

BAN CƠ YẾU CHÍNH PHỦ

DỰ ÁN

XÂY DỰNG TIÊU CHUẨN QUỐC GIA

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN TOÀN - QUẢN LÝ KHÓA -  
PHẦN 3: CÁC CƠ CHẾ SỬ DỤNG KỸ THUẬT KHÔNG ĐỐI XỨNG

HÀ NỘI - 2024

# DỰ ÁN XÂY DỰNG TIÊU CHUẨN QUỐC GIA

## 1. Tên tiêu chuẩn

- **Tiếng Việt:** TCVN XXXX-3:2024 (ISO/IEC 11770-3:2021), Công nghệ thông tin - Kỹ thuật an toàn - Quản lý khóa - Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng.

- **Tiếng Anh:** TCVN XXXX-3:2024 (ISO/IEC 11770-3:2021), Information security - Key management - Part 3: Mechanisms using asymmetric techniques.

- **Ký hiệu tiêu chuẩn:** TCVN XXXX-3:2024 (ISO/IEC 11770-3:2021).

Ghi chú: Số tiêu chuẩn sẽ được thay đổi sau khi có quyết định công bố của Bộ Khoa học và Công nghệ.

## 2. Phạm vi áp dụng của tiêu chuẩn

Tiêu chuẩn này mô tả các lược đồ có thể được sử dụng cho thỏa thuận khóa và các lược đồ có thể được sử dụng cho vận chuyển khóa.

Các hệ thống mật mã khóa công khai lần đầu tiên được đề xuất trong bài báo chuyên đề của Diffie và Hellman vào năm 1976. Tính bảo mật của nhiều hệ thống mật mã như vậy dựa trên tính khó giải được giả định của việc giải bài toán logarit rời rạc trên các trường hữu hạn nhất định. Các hệ thống mật mã khóa công khai khác như RSA dựa trên độ khó của bài toán phân tích thừa số nguyên.

Lớp thứ ba của hệ thống mật mã khóa công khai dựa trên các đường cong elliptic. Tính bảo mật của một hệ thống khóa công khai như vậy phụ thuộc vào độ khó của việc xác định các logarit rời rạc trong nhóm các điểm của một đường cong elliptic. Khi dựa trên một đường cong elliptic được lựa chọn cẩn thận, vấn đề này, với kiến thức hiện tại, khó hơn nhiều so với việc phân tích thành thừa số của các số nguyên hoặc tính toán các logarit rời rạc trong một trường hữu hạn có kích thước tương đương. Tất cả các thuật toán có mục đích chung đã biết để xác định logarit rời rạc của đường cong elip đều mất thời gian theo cấp số nhân. Do đó, các hệ thống khóa công khai dựa trên đường cong elip có thể sử dụng các tham số ngắn hơn nhiều so với hệ thống RSA hoặc các hệ thống dựa trên logarit rời rạc cổ điển sử dụng nhóm nhân của một số trường hữu hạn. Điều này mang lại chữ ký số ngắn hơn đáng kể, cũng như các tham số hệ thống,

Tiêu chuẩn này bao gồm các cơ chế dựa trên:

- Trường hữu hạn;
- Đường cong elip;
- Cặp song tuyến tính.

Tiêu chuẩn này xác định các cơ chế quản lý khóa dựa trên các kỹ thuật mã hóa phi đối xứng. Nội dung tiêu chuẩn đề cập cụ thể đến việc sử dụng các kỹ thuật phi đối xứng để đạt được các mục tiêu sau.

a) Thiết lập khóa bí mật dùng chung để sử dụng trong kỹ thuật mật mã đối xứng giữa hai thực thể A và B theo thỏa thuận khóa. Trong cơ chế thỏa thuận khóa bí mật, khóa bí mật được tính là kết quả của việc trao đổi dữ liệu giữa hai thực thể A và B. Không ai trong số họ có thể xác định trước giá trị của khóa bí mật được chia sẻ.

b) Thiết lập khóa bí mật dùng chung để sử dụng trong kỹ thuật mật mã đối xứng giữa hai thực thể A và B thông qua vận chuyển khóa. Trong cơ chế vận chuyển khóa bí mật, khóa bí mật được chọn bởi một thực thể A và được chuyển đến một thực thể B khác và được bảo vệ phù hợp bằng các kỹ thuật mật mã phi đối xứng.

c) Cung cấp khóa công khai của một thực thể cho các thực thể khác thông qua vận chuyển khóa. Trong cơ chế vận chuyển khóa công khai, khóa công khai của thực thể A được chuyển đến các thực thể khác thông qua xác thực nhưng không yêu cầu bảo mật.

Tiêu chuẩn này không đề cập đến một số khía cạnh của quản lý khóa, chẳng hạn như:

- Quản lý vòng đời khóa;
- Cơ chế tạo hoặc xác thực các cặp khóa phi đối xứng;
- Cơ chế lưu trữ, lưu trữ, xóa, hủy, ... các khóa.

Mặc dù tiêu chuẩn này không đề cập rõ ràng đến việc phân phối khóa riêng của thực thể từ bên thứ ba tin cậy đến thực thể yêu cầu, nhưng các cơ chế vận chuyển khóa được mô tả có thể được sử dụng để thực hiện phân phối khóa. Trong mọi trường hợp, khóa bí mật có thể được phân phối thông qua các cơ chế này trong khi đã tồn tại khóa thỏa hiệp có sẵn. Tuy nhiên, trong thực tế, việc phân phối khóa bí mật thường là một quy trình thủ công dựa trên các phương tiện công nghệ như: thẻ thông minh, ... .

Tiêu chuẩn này không chỉ định các biến đổi được sử dụng trong các cơ chế quản lý khóa.

### 3. Tổ chức đề nghị

- Tên tổ chức: Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã.
- Địa chỉ: số 23 Nguyễn Như Kon Tum, Nhân Chính, Thanh Xuân, Hà Nội.
- Điện thoại: 02432323313
- E-mail: info@nacis.gov.vn

- Tên cơ quan chủ quản: Ban Cơ yếu Chính phủ.

#### **4. Tình hình đối tượng tiêu chuẩn trong nước và ngoài nước**

##### **a) Trong nước**

Trong những năm qua, lĩnh vực CNTT của Việt Nam đã có những bước phát triển vượt bậc, đóng góp không nhỏ vào quá trình xây dựng và phát triển đất nước. CNTT đã được ứng dụng rộng rãi trong toàn xã hội, đặc biệt là được ứng dụng rộng khắp trong các hệ thống quan trọng như viễn thông, điện lực, tài chính, ngân hàng,... Sự phát triển mạnh mẽ của CNTT đã thúc đẩy quá trình kết nối giữa các hệ thống thông tin của mỗi quốc gia và giữa các quốc gia với nhau một cách nhanh chóng, đem lại rất nhiều lợi ích về mọi mặt của đời sống.

Đảng và Nhà nước ta đã và đang thực hiện mạnh mẽ chủ trương ứng dụng CNTT nhằm cải cách hành chính, hiện đại hóa cơ quan chính phủ, xây dựng một Chính phủ hiệu lực, hiệu quả hơn, thực sự của dân, do dân và vì dân, nâng cao năng lực cạnh tranh, tạo môi trường thuận lợi phát triển kinh tế - xã hội. Điều này được thể hiện rõ trong chiến lược phát triển kinh tế - xã hội, các chương trình về cải cách hành chính của đất nước. Cụ thể hóa chủ trương, đường lối của Đảng về phát triển ứng dụng CNTT, Quốc hội, Chính phủ, Thủ tướng Chính phủ đã ban hành nhiều văn bản quy phạm pháp luật, kế hoạch, chương trình ứng dụng CNTT trong các cơ quan nhà nước hết sức cụ thể, thiết thực, như: Luật Công nghệ thông tin; Luật giao dịch điện tử; Luật an ninh mạng; Luật an toàn thông tin mạng; Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước; Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước; Quyết định số 749/QĐ-TTg ngày 3/6/2020 về việc Phê duyệt “Chương trình chuyển đổi số Quốc gia đến năm 2025, định hướng năm 2030” và Quyết định số 942/QĐ-TTg ngày 15/6/2021 về việc Phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021-2025, định hướng năm 2030; Nghị định số 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng.

Gắn liền với sự phát triển của CNTT, việc đảm bảo an toàn an toàn thông tin là một yêu cầu không thể thiếu. Để bảo đảm tính thống nhất trong công tác quản lý chất lượng các thiết bị, phương pháp, các giải pháp bảo mật đảm bảo an toàn thông tin thì việc xây dựng một hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia là hết sức cần thiết. Một số quốc gia phát triển như Hoa Kỳ, Canada, Anh, Pháp, Đức, Nhật Bản,... đã xây dựng được cho họ một hệ thống tiêu chuẩn về an toàn thông tin và mật mã khá đầy đủ. Ở nước ta các tiêu chuẩn về bảo mật, an toàn thông tin vẫn còn chưa được đầy đủ.

Hiện nay, trong lĩnh vực mật mã dân sự, Ban Cơ yếu Chính phủ đã xây dựng và đề xuất Bộ Khoa học và Công nghệ công bố được 61 tiêu chuẩn quốc gia bao gồm:

TT	Ký hiệu	Tên tiêu chuẩn	Cơ quan đề xuất
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
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 11770-1:2010)	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần	Ban Cơ yếu Chính phủ

		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	Ban Cơ yếu Chính phủ.
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	Ban Cơ yếu Chính phủ
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
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.	Ban Cơ yếu Chính phủ
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
22	TCVN 12214-1:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
25	TCVN 11367-5:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật mã dựa trên định	Ban Cơ yếu Chính phủ

		danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	Ban Cơ yếu Chính phủ
36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an	Ban Cơ yếu

		toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	Ban Cơ yếu Chính phủ
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	Ban Cơ yếu Chính phủ
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	Ban Cơ yếu Chính phủ
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	Ban Cơ yếu Chính phủ
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù –	Ban Cơ yếu Chính phủ

		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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
58	TCVN 13722:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viển sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học	Ban Cơ yếu Chính phủ
59	TCVN 13723-1:2023	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 1: Giới thiệu, khái niệm và yêu cầu chung	Ban Cơ yếu Chính phủ
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)	Ban Cơ yếu Chính phủ
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin	Ban Cơ yếu

	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)	Chính phủ
--	--	-----------

Việt Nam là thành viên của ISO/IEC, việc xây dựng các tiêu chuẩn quốc gia dựa trên cơ sở chấp thuận hoàn toàn tương đương các tiêu chuẩn của ISO/IEC với mục đích phù hợp, hài hòa với các tiêu chuẩn quốc tế, tránh các rào cản thương mại, bảo vệ quyền lợi và lợi ích của các doanh nghiệp cung cấp cũng như của người sử dụng.

### b) Ngoài nước

Tiêu chuẩn hoá mật mã được khởi đầu vào cuối những năm 70 và đầu năm tám mươi của thế kỷ trước, khi công nghệ thông tin và mạng máy tính ra đời và được ứng dụng rộng rãi vào các lĩnh vực kinh tế xã hội. Công nghệ thông tin được phát triển và ứng dụng trước hết ở các quốc gia công nghiệp tiên tiến như Mỹ, Canada, Nhật Bản và các nước phương Tây. Do đó, vai trò quyết định trong quá trình hình thành hệ thống tiêu chuẩn ATTT nói chung và tiêu chuẩn mật mã nói riêng thuộc về các tổ chức tiêu chuẩn tại các quốc gia này, nổi bật là Viện tiêu chuẩn và Công nghệ quốc gia Hoa kỳ NIST, Viện tiêu chuẩn quốc gia Hoa kỳ ANSI, Viện tiêu chuẩn Anh BSI. Ngoài ra còn có một số tổ chức tiêu chuẩn công nghiệp như 3GPP (Third Generation Partnership Project), ETSI European Telecommunications Standards, IEEE (Institute of electrical and electronic Engineer), SECG (Standards for Efficient Cryptography Group), PKCS<sub>s</sub>) Public-Key Cryptography Standards).

Trong lĩnh vực tiêu chuẩn hoá nói chung và tiêu chuẩn hoá trong lĩnh vực kỹ thuật mật mã nói riêng, tổ chức tiêu chuẩn quốc tế ISO có vai trò đặc biệt. Đây là tổ chức liên kết các nước thành viên và hoạt động với mục tiêu “quốc tế hóa” các tiêu chuẩn trên phạm vi toàn cầu. Ngoài các cơ quan chính phủ và các tổ chức tiêu chuẩn uy tín nêu trên, một số tổ chức khác như Cộng đồng Internet (Internet Community) đã có đóng góp không nhỏ vào sự hình thành hệ thống tiêu chuẩn về ATTT, đặc biệt là trong việc xây dựng các tiêu chuẩn kỹ thuật.

Nhờ nỗ lực của các tổ chức kể trên đến nay, hiện nay, trên thế giới đã hình thành một hệ thống tiêu chuẩn mật mã khá đầy đủ, bao quát được hầu hết các khía cạnh của lĩnh vực này và có thể phân thành ba loại: tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn quốc gia. Tiêu chuẩn quốc tế (do các tổ chức quốc tế ISO và IEC tổ chức xây dựng và công bố), các Tiêu chuẩn quốc gia (do Chính phủ các nước công bố) và các Tiêu chuẩn của các tổ chức chuyên ngành (tương ứng ở nước ta gọi là tiêu chuẩn cơ sở). Tại các quốc gia đang phát triển, tiêu chuẩn quốc gia và tiêu chuẩn chuyên ngành phần lớn được xây dựng theo hướng chấp thuận nguyên vẹn hoặc tham khảo các tiêu chuẩn quốc tế ở các nước phát

triển, như là tiêu chuẩn của NIST, ANSI, BS và đặc biệt của ISO/IEC với một hệ thống tiêu chuẩn có ảnh hưởng trên phạm vi toàn cầu.

### 5. Lý do và mục đích xây dựng TCVN

- Tiêu chuẩn đáp ứng những mục tiêu nào sau đây:

- |                                  |                                     |                     |                          |
|----------------------------------|-------------------------------------|---------------------|--------------------------|
| + Thông tin, thông hiểu          | <input checked="" type="checkbox"/> | + Tiết kiệm         | <input type="checkbox"/> |
| + An toàn sức khoẻ môi trường    | <input type="checkbox"/>            | + Giảm chủng loại   | <input type="checkbox"/> |
| + Đòi hỏi                        | <input type="checkbox"/>            | + Các mục đích khác | <input type="checkbox"/> |
| + Chức năng công dụng chất lượng | <input checked="" type="checkbox"/> |                     |                          |

- Tiêu chuẩn có dùng để chứng nhận không?  Có  Không

- Căn cứ:

+ Tiêu chuẩn có liên quan đến yêu cầu phát triển KTXH của Nhà nước không?  Có  Không

+ Thuộc chương trình nào?

+ Yêu cầu hài hoà tiêu chuẩn (quốc tế và khu vực):  Có  Không

### 6. Những vấn đề sẽ xây dựng tiêu chuẩn

- Những vấn đề sẽ xây dựng tiêu chuẩn (hoặc sửa đổi bổ sung):

- |                                 |                                     |   |                                     |
|---------------------------------|-------------------------------------|---|-------------------------------------|
| + Thuật ngữ và định nghĩa       | <input type="checkbox"/>            | + Tiêu chuẩn cơ bản                       | <input checked="" type="checkbox"/> |
| + Phân loại                     | <input type="checkbox"/>            | + Yêu cầu an toàn vệ sinh                 | <input type="checkbox"/>            |
| + Ký hiệu                       | <input type="checkbox"/>            | + Yêu cầu về môi trường                   | <input type="checkbox"/>            |
| + Thông số và kích thước cơ bản | <input type="checkbox"/>            | + Lấy mẫu                                 | <input type="checkbox"/>            |
| + Yêu cầu kỹ thuật              | <input checked="" type="checkbox"/> | + Phương pháp thử và kiểm tra             | <input type="checkbox"/>            |
| + Tiêu chuẩn về quá trình       | <input type="checkbox"/>            | + Bao gói, ghi nhãn, vận chuyển, bảo quản | <input type="checkbox"/>            |
| + Tiêu chuẩn về dịch vụ         | <input type="checkbox"/>            | + Các khía cạnh và yêu cầu khác           | <input type="checkbox"/>            |

(ghi cụ thể ở dưới) :

- Bộ cục, nội dung các phần chính của TCVN dự kiến:

Giới thiệu

1. Phạm vi

2. Tài liệu viện dẫn
3. Thuật ngữ và định nghĩa
4. Ký hiệu và thuật ngữ viết tắt
5. Yêu cầu
6. Hàm dẫn xuất khóa
7. Phép nhân Cofactor
8. Cam kết khóa
9. Xác nhận khóa
10. Khung quản lý khóa
  - 10.1. Tổng quát
  - 10.2. Thỏa thuận khóa giữa hai bên
  - 10.3. Thỏa thuận khóa giữa ba bên
  - 10.4. Vận chuyển khóa bí mật
  - 10.5. Vận chuyển khóa công khai
11. Thỏa thuận khóa
  - 11.1. Cơ chế thỏa thuận khóa 1
  - 11.2. Cơ chế thỏa thuận khóa 2
  - 11.3. Cơ chế thỏa thuận khóa 3
  - 11.4. Cơ chế thỏa thuận khóa 4
  - 11.5. Cơ chế thỏa thuận khóa 5
  - 11.6. Cơ chế thỏa thuận khóa 6
  - 11.7. Cơ chế thỏa thuận khóa 7
  - 11.8. Cơ chế thỏa thuận khóa 8
  - 11.9. Cơ chế thỏa thuận khóa 9
  - 11.10. Cơ chế thỏa thuận khóa 10
  - 11.11. Cơ chế thỏa thuận khóa 11

Phụ lục A (Tham khảo) Định danh đối tượng

Phụ lục B (Tham khảo) Thuộc tính của các cơ chế thiết lập khóa

Phụ lục C (Tham khảo) Ví dụ về các hàm dẫn xuất khóa

Phụ lục D (Tham khảo) Ví dụ về cơ chế thiết lập khóa

Phụ lục E (Tham khảo) Ví dụ về cơ chế thiết lập khóa dựa trên đường cong Elliptic

Phụ lục F (Tham khảo) Ví dụ về cơ chế thiết lập khóa dựa trên ghép nối song tuyến tính

Phụ lục G (Tham khảo) Vận chuyển khóa bí mật

Tài liệu tham khảo

- Nhu cầu khảo nghiệm tiêu chuẩn quốc gia  Có  Không  
trong thực tế:

(nếu có, ghi rõ dự kiến nội dung cần khảo nghiệm, quy mô, địa điểm, thời gian khảo nghiệm)

### 7. Phương thức thực hiện và tài liệu làm căn cứ xây dựng TCVN

- Phương thức thực hiện:

+ Xây dựng mới  + Sửa đổi, bổ sung   
+ Chấp nhận tiêu chuẩn quốc tế  + Thay thế

- Tài liệu chính làm căn cứ xây dựng TCVN (bản chụp kèm theo):

*ISO/IEC 11770-3:2021, Information security – Key management – Part 3: Mechanisms using asymmetric techniques.*

### 8. Kiến nghị thành lập Ban kỹ thuật (hoặc Tiểu ban kỹ thuật)

Không.

### 9. Cơ quan phối hợp

- Ban kỹ thuật tiêu chuẩn có liên quan phải lấy ý kiến: Tiểu Ban kỹ thuật tiêu chuẩn TCVN/JTC 1/SC 27 “Các kỹ thuật mật mã”.

- Dự kiến các cơ quan, tổ chức, cá nhân lấy ý kiến góp ý cho dự thảo:

- + Cục Quản lý kỹ thuật nghiệp vụ mật mã, Ban Cơ yếu Chính phủ;
- + Cục Chứng thực số và Bảo mật thông tin, Ban Cơ yếu Chính phủ;
- + Viện Khoa học – Công nghệ Mật mã, Ban Cơ yếu Chính phủ;
- + Học viện kỹ thuật mật mã, Ban Cơ yếu Chính phủ;
- + Hiệp hội an toàn thông tin Việt Nam (VNISA);
- + Một số Công ty hoạt động trong lĩnh vực công nghệ thông tin.

### 10. Dự kiến tiến độ thực hiện

TT	Nội dung công việc	Thời gian	
		Bắt đầu	Kết thúc
1	Biên soạn dự thảo TCVN	5/2024	7/2024
	- Thu thập tài liệu		
	- Dịch và nghiên cứu các tài liệu chính làm cơ sở cho việc biên soạn tiêu chuẩn quốc gia		
	- Biên soạn dự thảo Ban kỹ thuật		
	- Gửi lấy ý kiến dự thảo Ban kỹ thuật		
	- Họp xem xét nội dung dự thảo Ban kỹ thuật		
	- Biên soạn dự thảo TCVN		
2	Lấy ý kiến dự thảo TCVN	7/2024	8/2024
3	Hội nghị chuyên đề	9/2024	10/2024
4	Hoàn chỉnh dự thảo TCVN và lập hồ sơ dự thảo TCVN	11/2024	11/2024
5	Thẩm tra Hồ sơ dự thảo TCVN	12/2024	12/2024
6	Gửi hồ sơ dự thảo TCVN để thẩm định	02/2025	02/2025
7	Thẩm định dự thảo TCVN	03/2025	04/2025
8	Lập hồ sơ TCVN trình duyệt	05/2025	05/2025
9	Trình duyệt và công bố	06/2025	06/2025

Hà Nội, ngày 24 tháng 4 năm 2024

TRƯỞNG BAN



Vũ Ngọc Thiềm