DỰ THẢO

Phụ lục I

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

(Ban hành kèm theo Thông tư số /2024/TT-BQP ngày tháng năm 2024 của Bộ trưởng Bộ Quốc phòng)

I. 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

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;
		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)	

[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
		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.
2	Mật mã phi đối xứng và chữ ký số	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: + $nlen^2 \geq 2048$ + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký. - Đối với thuật toán ECDSA, ECDH: + $nlen^2 \geq 256$ + 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.

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: + $L \geq 3072$, $N \geq 256$.[3] + 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	

[3] **Ký hiệu** **Mô tả**

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
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.
		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	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		NIST SP 800-90C	Recommendation for Random Bit Generator (RBG) Constructions	
		AIS-31	A proposal for: Functionality classes for random number generators	
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

II. Quy định về mã HS của thiết bị HSM

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mã HS	Mô tả sản phẩm hàng hóa
01		8471.30.90	

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mã HS	Mô tả sản phẩm hàng hóa
02	Sản phẩm mật mã dân sự thuộc nhóm sản phẩm sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã.	8471.41.90	Sản phẩm sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã.
03		8471.49.90	
04		8471.80.90	