời hạn hiệu lực của chứng thư

Để đưa EPSID vào thông điệp yêu cầu ký chứng thư số, EPSID phải được triển khai và lưu theo định dạng được mô tả trong Phụ lục A

PSID được mã hóa trong thông điệp yêu cầu ký chứng thư số cho CA như sau:

EPSID = E(PSID)

Tại đây, thuật toán mã hóa và khóa công khai có liên quan được trích xuất từ chứng thư phân phối khóa của CA. Kiểu ASN.1 cho EPSID được mô tả trong 8.3.

8.1.4. Gửi chứng thư ITU-T X.509 bao gồm PSID

Khi CA nhận được thông điệp yêu cầu chứng thư số, CA sẽ kiểm tra xem khóa tạo chữ ký số đang sở hữu có khớp với khóa xác minh chữ ký số của người dùng hay không. PSID được trích xuất bằng cách giải mã EPSID từ thông điệp yêu cầu chứng thư với khóa bí mật của CA. CA có thể kiểm tra tính đúng đắn của PSID được trích xuất bằng cách so sánh PSID nhận được từ RA. PSID sẽ được cấu hình như mô tả trong Phụ lục A và được chèn vào trường **subjectAltName** trong số các trường mở rộng của chứng thư ITU-T X.509. CA tạo chứng thư ITU-T X.509 của người dùng bao gồm PSID trong trường tiện ích mở rộng.

8.2. Quá trình xác thực viễn sinh trắc dựa trên BHSM

Người dùng yêu cầu một dịch vụ và được hướng dẫn đến máy chủ xác thực cho dịch vụ. Máy chủ xác thực tạo ra một số ngẫu nhiên R_a và gửi nó đến BHSM để sử dụng trong trao đổi thử thách/phản hồi nhằm chống tấn công phát lại. Người dùng đưa ra đặc điểm sinh trắc học có liên quan để xác thực cục bộ với BHSM. BHSM so sánh dữ liệu sinh trắc học đã thu được với tham chiếu sinh trắc học cho người dùng hợp lệ được lưu trữ trong BHSM. Nếu xác thực không thành công (sau một số lần thử cho phép), thì BHSM sẽ thông báo cho dịch vụ xác thực về việc xác thực không thành công và máy chủ xác thực chấm dứt giao dịch. Trong trường hợp đó, bất kỳ nỗ lực nào tiếp theo trong một khoảng thời gian ngắn sẽ không thành công.

CHÚ THÍCH - Tùy thuộc vào chính sách an toàn có hiệu lực, có thể thích hợp để từ chối bất kỳ nỗ lực xác thực nào khác trong một khoảng thời gian xác định trước

Nếu xác thực thành công, BHSM sẽ gửi PSID đã ký và thử thách R_a được mã hóa bằng khóa bí mật của người dùng đến máy chủ xác thực. Chứng thư ITU-T X.509 cũng được gửi đến máy chủ xác thực như một phần trong quá trình truyền. Máy chủ xác thực sẽ xác thực quyền sở hữu chứng thư ITU-T X.509 bằng cách so sánh PSID trong chứng thư với PSID đã giải mã được BHSM gửi trong lần truyền trước đó. Nếu cả hai giống hệt nhau, máy chủ xác thực chấp nhận yêu cầu dịch vụ và chuyển nó cho nhà cung cấp dịch vụ để xử lý.

8.3. Kiểu ASN.1 cho PSID được mã hóa

DataSetForEncryptedPSID gồm các thành phần sau:

- **version** tham chiếu đến số phiên bản của Tiêu chuẩn này. Khi Tiêu chuẩn này được tham chiếu, giá trị **v1 (0)** sẽ được sử dụng;
- **psidEncAlg** tham chiếu đến thuật toán mã hóa phi đối xứng và tham số được sử dụng để mã hóa PSID. Thuật toán phải giống với thuật toán có trong chứng thư của CA;
- **encryptedPsid** là PSID được mã hóa với khóa công khai của tổ chức chứng thực.

```
DataSetForEncryptedPSID ::=
        SEQUENCE { version [0]
        INTEGER DEFAULT 0,
        psidEncAlg      [1] PSIDEncryptionAlgorithm,
        encryptedPsid       [2] EncryptedPsid
}
PSIDEncryptionAlgorithm ::= AlgorithmIdentifier
Encryptedsid ::= OCTET STRING
```

Phụ lục A

PSID và thông tin liên quan

(quy định)

A.1. Tổng quan

Phụ lục này áp dụng cho cơ chế quy định tại Điều 7 và Điều 8.

A.2. PSID được mã hóa yêu cầu chứng thư ITU-T X509

Một thông điệp yêu cầu cấp chứng thư số với PSID được mã hóa sẽ được gửi đến CA. PKCS#10 bao gồm tên phân biệt của người dùng và thông tin khóa xác thực chữ ký số của người dùng, đồng thời bao gồm các thành phần thuộc tính để nhập thông tin bổ sung. Thành phần thuộc tính có thể bao gồm định danh đối tượng (OID) và tất cả các thuộc tính có cấu trúc cụ thể. Do đó, thành phần có thể bao hàm PSID cho **EncryptedPsid** được mã hóa cần sử dụng OID.

A.3. ASN.1 cho PSID

```
XBHSM {iso(1) standard(0) bhsm(17922) modules(0) version1(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS authenticationFramework
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1)
        usefulDefinitions(0) 7}
        ALGORITHM, AlgorithmIdentifier{}
        FROM AuthenticationFramework authenticationFramework;

        DataSetForEncryptedPSID ::= SEQUENCE {
                version  INTEGER DEFAULT 0,
                psidEncAlg       PSIDEncryptionAlgorithm,
                encryptedPsid    EncryptedPsid
                }
        PSIDEncryptionAlgorithm ::= AlgorithmIdentifier
                {{SupportedEncryptionAlgorithms}}
        SupportedEncryptionAlgorithms     ALGORITHM ::= {...}
        EncryptedPsid ::= OCTET STRING
        PSID ::= SEQUENCE {
                hashAlg HashAlgorithm,
                hashContent      HashContent
                }
        HashAlgorithm ::= AlgorithmIdentifier{{SupportedHashAlgorithms}}
        SupportedHashAlgorithms ALGORITHM ::= {...}

        HashContent ::= SEQUENCE {
                bR       PrintableString,
                randomNum       BIT STRING
                }
        bhsmpsid          OBJECT IDENTIFIER ::=
                {iso(1) standard(0) bhsm(17922) contentType(2) bhsmps(1)}
        BHSM-PSID ::= TYPE-IDENTIFIER
        bioRef   BHSM-PSID ::=
                {BIT STRING IDENTIFIED BY {bhsmpsid 3}}
        InstanceOfBHSM-PID ::= INSTANCE OF BHSM-PSID({SupportedBHSM-PSID})
        SupportedBHSM-PSID BHSM-PSID ::= {bioRef,...}
END
```

Cấu trúc PSID gồm các thành phần sau:

- **hashAlg** tham chiếu đến thuật toán băm và tham số được sử dụng để tạo PSID.

Cấu trúc **HashContent** bao gồm các thành phần sau:

- **bR** là tham chiếu sinh trắc học được trích xuất từ thông tin sinh trắc học. Có thể sử dụng bất kỳ phương thức sinh trắc học nào (vân tay, khuôn mặt, mống mắt, v.v.). Để thể hiện **bR**, phải sử dụng một phần thích hợp của loạt tiêu chuẩn ISO/IEC 19794.
- **randomNum** là số ngẫu nhiên R

Chú thích - Khuyến nghị về tham chiếu sinh trắc học được thể hiện bằng Bản ghi thông tin sinh trắc học (BIR) được đặc tả trong ISO/IEC 19785-1.

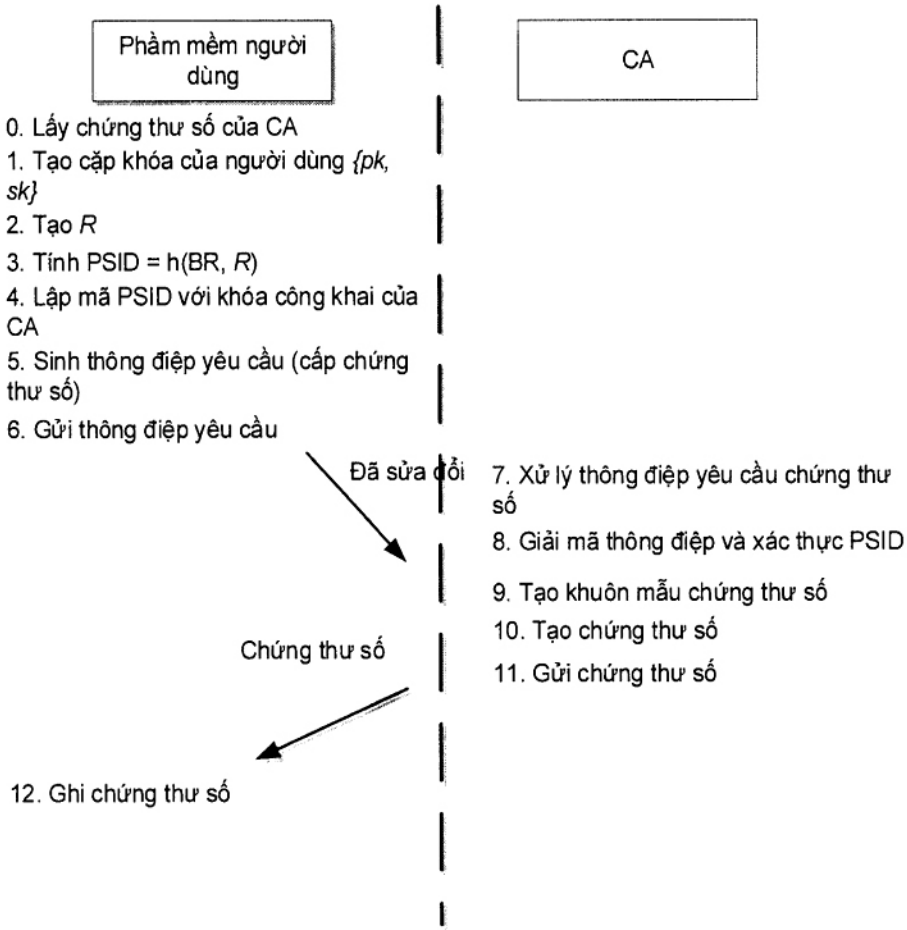
Để chèn PSID vào chứng thư ITU-T X.509, nó sẽ được ghi trong trường mở rộng **subjectAltName** có chứa **directoryName**.

Trường **realName** chứa tên được mã UTF8String của chủ sở hữu chứng thư số và trường **userInfo** chứa thông tin định danh bổ sung của chủ sở hữu chứng thư số, cũng như PSID

Phụ lục B

Các quá trình chèn PSID sử dụng PKCS #10 có sửa đổi

(tham khảo)



Tài liệu tham khảo

[1]. TCVN 11817-1:2017, Công nghệ thông tin - Các kỹ thuật an toàn - Xác thực thực thể - Phần 1: Tổng quan, (ISO/IEC 9798-1:2010, Information technology – Security techniques – Entity Authentication – Part1: General).

[2]. ISO/IEC 2382-37:2012, Information technology – Vocabulary –Part 37: Biometrics.

[3]. ISO/IEC 15945:2002, Information technology – Security techniques – Specification of TTP services to support the application of digital signature.