BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /2023/TT-BQP	*Hà Nội, ngày tháng năm 2023*

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

Căn cứ Luật Tiêu chuẩn và Quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Quốc phòng;

Căn cứ Nghị định số 09/2014/NĐ-CP ngày 27 tháng 01 năm 2014 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

Căn cứ Nghị định số 59/2022/NĐ-CP ngày 05 tháng 9 năm 2022 của Chính phủ quy định về định danh và xác thực điện tử;

Theo đề nghị của Trưởng ban Ban Cơ yếu Chính phủ;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư quy định Danh mục tiêu chuẩn bắt buộc về kỹ thuật mật mã dân sự áp dụng cho thiết bị HSM trong hoạt động định danh và xác thực điện tử.

Điều 1. Phạm vi điều chỉnh

Thông tư này 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 thuộc lĩnh vực kinh tế xã hội *(Phụ lục kèm theo)*.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với tổ chức cung cấp dịch vụ định danh và xác thực điện tử; tổ chức, cá nhân phát triển ứng dụng định danh và xác thực điện tử; tổ chức khai thác cơ sở dữ liệu về định danh và xác thực điện tử.

Điều 3. Tổ chức thực hiện

1. Ban Cơ yếu Chính phủ rà soát, báo cáo Bộ trưởng Bộ Quốc phòng sửa đổi, bổ sung Danh mục tiêu chuẩn bắt buộc về kỹ thuật mật mã dân sự áp dụng cho

thiết bị HSM trong hoạt động định danh và xác thực điện tử quy định tại Điều 1 Thông tư này phù hợp với tình hình phát triển công nghệ và chính sách quản lý của Nhà nước.

2. Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã – Ban Cơ yếu Chính phủ có trách nhiệm hướng dẫn, kiểm tra, đánh giá việc áp dụng các tiêu chuẩn Danh mục tiêu chuẩn bắt buộc về kỹ thuật mật mã dân sự áp dụng cho thiết bị HSM trong hoạt động định danh và xác thực điện tử quy định tại Điều 1 Thông tư này.

Điều 4. Điều khoản thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày … tháng … năm 2023.

2. Trưởng ban Ban Cơ yếu Chính phủ, Thủ trưởng các cơ quan, đơn vị và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, tổ chức và cá nhân phản ánh kịp thời về Ban Cơ yếu Chính phủ để báo cáo Bộ trưởng Bộ Quốc phòng xem xét, giải quyết./.

Nơi nhận:
- Thủ tướng Chính phủ, các Phó Thủ tướng Chính phủ (để b/c);
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Thủ trưởng BQP, CN TCCT;
- Ban Cơ yếu Chính phủ;
- Cục Kiểm tra văn bản QPPL Bộ Tư pháp;
- Cục Tiêu chuẩn - Đo lường - Chất lượng/BTTM;
- Công báo, Cổng TTĐTCP;`
- Vụ Pháp chế/BQP;
- Cổng TTĐTBQP;
- Lưu: VT, BCY. BN110.

BỘ TRƯỞNG

Đại tướng Phan Văn Giang

DỰ THẢO

Phụ lục

DANH MỤC TIÊU CHUẨN BẮT BUỘC VỀ KỸ THUẬT MẬT MÃ DÂN SỰ ÁP DỤNG CHO THIẾT BỊ HSM[1] TRONG HOẠT ĐỘNG ĐỊNH DANH VÀ XÁC THỰC ĐIỆN TỬ

(Ban hành kèm theo Thông tư số /2023/TT-BQP ngày tháng năm 2023 của Bộ trưởng Bộ Quốc phòng)

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
I. Tiêu chuẩn về đặc tính kỹ thuật mật mã				
1	Mật mã đối xứng và chế độ hoạt động	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; + Sử dụng một trong các chế độ: CBC, CFB, OFB, CTR.
		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 sử dụng xác thực (Information security – Authenticated encryption)	
		NIST Special Publication 800-38E	Recommendation for Block Cipher Modes of	

[1] HSM: Hardware Security Module - Mô-đun an toàn phần cứng

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Operation: The XTS-AES Mode for Confidentiality on Storage Devices	
2	Mật mã phi đối xứng và chữ ký số [2]	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 phối khóa và ECDSA để ký.
		PKCS #1	RSA Cryptography Standard	

[2] **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.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		ANSI.X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	- Đối với thuật toán DSA, DH: + $L \geq 3072$, $N \geq 256$. + Áp dụng DH để phân phối khóa và DSA để ký.
3	Thuật toán băm	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	
4	Thuật toán xác thực thông điệp	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.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	
5	Hàm dẫn xuất khóa	NIST SP 800-132	Recommendation for Password-Based Key Derivation Part 1: Storage Applications	Áp dụng PBKDF2, phiên bản 2.0 trở lên.
6	Bộ tạo bit ngẫu nhiên	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	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
7	Lưu trữ các tham số an toàn	SP800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	Các tham số an toàn phải áp dụng AES chế độ KW hoặc KWP để mã hóa được lưu trữ trên thiết bị.
8	Giao diện lập trình ứng dụng	PKCS#11	Cryptographic Token Interface Base Specification	Phiên bản 2.2 trở lên