BAN CƠ YẾU CHÍNH PHỦ

CỤC QUẢN LÝ MẬT MÃ DÂN SỰ VÀ KIỂM ĐỊNH SẢN PHẨM MẬT MÃ

THUYẾT MINH

Dự thảo "Thông tư quy định Danh mục tiêu chuẩn bắt buộc về kỹ thuật mật mã áp dụng cho thiết bị HSM trong hoạt động định danh và xác thực điện tử"

Hà Nội, 2023

MỤC LỤC

CHỮ VIẾT TẮT

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
BSI	Federal Office for Information Security (tên gốc: Bundesamt für Sicherheit in der Informationstechnik)	Cơ quan an toàn thông tin liên bang (Đức)
CBC	Cipher Block Chaining Mode	Chế độ móc xích khối mã
CCM	Counter Mode with CBC-MAC Mode	Chế độ CTR với chế độ CBC-MAC
CFB	Cipher Feedback Mode	Chế độ phản hồi bản mã
CTR	Counter Mode	Chế độ bộ đếm
CTR_DRBG	Counter - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm
DH	Diffie-Hellman	Thuật toán trao đổi khóa Diffie-Hellman
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
EC	Elliptic Curve	Đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ Galois/Bộ đếm
GOST	Gosudarstvennyy standart	Tiêu chuẩn quốc gia Liên bang Nga
Hash_DRBG	Hash Deterministic Random	Bộ tạo bit ngẫu nhiên tất định

	Bit Generator	dựa trên hàm băm
HMAC	Hashed Message Authentication Code	Mã xác thực thông báo dựa trên hàm băm
HMAC_DRBG	HMAC - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên HMAC
HSM	Hardware Security Module	Mô-đun an toàn phần cứng
IKE	Internet Key Exchange	Giao thức trao đổi khóa sử dụng trong công nghệ IPsec
IPS	Intrusion Prevention System	Hệ thống ngăn ngừa xâm nhập
NIAP	National Information Assurance Partnership	Hiệp hội bảo đảm an toàn thông tin quốc gia (Hoa Kỳ)
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ quốc gia (Hoa Kỳ)
NRBG	Non-deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên bất định
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn xuất khóa dựa trên mật khẩu 2
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF (Internet Engineering Task Force) công bố
RSA	Rivest - Shamir - Adleman	Tên của hệ mã do ba nhà toán học Rivest, Shamir và Adleman phát minh
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
SP	Special Publication	Ấn phẩm đặc biệt (Viện Tiêu chuẩn và Kỹ thuật quốc gia Hoa Kỳ)
TCVN		Tiêu chuẩn quốc gia Việt Nam

TDEA	Triple Data Encryption Algorithm	Thuật toán mã hóa dữ liệu Triple-DES
TLS	Transport Layer Security	Giao thức bảo mật tầng giao vận
TOE	Target of Evaluation	Mục tiêu đánh giá

TỔNG QUÁT

Hiện nay, danh tính số đã và đang được sử dụng rộng rãi tại các dịch vụ trong nhiều lĩnh vực của cuộc sống hàng ngày, từ y tế, giáo dục, thương mại điện tử, đô thị thông minh cho tới giải trí, giao dịch xã hội,....

Hệ thống phục vụ cho việc thực hiện giao dịch danh tính số giữa các thực thể gọi là hệ thống định danh và xác thực điện tử (hệ thống nhận dạng). Mục đích của những hệ thống nhận dạng là cho phép các người sử dụng (thực thể/đối tượng) không có quan hệ (không biết nhau) trước đó tham gia vào các giao dịch tin cậy. Trong hệ thống định danh và xác thực điện tử, các thuộc tính của người sử dụng được bên thứ ba tin đáng cậy (có thể là một hoặc nhiều cơ quan/tổ chức) chứng thực. Các bên thứ ba này phát hành các thông tin định danh điện tử và phương thức xác thực gắn với một đối tượng. Người dùng có thể dùng các thông tin xác thực tham gia vào các giao dịch mà trong đó các đối tượng giao dịch khác yêu cầu người dùng chứng minh danh tính (xác thực điện tử).

Nhằm quy định về danh tính điện tử, định danh điện tử, xác thực điện tử; dịch vụ xác thực điện tử; quyền, nghĩa vụ của bên sử dụng dịch vụ xác thực điện tử; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, Chính phủ đã ban hành Nghị định số 59/2022/NĐ-CP ngày 05/9/2022. Trong đó tại khoản 2 Điều 38 quy định về trách nhiệm của Ban Cơ yếu Chính phủ: "Hướng dẫn áp dụng tiêu chuẩn, quy chuẩn kỹ thuật mật mã dân sự và sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ trong hoạt động định danh và xác thực điện tử". Trong hoạt động định danh và xác thực điện tử, các kỹ thuật mật mã dân sự là một trong các yếu tố rất quan trọng. Áp dụng và sử dụng đúng các kỹ thuật mật mã được đảm bảo giúp cho nâng cao tính an toàn, độ tin cậy và hiệu suất hoạt động của toàn bộ quá trình định danh và xác thực điện tử. Vì vậy, việc đưa ra các quy định trong việc sử dụng các kỹ thuật mật mã trong hoạt động định danh và xác thực điện tử là rất quan trọng và cấp thiết trong tình hình hiện nay.

1 Sự cần thiết xây dựng Danh mục tiêu chuẩn

1.1 Sở cứ xây dựng Danh mục tiêu chuẩn

– Thực hiện quy định tại điểm a khoản 4 Điều 52 Luật An toàn thông tin mạng, Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng *"xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự"*.

– Thực hiện quy định tại khoản 1 Điều 38 Nghị định số 59/2022/NĐ-CP của Chính phủ về Trách nhiệm của Ban Cơ yếu Chính phủ "*Hướng dẫn áp dụng tiêu chuẩn, quy chuẩn kỹ thuật mật mã dân sự và sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ trong hoạt động định danh và xác thực điện tử*".

– Thực hiện Quyết định số 569/QĐ-BQP ngày 07 tháng 02 năm 2024 của Bộ trưởng Bộ Quốc phòng về ban hành Chương trình xây dựng văn bản quy phạm pháp luật năm 2024 của Bộ Quốc phòng, Ban Cơ yếu Chính phủ xây dựng dự thảo Thông tư quy định Danh mục tiêu chuẩn bắt buộc về kỹ thuật mật mã áp dụng cho thiết bị HSM trong hoạt động định danh và xác thực điện tử

1.2 Tình hình thực tiễn về hoạt động định danh và xác thực điện tử

1.2.1 Tình hình chung trên thế giới

Trên thế giới, trong xu hướng số hóa của toàn xã hội, danh tính số (Digital Identity/ID Số) đang ngày càng được nhiều quốc gia công nhận và đưa vào sử dụng. Ủy ban Châu Âu đã công bố đề xuất về danh tính số cho tất cả công dân Châu Âu, cho phép tất cả các tài liệu chính thức được lưu trữ và quản lý thông qua ví kỹ thuật số. Một ví dụ thực tế là Estonia, một quốc gia châu Âu nhỏ với khoảng 1,3 triệu dân thì 99% các dịch vụ có thể được truy cập điện tử như: bỏ phiếu, mở công ty và thậm chí cấp giấy khai sinh. Đằng sau đó là một hệ sinh thái ID số kết nối mọi người với các cơ sở này. Tuy nhiên, công nghệ này không chỉ làm cho cuộc sống của công dân dễ dàng hơn mà quốc gia này đã tiết kiệm được 2% GDP bằng cách chuyển sang dùng danh tính số. Ấn Độ đã triển khai hệ thống ID số quốc gia được gọi là dự án Aadhaar. Ngoài việc giảm chi phí và nạn quan liêu trong nước, ID số cũng tăng cường bảo mật bằng cách thay thế các tài liệu vật lý - giúp giảm gian lận, kém hiệu quả và tham nhũng. Công dân trở nên dễ dàng hơn khi thuê các dịch vụ tư nhân, điều này giúp Ấn Độ thu hút đầu tư, tăng cạnh tranh và dẫn đến các sản phẩm dịch vụ tốt hơn với giá thấp hơn. Vào năm 2020, Chính phủ Úc thông báo việc phát triển hệ thống ID số sẽ là trọng tâm trong gói ngân sách công nghệ trị giá 800 triệu USD.

Theo báo cáo của Công ty McKinsey, thống kê tại Brazil, Trung Quốc, Ethiopia, Ấn Độ, Nigeria, Vương quốc Anh và Hoa Kỳ chỉ ra rằng các quốc gia có thể đạt được giá trị kinh tế tương đương từ 3% - 13% GDP vào năm 2030 từ việc triển khai các chương trình định danh và xác thực điện tử. Ở các nền kinh tế mới nổi, chỉ riêng định danh điện tử cơ bản có thể mở khóa 50% - 70% tiềm năng kinh tế với giả sử tỷ lệ ứng dụng khoảng 70%. McKinsey dự đoán, vào năm 2030, định danh điện tử có tiềm năng tạo ra giá trị kinh tế tương đương 6% GDP ở các nền kinh tế mới nổi và 3% ở các nền kinh tế đã phát triển.

Một số khái niệm cơ bản đang được các nước sử dụng trong lĩnh vực định danh và xác thực điện tử:

Danh tính (Identity) là một hoặc nhiều thuộc tính miêu tả duy nhất một đối tượng/thực thể trong một ngữ cảnh cụ thể.

Danh tính số (Digital Identity) là danh tính của một thực thể đủ chi tiết để phân biệt thực thể đó trong một ngữ cảnh số.

Danh tính số của một người có thể bao gồm nhiều thuộc tính: dữ liệu tiểu sử (như: tên, tuổi, giới tính, địa chỉ,…), dữ liệu sinh trắc học (như: vân tay, mống mắt,) cũng như các thuộc tính mở rộng khác liên quan đến những gì người đó làm hoặc điều gì đó mà người khác biết về cá nhân đó. Khi những dữ liệu này được thu thập và xác minh, chúng có thể được sử dụng để xác định một người bằng cách trả lời câu hỏi "Bạn là ai?". Các thuộc tính này, cùng với thông tin xác thực do nhà cung cấp dịch vụ cấp (như: số ID duy nhất, eDocument, eID, mobile ID), sau đó cũng có thể được sử dụng làm yếu tố xác thực để trả lời câu hỏi "Bạn có phải là người mà bạn tuyên bố không?". Các thuộc tính và yếu tố xác thực được sử dụng trong danh tính số có thể thay đổi tùy theo ngữ cảnh hoặc tùy thuộc mỗi hệ thống nhận dạng.

Định danh (Identification) là quá trình thiết lập, xác định hoặc công nhận danh tính của một đối tượng.

Định danh điện tử (Electronic Identification) là quá trình thiết lập, xác định hoặc công nhận danh tính số của một đối tượng.

Xác thực điện tử (Authentication) là quá trình xác minh điện tử đối với danh tính một thực thể. Thực thể có thể người sử dụng máy tính/điện thoại, là chính máy tính/điện thoại hoặc là một chương trình máy tính/ứng dụng/thiết bị. Xác thực là cách đảm bảo là người sử dụng đang định thực hiện các chức năng của hệ thống đúng thật là người sử dụng đã được cho quyền làm điều đó.

Về cơ bản, hệ thống định danh và xác thực điện tử bao gồm các thành phần là: Người sử dụng (đầu cuối); các tổ chức cung cấp danh tính số (Identity Provider - IdP); các bên thứ ba tin cậy (Authenticatioin Provider/Relying Party); các tổ chức cung cấp dịch vụ điện tử sử dụng dịch vụ từ IdP, cơ quan quản lý nhà nước và nền tảng trao đổi thuộc tính (chức năng). Trong đó:

- Người sử dụng (ví dụ: Citizen/EndUser/Device/Sensor/Terminal…): là đối tượng được hệ thống cung cấp danh tính số để cho phép tham gia thực hiện các trao đổi/giao dịch điện tử.

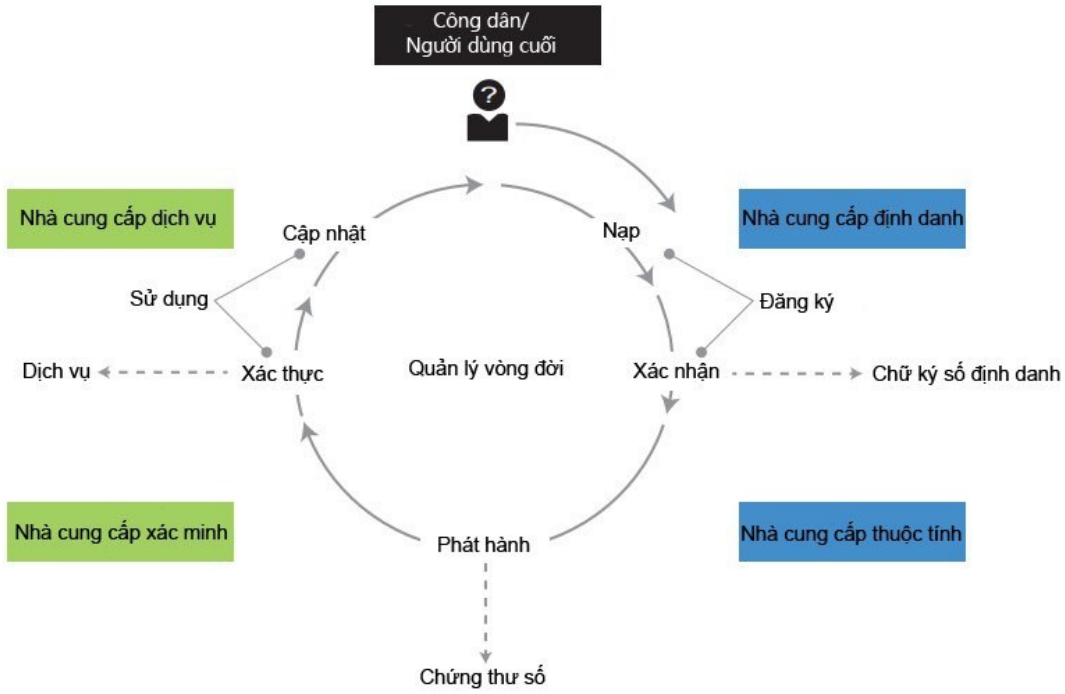
- Tổ chức cung cấp danh tính số (ID Provider): là tổ chức nắm giữ các thuộc tính xác thực của người sử dụng, cung cấp dịch vụ thiết lập danh tính số, xác thực danh tính người dùng và các dịch vụ khác liên quan phục vụ giao dịch điện tử. Ví dụ: Bộ Công an, ngân hàng, cơ quan bảo hiểm, công ty viễn thông,…

- Bên tin tưởng (Service Provider): là các tổ chức, cá nhân chấp nhận chứng thực từ nhà cung cấp danh tính về danh tính người dùng để cho phép người dùng truy cập, sử dụng dịch vụ của họ. Ví dụ: cơ quan cung cấp dịch vụ công trực tuyến, ngân hàng …

- Nền tảng trao đổi thuộc tính: thực hiện việc hoàn thành các giao dịch bằng cách đối sánh các truy vấn nhận dạng từ Bên tin tưởng với các thuộc tính từ Tổ chức cung cấp danh tính, trao đổi thuộc tính hoặc bằng chứng nhận dạng.

- Cơ quan quản lý nhà nước là thành phần thực hiện nhiều vai trò, bao gồm: cơ quan thực hiện việc quản lý danh tính số (Provider), cung cấp dịch vụ nhận dạng (Service, Authentication-CA), giám sát hệ thống và đưa ra các quy định pháp lý, tiêu chuẩn/quy chuẩn công nghệ… cho hoạt động định danh và xác thực điện tử.

Một cách tổng quan, trên thế giới hiện tại, hệ thống định danh và xác thực điện tử có thể bao gồm các thành phần chính được quy định tại hình 1:



Hình 1. Tổng quan các thành phần hệ thống định danh và xác thực điện tử

Nhìn chung, danh tính số, định danh và xác thực điện tử có vai trò hết sức quan trọng cuộc sống và là nền tảng của chuyển đổi số (CĐS). Trước mắt, các nước bắt đầu xây dựng, triển khai hệ thống định danh và xác thực điện tử thì tác động đối với từng nhóm đối tượng sẽ như sau: Đối với cơ quan nhà nước: Danh tính số là một yếu tố quyết định cho việc CĐS các dịch vụ công của chính phủ và là một khối nền tảng cho kinh tế số. Danh tính số được triển khai chính xác sẽ cung cấp sự tin tưởng (niềm tin, sự tin cậy) cho các dịch vụ khi giao dịch với người dùng, giảm trùng lặp giữa các cơ quan nhà nước, đơn giản hóa việc triển khai cho các nhà cung cấp dịch vụ, cụ thể:

(i) Đảm bảo tính sẵn sàng của các dịch vụ công trực tuyến (DVCTT) (24/7).

(ii) Giảm thiểu những sai sót, gian lận của con người trong quá trình thực hiện xác thực danh tính.

(iii) Nâng cao hiệu quả hoạt động của Chính phủ.

(iv) Giảm chi phí vận hành.

(v) Tăng cường tính minh bạch, trách nhiệm giải trình của các cơ quan nhà nước.

(vi) Cải thiện cung cấp dịch vụ.

(vii) Đảm bảo an toàn.

(viii) Tạo ra khả năng cho thương mại, thanh toán quốc tế.

Đối với doanh nghiệp:

(i) Cải thiện chất lượng dịch vụ theo hướng lấy khách hàng làm trung tâm.

(ii) Đảm bảo an toàn cho các giao dịch số, giảm thiệt hại cho các doanh nghiệp từ các vụ gian lận, trộm cắp danh tính.

(iii) Mở ra cơ hội kinh doanh mới cho các doanh nghiệp, đặc biệt trong lĩnh vực tài chính ngân hàng.

(iv) Cắt giảm chi phí và thời gian vận hành: các doanh nghiệp có thể giảm chi phí mà họ phải duy trì để tiếp cận với khách hàng và xác thực định danh của khách hàng như giảm nhân sự, giảm điểm giao dịch, giảm giấy tờ và thời gian cần thiết để hoàn thành yêu cầu của người dùng…

Đối với người sử dụng dịch vụ (bao gồm cơ quan nhà nước, doanh nghiệp và người dân, trong đó người dân là đối tượng được hưởng lợi nhiều nhất từ việc xây dựng hệ thống định danh và xác thực điện tử thông qua nhiều vai trò như: là công dân được bảo đảm quyền lợi theo pháp luật, là người sở hữu danh tính, là đối tượng quản lý của các chính sách Pháp luật và Nhà nước, là người lao động trong doanh nghiệp hoặc cơ quan nhà nước, là khách hàng…):

(i) Được đảm bảo an toàn về danh tính. Được chủ động quản lý, sử dụng, cho phép sử dụng các dữ liệu cá nhân của mình một cách dễ dàng, hiệu quả.

(ii) Gia tăng mức độ hài lòng và hưởng thụ các dịch vụ số: người dân và doanh nghiệp được trao quyền và chủ động hơn trong việc lựa chọn cách thức tiếp cận dịch vụ.

(iii) Gia tăng tính thuận tiện của dịch vụ, tiết kiệm chi phí thực hiện dịch vụ.

1.2.2 Tình hình tại Việt Nam

Trong thời gian qua, Đảng và Nhà nước đã có nhiều chủ trương, chính sách thúc đẩy mạnh mẽ việc ứng dụng và phát triển công nghệ thông tin và truyền thông (CNTT-TT) trong phát triển kinh tế - xã hội, đặc biệt là tham gia cuộc Cách mạng công nghiệp (CMCN) 4.0 và CĐS nhằm phát triển kinh tế số, chính quyền điện tử,

tiến tới chính quyền số, xã hội số. Tại các văn bản quan trọng như Nghị quyết số 52- NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc CMCN lần thứ tư, Quyết định số 749/QĐ-TTg ngày 6/3/2020 của Thủ tướng Chính phủ phê duyệt Chương trình CĐS quốc gia đến năm 2025, định hướng 2030, đều xác định danh tính số, định danh và xác thực điện tử là yếu tố nền tảng cho CĐS.

Ngày 08/11/2021, Thủ tướng Chính phủ ban hành Quyết định số 34/2021/QĐ-TTg quy định về định danh và xác thực điện tử trên nền tảng Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu căn cước công dân và Cơ sở dữ liệu quốc gia về xuất nhập cảnh.

Việc sử dụng định danh và xác thực điện tử như đã nêu ở phần trên mang lại rất nhiều lợi ích cho Chính phủ, Doanh nghiệp và cả người dân. Chính phủ cũng đã có nhưng chính sách rất cụ thể và đẩy nhanh việc triển khai, áp dụng hệ thống định danh và xác thực điện tử. Ngày 05/09/2022, Chính phủ banh hành Nghị định số 59/2022/NĐ-CP quy định về định danh và xác thực điện tử. Nghị định này quy định về danh tính điện tử, định danh điện tử, xác thực điện tử; dịch vụ xác thực điện tử; quyền, nghĩa vụ của bên sử dụng dịch vụ xác thực điện tử; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Nghị định này áp dụng đối với cơ quan, tổ chức, công dân Việt Nam; tổ chức, cá nhân nước ngoài cư trú, hoạt động trên lãnh thổ Việt Nam liên quan đến định danh và xác thực điện tử. Sau khi Nghị định này được ban hành và có hiệu lực, các cơ quan, tổ chức, cá nhân có liên quan đều khẩn trương thực hiện để sớm đưa việc sử dụng định danh và xác thực điện tử vào trong cuộc sống.

Nghị định quy định Ban Cơ yếu Chính phủ có trách nhiệm:

1. Hướng dẫn áp dụng tiêu chuẩn, quy chuẩn kỹ thuật mật mã dân sự và sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ trong hoạt động định danh và xác thực điện tử.

2. Chủ trì, phối hợp với Bộ Công an đánh giá an toàn mật mã đối với bên sử dụng dịch vụ xác thực điện tử.

3. Phối hợp với Bộ Công an bảo đảm an toàn, bảo mật thông tin sử dụng sản phẩm mật mã cơ yếu đối với hệ thống định danh và xác thực điện tử, sử dụng danh tính điện tử, tài khoản định danh điện tử trong việc cung cấp dịch vụ chữ ký số chuyên dùng Chính phủ.

1.2.3 Kết luận

Để thực hiện được tốt các nhiệm vụ trên, Ban Cơ yếu Chính phủ cần phải xây dựng và tham mưu các cơ quan có thẩm quyền ban hành các Quy chuẩn kỹ thuật quốc gia (QCVN), Tiêu chuẩn quốc gia (TCVN) về kỹ thuật mật mã áp dụng trong hoạt động định danh và xác thực điện tử. Trong đó yêu cầu phải đưa ra được các quy định về kỹ thuật mật mã dân sự đảm bảo được tính an toàn, bảo mật đối với toàn bộ hệ thống cũng như từng thành phần cụ thể trong hệ thống, điển hình như các thành

phần quan trọng bao gồm: HSM, thiết bị bị lưu trữ giữ liệu định danh… Trong đó thành phần quan trọng nhất và sử dụng các kỹ thuật mật mã trong hầu hết các hành động chính là thiết bị HSM (Hardware Security Module).

Hiện nay, các thiết bị HSM thương mại hầu hết do nước ngoài sản xuất, và các thiết bị này đều được trang bị và hỗ trợ đầy đủ các các kỹ thuật mật mã để đảm bảo được sự tương thích và khả năng giải quyết tất cả các trường hợp xảy ra. Nhưng trong các kỹ thuật mật mã đó bao gồm cả thuật toán đã bị tấn công và không còn được sử dụng bởi hầu hết các quốc gia trên thế giới. Do vậy việc đưa ra các quy định về các kỹ thuật mật mã được phép sử dụng cho thiết bị HSM sử dụng trong định danh và xác thực điện tử là điều cần sớm được thực hiện.

2 Cơ sở tham chiếu cho việc xây dựng Danh mục tiêu chuẩn

2.1 Hiện trạng chuẩn hóa về định danh và xác thực điện tử

Để xây dựng và phát triển hệ thống định danh và xác thực điện tử được hiệu quả, các quốc gia trên thế giới đang bắt đầu công việc tạo dựng môi trường pháp lý hay Khung danh tính số quốc gia. Đây là việc hết sức quan trọng và cấp thiết. Khung danh tính số quốc gia là tập hợp các chính sách, quy định của pháp luật; quy trình, thủ tục; tiêu chuẩn kỹ thuật; công nghệ và các thành phần khác để xây dựng, thiết lập môi trường phát triển, sử dụng định danh số một cách tin cậy trong các hoạt động giao dịch điện tử. Khung Danh tính số quốc gia sẽ làm rõ một số nội dung quan trọng sau đây:

- Một là, hình thành các tổ chức cung cấp danh tính số (IdP). Trong đó, Primary IdP là tổ chức nguyên gốc, chính yếu cung cấp dịch vụ trực tiếp từ cơ sở dữ liệu (CSDL) quốc gia về dân cư (CSDL về CCCD) và Secondary IdP là tổ chức thứ cấp cung cấp dịch vụ trên cơ sở Primary ID, ví dụ như các Nhà mạng di động cung cấp danh tính số (Digital ID) trên cơ sở CSDL thuê bao được thiết lập ban đầu dựa trên thông tin nhận dạng cá nhân là chứng minh nhân dân/căn cước công dân (CMND/CCCD).

- Hai là, Mô hình Danh tính số quốc gia (National Digital Identity Scheme) được xây dựng theo hướng mô hình định danh liên hợp (Federated Identification Model). Dịch vụ từ các IdP được tích hợp và sử dụng rộng rãi bởi các tổ chức cung cấp dịch vụ trực tuyến thông qua hệ thống National Digital Identity Exchange.

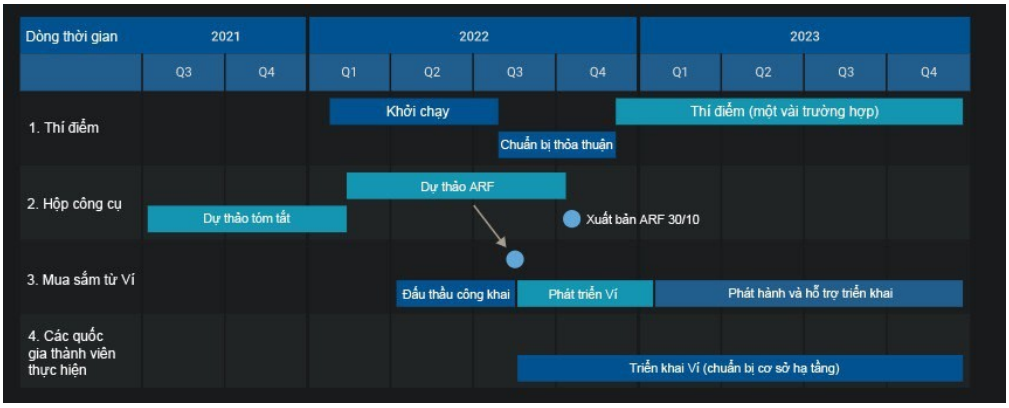
- Ba là, Digital Identity Framework sẽ tạo môi trường cho Hệ sinh thái về danh tính số phát triển (Digital Identity Ecosystem) với các thành phần cơ bản là tổ chức cung cấp danh tính số (IdP), tổ chức cung cấp dữ liệu thuộc tính (Attribute Provider - AP), các bên tin tưởng (RP) và cơ quan quản lý nhà nước (Accreditation Authority) thực hiện chức năng thẩm định và cấp phép dịch vụ cho các IdP.

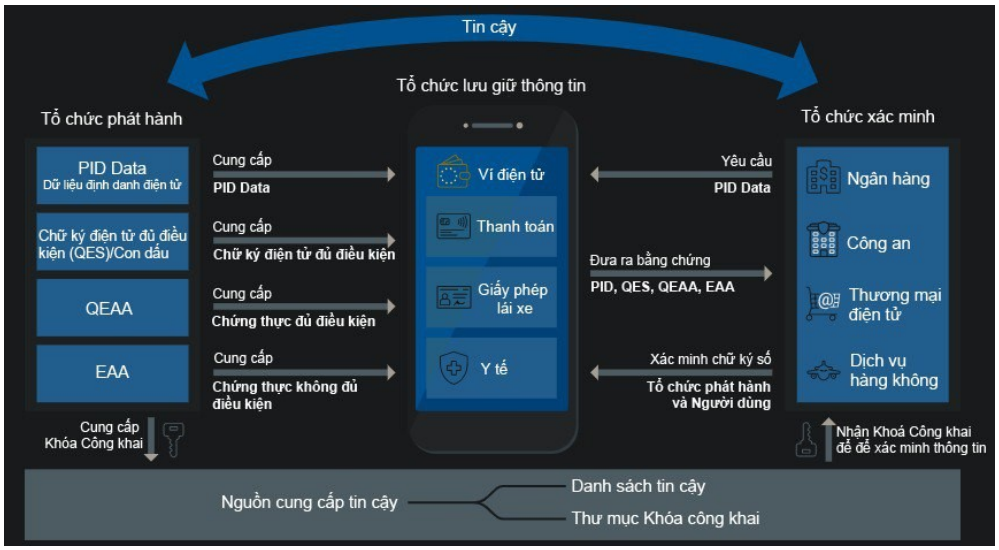
- Bốn là, phương pháp luận đánh giá rủi ro nhất quán để xác định yêu cầu về mức độ đảm bảo (LoA) của các dịch vụ trực tuyến, cũng như của dịch vụ do IdP cung cấp và các nguyên tắc về đảm bảo an toàn thông tin cá nhân khi cung cấp, chia sẻ

thông tin danh tính cá nhân, tổ chức theo hướng mọi thông tin cá nhân chỉ được chia sẻ khi có sự đồng ý tường minh của người dùng.

Trong đó, nội dung ban hành các tiêu chuẩn/quy chuẩn kỹ thuật là nội dung quan trọng trong hình thành Khung pháp lý danh tính. Tuy nhiên, việc xây dựng và phát triển hệ thống định danh và xác thực điện tử trên thế giới đa số các nước cũng chỉ mới bắt đầu nên chưa có nhiều tiêu chuẩn/quy chuẩn (về bảo mật) chính thức cho hệ thống này. Tại Mỹ, dựa trên tinh thần của đạo luật giao dịch điện tử (The Uniform Electronic Transactions Act -UETA) thì viện tiêu chuẩn công nghệ NIST cũng bắt đầu ban hành các tiêu chuẩn cho hệ thống định danh và xác thực điện tử. Hiện tại, các tài liệu được phân loại như NIST SP 800-63x (Digital Identity Guidelines) cũng đang được xây dựng và lấy ý kiến từ các chuyên gia để ban hành thành tiêu chuẩn trong thời gian tới.

Tại Châu Âu, Quy định về "Định danh, Xác thực Điện tử và Dịch vụ Tin cậy"-eIDAS dành cho thị trường Chung Châu Âu chính thức được công nhận vào tháng 9 năm 2018. Với quy định mới này, cư dân và doanh nghiệp tại Châu Âu có thể sử dụng hệ thống định danh cấp quốc gia để xác thực danh tính khi truy cập dịch vụ công. Quy định eIDAS được kỳ vọng sẽ thay thế cho Chỉ thị về Chữ ký điện tử 1999/93/EC. eIDAS vẫn đang được phát triển và cập nhật cho các dịch vụ tương lai, ví dụ hình sau là lộ trình xây dựng cập nhật cho dịch vụ ví điện tử:Swedish Civil Contingencies Agency, "File Encryption Protection Profile", Version: 1.0, 04-7-2018.





Hình 2 – Phát triển dịch vụ ví điện tử trong hệ thống định danh và xác thực điện tử

2.2 Tình hình tiêu chuẩn hóa tại Việt Nam

Quy chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên quy chuẩn	Ghi chú
1	QCVN 4 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng	Ban hành kèm theo Thông tư 161/2016/TT-BQP ngày 21/10/2016
2	QCVN 5 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về chữ ký số sử dụng trong lĩnh vực ngân hàng	
3	QCVN 6 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về quản lý khóa sử dụng trong lĩnh vực ngân hàng	
4	QCVN 12 : 2022/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS	Ban hành kèm theo Thông tư 23/2022/TT-BQP ngày 04/4/2022
5	QCVN XX : 2023/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	Đang làm các thủ tục ban hành năm 2023

Tiêu chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên tiêu chuẩn	Ghi chú
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	

2	TCVN 7816:2007	Công nghệ thông tin – Kỹ thuật mật mã thuật toán mã dữ liệu AES	Phiên bản mới nhất TCVN 11367-3:2016
3	TCVN 7817-1:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 11770-3:2021
4	TCVN 7817-2:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng	Phiên bản mới nhất ISO/IEC 11770-2:2018
5	TCVN 7817-3:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng	Phiên bản mới nhất ISO/IEC 11770-3:2021
6	TCVN 7817-4:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 4: Cơ chế dựa trên bí mật yếu	Phiên bản mới nhất ISO/IEC 11770-4:2017
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 18014-1:2008
8	TCVN 7818-2:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 2: Cơ chế token độc lập	Phiên bản mới nhất ISO/IEC 18014-2:2021
9	TCVN 7818-3:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 3: Cơ chế tạo thẻ liên kết	Phiên bản mới nhất ISO/IEC 18014-3:2009
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	
11	TCVN 11367-1:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 1: Tổng quan	Phiên bản mới nhất ISO/IEC 18033-1:2021
12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	
13	TCVN 11367-3:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã	

		khối	
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	
16	TCVN 11816-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 2: Hàm băm sử dụng mã khối n-bit.	
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	
18	TCVN 11816-4:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 4: Hàm băm sử dụng số học đồng dư	
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	
20	TCVN 11817-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng	
21	TCVN 11817-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Cơ chế sử dụng kỹ thuật chữ ký số	
22	TCVN 12214-1:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan	
23	TCVN 12214-2:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 2: Các cơ chế dựa trên phân tích số nguyên	
24	TCVN 12214-3:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 3: Các cơ chế dựa trên logarit rời rạc	
25	TCVN 11367-	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật	

	5:2018	mã dựa trên định danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	
27	TCVN 12212:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô đun mật mã	
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	
29	TCVN 12852-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan	
30	TCVN 12852-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Các kỹ thuật tạo đường cong elliptic	
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	
32	TCVN 12855-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 2: Các cơ chế dựa trên phân tích số nguyên	
33	TCVN 12855-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 3: Các cơ chế dựa trên bài toán Logarit rời rạc	
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ -Phần 1: Tổng quan	
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	
36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	

37	TCVN 12854-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng	
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	
39	TCVN 11817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Cơ chế sử dụng kỹ thuật tri thức không	
40	TCVN 11817-6:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Cơ chế sử dụng truyền dữ liệu thủ công	
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	
44	TCVN 13177:2020	Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mật mã và kiểm thử phù hợp các cơ chế an toàn	
45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	
47	TCVN 13178-2: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký sử dụng một nhóm khóa công khai	
48	TCVN 13178-4: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu	

49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 2: Các cơ chế dựa trên logarit rời rạc	
52	TCVN 13461-1: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 1: Tổng quan	
53	TCVN 13461-2: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 2: Các cơ chế sử dụng một khóa công khai nhóm	
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	
55	TCVN 13462-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản	
56	TCVN 13720:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Kiểm thử các mô-đun mật mã trong môi trường hoạt động,	
57	TCVN 13721:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408),	
58	TCVN 13722:2023	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	
59	TCVN 13723-	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử	

	1:2023	viên và đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung	
60	TCVN 13723-2:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)	
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với đánh giá viên theo TCVN 8709 (ISO/IEC 15408)	

3 Nguyên tắc và cơ sở xây dựng

3.1 Nguyên tắc

– Các tham số an toàn được lựa chọn theo các khuyến nghị của ISO/IEC, NIST, CC, BSI và các tổ chức quốc tế khác để đảm bảo an toàn và phù hợp nhất.

– Phù hợp với điều kiện thực tế đối với các sản phẩm HSM đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế.

– Đáp ứng được sự phát triển của công nghệ từ 5 đến 10 năm tới.

3.2 Cơ sở xây dựng

Về căn cứ pháp lý, Luật An toàn thông tin mạng (có hiệu lực thi hành từ ngày 01 tháng 7 năm 2016) quy định về trách nhiệm quản lý chất lượng sản phẩm mật mã dân sự, trong đó giao Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự, quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự, quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy sản phẩm mật mã dân sự (khoản 4 Điều 52);*"xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự"* (khoản 7 Điều 38); khoản 1 Điều 38 Nghị định số 59/2022/NĐ-CP của Chính phủ về Trách nhiệm của Ban Cơ yếu Chính phủ "*Hướng dẫn áp dụng tiêu chuẩn, quy chuẩn kỹ thuật mật mã dân sự và sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ trong hoạt động định danh và xác thực điện tử*"

4 Nội dung Danh mục tiêu chuẩn

Nội dung Danh mục tiêu chuẩn dưới đây là bao gồm quy định về mức giới hạn của đặc tính kỹ thuật mật mã được sử dụng cho sản phẩm HSM trong hoạt động định danh và xác thực điện tử phải tuân thủ để đảm bảo an toàn; bảo vệ lợi ích và an ninh quốc gia và các yêu cầu thiết yếu khác.

4.1 Thuật toán mật mã đối xứng

Tổng hợp đánh giá độ an toàn của một số thuật toán mật mã đối xứng được sử dụng phổ biến trên thế giới được mô tả trong bảng sau:

Thuật toán mã hóa	Kích cỡ khóa (bít)	Kích cỡ khối (bít)	Các tấn công đã biết	Mô tả
AES	128, 192, 256	128	Chưa có các tấn công thám mã đã biết	Chuẩn mã dữ liệu của Mỹ hiện tại.
DES	56	64	Kích cỡ khối và khóa nhỏ, dễ bị tấn công bởi các phương pháp vét cạn, ngày sinh, vi sai, tuyến tính, khóa yếu.	Chuẩn mã dữ liệu của Mỹ đến năm 2005.
TDES	128, 192	64	Chưa có các tấn công thám mã đã biết	TDES thường được biết đến như là DES bội ba (Triple - DES)
IDEA	128	64	Hạn chế của mã pháp này là kích cỡ khối nhỏ, lược đồ khóa đơn giản và chứa các lớp khóa yếu. Không có các tấn công thực tế, tuy nhiên có các tấn công lên số vòng nhỏ và khóa yếu. Tấn công tốt nhất lên IDEA là tấn công Bicliques. • Khovratovich, Dmitry; Leurent, Gaëtan; *Rechberger*, Christian	Là mã khối có bản quyền và hết hạn từ năm 2012, tuy nhiên là miễn phí cho mục đích phi thương mại.

			(2012). *Narrow-Bicliques: Cryptanalysis of Full IDEA. Advances in Cryptology – EUROCRYPT 2012*. Lecture Notes in Computer Science. **7237**. pp. 392–410 • Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", *Advances in Cryptology, CRYPTO 93 Proceedings*: 224–231	
RC2	40	64	Kích cỡ khóa quá nhỏ, kích cỡ khối nhỏ. Dễ tổn thương trước các dạng tấn công khác nhau.	Mã khối của Mỹ nhằm mục đích hạn chế xuất khẩu mật mã của Mỹ (NSA).
RC5	0-2040	32, 64, 128	Tồn tại một số tấn công lên phiên bản rút gọn 12-vòng với phiên bản kích cỡ khối 64-bít (thám mã vi sai) với độ phức tạp 2^{44} bản rõ chọn lọc.	Một mã khối sử dụng phép dịch vòng phụ thuộc dữ liệu.
RC6	128, 192, 256	128	Không tồn tại các tấn công thám mã đã biết.	Là thuật toán mã hóa có bản quyền của công ty bảo mật RSA, tuy nhiên đã hết hạn năm 2017.
ARIA	128, 192, 256	128	• *Wenling Wu; Wentao Zhang; Dengguo Feng (2006). "Impossible*	Là thuật toán Chuẩn mã khối của Hàn Quốc từ năm

			Differential Cryptanalysis of ARIA and Camellia" . Retrieved January 19, 2007. • *Xuehai Tang; Bing Sun; Ruilin Li; Chao Li (March 30, 2010). "A Meet-in-the-Middle Attack on ARIA" . Retrieved April 24, 2010.*	2004.
Blowfish	32-448	64	Tấn công ngày sinh (vì kích cỡ khối nhỏ). Tồn tại các khóa yếu.	Là thuật toán mã khối do Bruce Schneier thiết kế năm 1993 (không có bản quyền).
Camellia	128, 192, 256	128	Có độ an toàn được xem là tương đương với AES.	Là thuật toán được công nhận trong chuẩn ISO/IEC. Đây là mã khối có bản quyền và được dùng miễn phí trong dự án OpenSSL.
SEED	128	128	Chưa có các tấn công đã biết với phiên bản đầy đủ.	Thuật toán được công bố trong chuẩn ISO/IEC 18033-3:2010 và nhiều RFC khác (như RFC 4010, RFC 4162, RFC 4196).
CAST	64	64	Kích cỡ khóa/khối quá nhỏ bị tấn công ngày sinh, các tấn công khác	

			như vi sai tuyến tính.	
CAST-128 (còn gọi là CAST5)	40-128	64	Kích cỡ khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Không có bản quyền, được mô tả trong RFC 2144.
CAST-256	128, 192, 256	128	Tấn công tốt nhất là tấn công tương quan không (zero-correlation) với độ phức tạp thời gian là $2^{246.9}$ và dữ liệu là $2^{98.8}$. Tấn công này không ảnh hưởng tới độ an toàn của thuật toán. Bogdanov, Andrey; Leander, Gregor; Nyberg, Kaisa; Wang, Meiqin (2012). *Integral and multidimensional linear distinguishers with correlation zero*. *Lecture Notes in Computer Science*. **7658**. pp. 244–261.	Không có bản quyền. Được mô tả trong RFC 2612.
SM4	128	128	Chưa có tấn công đã biết nào được công bố.	Thuật toán mã khối được công nhận là Chuẩn Quốc gia Trung Quốc tháng 8/2016. Thuật toán này được xác định để bảo mật dữ liệu không dây.

Dựa theo nhiều phương pháp đánh giá hiện nay, kích cỡ khóa an toàn tối thiểu là 80 bít và đến năm 2027 là 128 bít (nguồn https://www.keylength.com/).

Bảng Khuyến nghị về kích cỡ khóa an toàn tối thiểu của ECRYPT-CSA (Cộng đồng chung Châu Âu tháng 2/2018) được mô tả trong bảng sau

Mức độ bảo vệ	**Mật mã**	**Phân**	**Logarithm rời**	**Đường**	**Kích cỡ**

	khóa đối xứng	tích thừa số	rạc		cong Elliptic	hàm băm
			Khóa	Nhóm		
Mức chuẩn hiện tại *Không sử dụng với các hệ thống mới*	80	1024	160	1024	160	160
Bảo vệ ngắn hạn *An toàn cho ít nhất 10 năm (2019-2028)*	128	3072	256	3072	256	256
Bảo vệ dài hạn *An toàn cho 30 năm tới 50 năm (2019-2068)*	256	15360	512	15360	512	512

Căn cứ vào quá trình rà soát các đặc tính kỹ thuật mật mã được sử dụng trong các sản phẩm thiết bị HSM đã được Ban cơ yếu Chính phủ cấp phép và các phân tích đưa ra như trên nhóm biên soạn đề xuất các quy định trong bảng sau:

Ký hiệu tiêu chuẩn	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
TCVN 11367-3:2016 (ISO/IEC 18033-3:2010)	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối.	- Áp dụng TCVN 11367-3:2016 (ISO/IEC 18033-3:2010) và ít nhất một trong ba tiêu chuẩn về chế độ hoạt động của mã khối. - Sử dụng một trong hai thuật toán AES hoặc TDEA. - Đối với thuật toán AES: + Sử dụng khóa có kích thước tối thiểu là 128 bit; + Sử dụng một trong các chế độ: CBC, CFB, OFB, GCM, CCM, CTR, XTS. - Đối với thuật toán TDEA: + Sử dụng độ dài khóa có kích thước là 192 bit;
TCVN 12213:2018 (ISO/IEC 10116:2017).	Chế độ hoạt động của mã khối n-bit trong CNTT.	
ISO/IEC 19772:2020	An toàn thông tin – Mã hóa có xác thực (Information security – Authenticated encryption)	

NIST Special Publication 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices	+ Sử dụng một trong các chế độ: CBC, CFB, OFB, CTR.

4.2 Thuật toán mật mã phi đối xứng

Đầu tiên cần xem xét đến độ an toàn phân loại theo kích thước khóa tối thiểu mà tổ chức/cá nhân nên áp dụng. Tham khảo [8], tài liệu này cung cấp trạng thái phê duyệt của các thuật toán mật mã và độ dài khóa được NIST phê duyệt. Trạng thái được biểu thị bằng các điều khoản được chấp nhận, không được phép và sử dụng kế thừa, có nghĩa là thuật toán và độ dài khóa có thể được sử dụng, nhưng rủi ro khi thực hiện phải chấp nhận được.

Trạng thái phê duyệt của các thuật toán được sử dụng để tạo và xác minh chữ ký số được mô tả trong bảng sau:

Quá trình ký số	**Tham số miền**	**Trạng thái**
Tạo chữ ký số	Độ an toàn < 112 bit: + **DSA**: *(L, N)* ≠ (2048, 224), (2048,256) hoặc (3072, 256). + **ECDSA**: $n < 224$. + **RSA**: *nlen* < 2048.	Không được chấp nhận
	Độ an toàn ≥ 112 bit: + **DSA**: *(L, N)* = (2048, 224), (2048,256) hoặc (3072, 256). + **ECDSA** và **EdDSA**: $n \geq 224$. + **RSA**: *nlen* ≥ 2048.	Được chấp nhận
Kiểm tra chữ ký số	Độ an toàn <112 bit: + **DSA**: ((512 ≤ *L*< 2048) hoặc (160 ≤ *N* < 224)). + **ECDSA**: $160 \leq n < 224$. + **RSA**: 1024 ≤ *nlen* < 2048.	Không được chấp nhận
	Độ an toàn ≥ 112 bit: + **DSA**: *(L, N)* = (2048, 224), (2048, 256) hoặc (3072, 256). + **ECDSA** và **EdDSA**: $n \geq 224$. + **RSA**: *nlen* ≥ 2048.	Được chấp nhận

Trong [7] của BSI trình bày khuyến nghị về kích thước khóa an toàn tối thiểu công bố vào 28 tháng 1 năm 2022 được tổng hợp trong bảng sau:

STT	Thuật toán	Kích thước khóa theo bit	Năm sử dụng
1	RSA	2000	2022
		≥ 3000	2023-2028
2	DSA	2000	2022
		≥ 3000	2023-2028
4	ECDSA	≥ 250	2023-2028
5	ECDH	≥ 250	2023-2028

Tham khảo [7] của BSI xuất bản 28/1/2022, về nội dung khuyến nghị, tổ chức BSI đã đưa ra đánh giá về tính an toàn của các cơ chế mật mã đã chọn, kết hợp với định hướng lâu dài cho việc sử dụng. Các khuyến nghị này cũng được đưa ra, được xem xét hàng năm và điều chỉnh nếu cần thiết. Thông qua các khuyến nghị được nêu trong tài liệu này, nhóm biên soạn tổng hợp lại nội dung khuyến nghị cho mật mã phi đối xứng được mô tả trong bảng sau:

Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	Áp dụng một trong các thuật toán mật mã sau: - Đối với thuật toán RSA: + nlen ≥ 2048 + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký. - Đối với thuật toán ECDSA, ECDH: + nlen ≥ 256 + Áp dụng ECDH để phân
PKCS #1	RSA Cryptography Standard	

ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	phối khóa và ECDSA để ký. - Đối với thuật toán DSA, DH: + $L \geq 3072$, $N \geq 256$. + Áp dụng DH để phân phối khóa và DSA để ký.

Ký hiệu	Mô tả
nlen	Đối với thuật toán RSA: *nlen* là độ dài modulo theo bit; Đối với thuật toán ECDH, ECDSA,: *nlen* là độ dài theo bit của cấp của phần tử sinh.
L	Đối với thuật toán DSA, DH: *L* là độ dài của tham số miền *p* theo bit.
N	Đối với thuật toán DSA, DH: *N* là độ dài của tham số miền *q* theo bit.

4.3 Thuật toán băm và mã xác thực thông báo

Danh sách các thuật toán băm phổ biến và các tấn công đã biết được mô tả trong bảng sau:

Thuật toán	Kích thước băm (bit)	Các tấn công đã biết	Mô tả
MD2	128	Các tấn công lên hàm nén, tấn công tìm tiền ảnh với độ phức tạp 2^{73} (năm 2008), tấn công tìm va chạm với độ phức $2^{63.3}$ (năm 2009).	Được mô tả trong chuẩn RFC 1319. Đến nay không còn an toàn để sử dụng.
MD4	128	Tấn công tìm va chạm lên MD4 đủ số vòng với độ phức tạp nhỏ chỉ 2 lần tính toán hàm băm (mất một vài micro giây) năm 2007. Yu Sasaki, Lei Wang, Kazuo Ohta, Noboru Kunihiro: *New Message Difference for MD4*. Fast Software Encryption 2007: 329–348	Được mô tả trong chuẩn RFC 1320. Đến nay không còn an toàn để sử dụng.
MD5	128	Năm 2013, tấn công tìm va chạm của X. Tao và cộng sự lên MD5 với độ phức tạp	Được mô tả trong chuẩn RFC 1321. Đến nay không còn an toàn để sử dụng.

		chỉ là 2^{18} (1 giây trên máy tính thông thường).	Mặc dù, thuật toán này bị phá vỡ hoàn toàn trong thời gian không đáng kể, song đến nay (2020) MD5 vẫn được sử dụng rộng rãi trong nhiều sản phẩm.
MDC2	112	Tấn công tìm va chạm có độ phức tạp 2^{32} và tìm tiền ảnh là $2^{64.3}$ (khi sử dụng DES)	Thuật toán băm dựa trên mật mã đối xứng, được chuẩn hóa trong tiêu chuẩn ISO/IEC 10118-2.
RIPEMD	128, 160, 256, 320	Thuật toán RIPEMD gốc (gọi là RIPEMD-128) là không an toàn vì các điểm yếu trong thiết kế và kích thước băm nhỏ. Phiên bản RIPEMD-160 có Kích thước băm chưa đủ lớn để an toàn ở thời điểm hiện nay. Mặc dù các phiên bản RIPEMD-256 và RIPEMD-320 chưa có những tấn công cụ thể, song ít được sử dụng.	Là một họ các thuật toán băm được phát triển vào năm 1992.
SHA-1	160	Năm 2011, Marc Steven đưa ra tấn công va chạm lên SHA-1 đầy đủ số vòng với độ phức tạp khoảng $2^{63.3}$.	Được mô tả trong tiêu chuẩn FIPS 180-4. Hiện nay SHA-1 không được xem là an toàn, song vẫn còn được sử dụng nhiều trên thế giới.
SHA-2	224, 256, 384, 512	Năm 2011 tấn công tìm tiền ảnh lên 57/80 vòng của SHA-512 và 52/64 vòng của SHA-256. Tấn công giả va chạm lên 46/64 vòng của SHA-256. Hiện chưa có các tấn công lên các phiên bản đầy đủ của SHA-2.	Được mô tả trong tiêu chuẩn FIPS 180-4 (Liên bang Mỹ).

SHA-3	224, 256, 384, 512	Tấn công tiền ảnh lên 8 vòng yêu cầu độ phức tạp $2^{511.5}$ và độ phức tạp dữ liệu 2^{508}. Chưa có tấn công lên phiên bản đầy đủ của SHA-3.	Được mô tả trong tiêu chuẩn FIPS 202 (Liên bang Mỹ).
Whirlpool	512	Chưa có tấn công lên phiên bản thuật toán băm đầy đủ.	Được mô tả trong tiêu chuẩn ISO/IEC 10118-3.
BLAKE	224, 256, 384, 512	Chưa có tấn công lên phiên bản thuật toán băm đầy đủ.	Thuật toán băm dựa trên mã dòng Chacha (sử dụng cấu trúc HAIFA).
Poly1305	128	Độ an toàn của Poly1305 được xem là phụ thuộc vào thuật toán sử dụng cùng.	Thuật toán gốc Poly1305-AES sử dụng thuật toán AES để tính giá trị mã xác thực MAC. Thuật toán xác thực thông điệp (MAC) không sử dụng AES được mô tả trong RFC 8439. Poly1305 sử dụng Chacha20 được định nghĩa trong RFC 7905. Một số chuẩn còn sử dụng thuật toán Salsa cho Poly1305.
Streebog	256, 512	Tấn công tốt nhất là tìm tiền ảnh thứ 2 với độ phức tạp thời gian 2^{666}. Chưa có tấn công hiệu quả nào lên phiên bản đầy đủ của Streebog.	Thuật toán băm được mô tả trong tiêu chuẩn quốc gia của Liên bang Nga (GOST R.34.11-2012), và trong RFC 6986.
SM3	256	Chưa có tấn công hiệu quả nào lên phiên bản đầy đủ của SM3.	Thuật toán băm của Trung Quốc và được mô tả trong tiêu chuẩn ISO/IEC 10118-3:2018.

Theo khuyến cáo của các tổ chức tiêu chuẩn thế giới cũng như các khuyến cáo của NIST cụ thể là NIST SP 800-107, cho đến thời điểm hiện tại các thuật toán băm từ SHA2, SHA3 được coi là an toàn và khó bị tấn công khi sử dụng để bảo tính xác thực và toàn vẹn cho dữ liệu. Hiện nay thuật toán SHA-1 đã được các tổ chức trên thế giới khuyến cáo không nên sử dụng, tại một số Quốc gia như Mỹ, Liên minh Châu Âu đã bắt buộc sử dụng SHA2 trở lên

Tham khảo [7] của BSI xuất bản 28/1/2022. Về nội dung khuyến nghị, tổ chức BSI đã đưa ra đánh giá về tính an toàn của các cơ chế mật mã đã chọn, kết hợp với định hướng lâu dài cho việc sử dụng. Các khuyến nghị này cũng được đưa ra, được xem xét hàng năm và điều chỉnh nếu cần thiết. Thông qua các khuyến nghị được nêu trong tài liệu này, nhóm biên soạn tổng hợp lại nội dung khuyến nghị trong bảng sau:

Thuật toán băm:

Ký hiệu tiêu chuẩn	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
TCVN 11816-3:2017	Công nghệ thông tin-Các kỹ thuật an toàn-Hàm băm-Phần 3: Hàm băm chuyên dụng	Sử dụng một trong các thuật toán sau: SHA-256, SHA-384, SHA-512/256, SHA-512, SHA3-256, SHA3-384, SHA3-512.
FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

Thuật toán xác thực thông điệp:

Ký hiệu tiêu chuẩn	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
TCVN 11495-1:2016	Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC) - Phần 2: Cơ chế sử dụng hàm băm chuyên dụng.	Sử dụng một trong các thuật toán sau: HMAC-SHA-256/128, HMAC-SHA-256, HMAC-SHA-384/192, HMAC-SHA-384, HMAC-SHA-512/256, HMAC-SHA-512, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512
FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

4.4 Hàm dẫn suất khóa

Hàm dẫn xuất khóa (KDF) là thành phần cơ bản và cần thiết của các hệ thống mật mã. Mục tiêu của nó là từ nguồn tư liệu khóa ban đầu nào đó (thông thường chứa một độ ngẫu nhiên nhất định nào đó, nhưng không có phân bố đều hoặc kẻ tấn công có một phần tri thức về nguồn dữ liệu đó) điều chế thành một hoặc nhiều khóa mật mã mạnh.

Số lượng và độ dài của các khóa mật mã phụ thuộc vào các thuật toán mật mã cụ thể cần đến những khóa đó. Nhìn chung, các hàm dẫn xuất khóa phải đáp ứng được mọi mức độ về số lượng và độ dài nói trên. Thuật ngữ "khóa mật mã mạnh" được đề cập ở đây mang ý nghĩa là các khóa giả ngẫu nhiên mà người ta không thể phân biệt được với một xâu các ký tự ngẫu nhiên phân bố đều, có độ dài được xác định bởi sức mạnh tính toán trên thực tế. Đặc biệt, các hàm dẫn xuất khóa phải bảo đảm rằng thông tin về một phần các bit hoặc khóa từ đầu ra của hàm KDF không làm lộ thông tin về các bit khác được sinh ra.

Hàm dẫn suất khóa dựa trên mật khẩu 2 (PBKDF 2) là lược đồ được tiêu chuẩn hóa duy nhất (tại [19] và "*RFC 2898*"). PBKDF2 sử dụng các hàm giả ngẫu nhiên (PRF), thường được triển khai bởi HMAC (thông thường là hàm HMAC-SHA-256).

Căn cứ vào các nghiên cứu kể trên, nhóm biên soạn tổng hợp lại nội dung khuyến nghị cho hàm dẫn xuất khóa được mô tả trong bảng sau:

Ký hiệu tiêu chuẩn	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
NIST SP 800-132	Recommendation for Password-Based Key Derivation Part 1: Storage Applications	Áp dụng PKDF2

4.5 Bộ tạo bít ngẫu nhiên

Bộ tạo bít ngẫu nhiên được phân làm hai dạng chính bao gồm:

- Bộ tạo bít ngẫu nhiên tất định (bộ tạo bít giả ngẫu nhiên);

- Bộ tạo bít ngẫu nhiên bất định;

Bộ tạo bít ngẫu nhiên tất định là cấu trúc mật mã được xây dựng với trạng thái bên trong có thể được tạo mầm và làm mới bằng đầu ra của nguồn ngẫu nhiên và từ đó có thể trích xuất các bit giả ngẫu nhiên. Theo [3], [14], các bộ tạo bít ngẫu nhiên bao gồm Hash_DRBG, HMAC_DRBG, CTR_DRBG(AES), MS_DRBG và MQ_DRBG được các tổ chức quốc tế khuyến cáo sử dụng. Trong thực tế, các thiết bị HSM đang lưu thông trên thị trường đều hỗ trợ các bộ tạo bít ngẫu nhiên này.

Bộ tạo bít ngẫu nhiên bất định bao gồm các nguồn ngẫu nhiên vật lý. Các nguồn ngẫu nhiên vật lý này là một phần cứng quan trọng và được ứng dụng rộng rãi trong bảo mật thông tin và mật mã, thường được sử dụng để tạo ra các khóa phiên, mật khẩu dùng một lần, làm mầm ngẫu nhiên, làm IV trong mã hóa… Các bộ tạo số ngẫu nhiên dựa trên nguồn nhiễu không thể điều khiển và dự đoán được. Trên thế giới có một số tiêu chuẩn đã được ban hành bởi các tổ chức quốc tế như NIST, BSI…, bao gồm [20], [21]. Trong đó các bộ tạo bít ngẫu nhiên bất định gồm XOR-NRBG và Oversampling-NRBG được khuyến cáo và được sử dụng phổ biến, đảm bảo an toàn.

Căn cứ vào các nghiên cứu kể trên, nhóm biên soạn tổng hợp lại nội dung

khuyến nghị cho bộ tạo bít ngẫu nhiên được mô tả trong bảng sau:

Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
TCVN 12853:2020	Các kỹ thuật an toàn - Bộ tạo bit ngẫu nhiên	Áp dụng một trong bốn tiêu chuẩn và sử dụng một trong các bộ tạo bit ngẫu nhiên sau: Hash_DRBG, HMAC_DRBG, CTR_DRBG(AES), MS_DRBG, MQ_DRBG, XOR-NRBG, Oversampling-NRBG.
NIST SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	
NIST SP 800-90C	Recommendation for Random Bit Generator (RBG) Constructions	
AIS-31	A proposal for: Functionality classes for random number generators	

4.6 Lưu trữ các tham số an toàn

Các thiết bị HSM đều lưu trữ các tham số an toàn trên chính thiết bị, bao gồm khóa của thuật toán mật mã đối xứng, khóa bí mật của thuật toán phi đối xứng… Các tham số này cần được bảo vệ.

Trong mật mã, cấu trúc bọc khóa là một loại thuật toán mã hóa đối xứng được thiết kế để đóng gói (mã hóa) tài liệu khóa mật mã. Thuật toán Key Wrap dành cho các ứng dụng như bảo vệ khóa khi được lưu trữ không tin cậy hoặc truyền khóa qua mạng truyền thông không tin cậy.

Gói khóa có thể được coi là một dạng thuật toán đóng gói khóa, mặc dù không nên nhầm lẫn nó với các thuật toán đóng gói khóa bất đối xứng (khóa công khai) phổ biến hơn (ví dụ: PSEC-KEM). Thuật toán Key Wrap có thể được sử dụng trong một ứng dụng tương tự: để vận chuyển khóa phiên một cách an toàn bằng cách mã hóa nó bằng khóa mã hóa dài hạn. Trong [22], các chế độ KW và KWP được các tổ chức trên thế giới khuyến nghị.

Căn cứ vào các nghiên cứu kể trên, nhóm biên soạn tổng hợp lại nội dung khuyến nghị cho bộ tạo bít ngẫu nhiên được mô tả trong bảng sau:

Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
SP800-38F	Recommendation for	Các tham số an toàn phải áp dụng AES chế độ KW hoặc

	Block Cipher Modes of Operation: Methods for Key Wrapping	KWP để mã hóa được lưu trữ trên thiết bị.

4.7 Giao diện lập trình ứng dụng

Trong hệ thống thiết bị thông tin, thông thường có rất nhiều các giao diện khác nhau, HSM cũng không là ngoại lệ và được phân chia theo ứng dụng và hệ điều hành được thiết kế. Thông thường sẽ có 3 loại giao diện lập trình ứng dụng độc lập gồm:

- Giao diện lập trình quản lý khóa;

- Giao diện lập trình lệnh;

- Giao diện lập trình quản lý người dùng.

Tiêu chuẩn PKCS#11 là API cho HSM, chứa các thông tin về mật mã và thực hiện các thuật toán mật mã. PKCS là chuẩn cho mã hóa công khai được phát triển từ năm 1991 bởi RSA Laboratories, đối với HSM, giao diện PKCS#11 là giao diện được sử dụng rộng rãi nhất.

Một trong những lợi ích chính của PKCS#11 là khả năng liên kết hoạt động giữa ứng dụng và mô-đun bảo mật. PKCS#11 cũng cung cấp các phương thức mật mã.

Trong thực tiễn, các thiết bị HSM trên thị trường hiện nay đều hỗ trợ và áp dụng tiêu chuẩn này. Qua đó nhóm biên soạn khuyến nghị cho giao diện lập trình ứng dụng được mô tả trong bảng sau:

Ký hiệu tiêu chuẩn	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
PKCS#11	Cryptographic Token Interface Base Specification	Phiên bản 2.2 trở lên

Tài liệu tham khảo

[1]. TCVN 11367-3:2016 (ISO/IEC 18033-3:2010) "*Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối*".

[2]. TCVN 12213:2018 (ISO/IEC 10116:2017) "*Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động của mã khối n-bit*".

[3]. TCVN 12853:2020 (ISO/IEC 18031:2011 With amendment 1:2017) "*Công nghệ thông tin - Các kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên*".

[4]. TCVN 11816 (ISO/IEC 10118) "*Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng*".

[5]. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "*Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác nhận thông điệp*".

[6]. ISO/IEC 27040:2015 "*Information technology – Security techniques – Storage security*".

[7]. Federal Office for Information Security, BSI TR-02102-1 *"Cryptographic Mechanisms: Recommendations and Key Lengths"*, January 2022.

[8]. National Institute of Standards and Technology, Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths",* March 2019.

[9]. National Institute of Standards and Technology, Special Publication 800-132 *"Recommendation for Password-Based Key Derivation: Part 1: Storage Applications"*, December 2010.

[10]. National Institute of Standards and Technology, FIPS 186-4 "*Digital Signature Standard (DSS)*", July 2013.

[11]. National Institute of Standards and Technology, FIPS 180-4 "*Secure Hash Standard (SHS)*", August 2015.

[12]. National Institute of Standards and Technology, FIPS 202 "*SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*", August 2015.

[13]. National Institute of Standards and Technology, Special Publication 800-38E "*Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*", January 2010.

[14]. National Institute of Standards and Technology, Special Publication 800-90A *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*, June 2015.

[15]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General",* May 2020.

[16]. National Institute of Standards and Technology, Special Publication 800-56B Revision 2 *"Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography",* March 2019.

[17]. National Institute of Standards and Technology, Special Publication 800-38D*, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC"*, November 2007.

[18]. National Institute of Standards and Technology, Special Publication 800-38C "*Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality"*, July 2007.

[19]. RSA Laboratories' Public-Key Cryptography Standards (PKCS) series (PKCS #5 v2.0

[20]. National Institute of Standards and Technology, Special Publication NIST SP 800-90C, *"Recommendation for Random Bit Generator (RBG) Constructions",* September 2022.

[21]. Bundesamt für Sicherheit in der Informationstechnik (BSI), AIS-31, *A proposal for: Functionality classes for random number generators Version 2.0, 18 September 2011*

[22]. National Institute of Standards and Technology, Special Publication NIST SP800-38F, *"Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping",* December 2012.