BỘ QUỐC PHÒNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 87 /2024/TT-BQP	*Hà Nội, ngày 26 tháng 10 năm 2024*

THÔNG TƯ

Quy định Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng 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 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 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 kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử.

Điều 1. Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử

Tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước thực hiện theo Danh mục ban hành kèm theo Thông tư này.

Điều 2. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành từ ngày 11 tháng 11 năm 2024.

Điều 3. Tổ chức thực hiện

1. Ban Cơ yếu Chính phủ rà soát, đề xuất Bộ trưởng Bộ Quốc phòng sửa đổi, bổ sung Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử theo 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. Ban Cơ yếu Chính phủ xem xét chấp nhận các kết quả thử nghiệm của các tổ chức thử nghiệm đủ năng lực phục vụ cho quá trình đánh giá.

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./.

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.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Đại tướng Nguyễn Tân Cương

Phụ lục

DANH MỤC TIÊU CHUẨN KỸ THUẬT MẬT MÃ ÁP DỤNG BẮT BUỘC CHO MÔ-ĐUN AN TOÀN PHẦN CỨNG TRONG HOẠT ĐỘNG ĐỊNH DANH VÀ XÁC THỰC ĐIỆN TỬ

(Kèm theo Thông tư số 87/2024/TT-BQP ngày 26 tháng 10 năm 2024 của Bộ trưởng Bộ Quốc phòng)

I. Quy định Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng 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 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).	Công nghệ thông tin - Các kỹ thuật an toàn - 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 Operation: The XTS-AES Mode for Confidentiality on Storage Devices	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
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 ≥ 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. - Đối với thuật toán DSA, DH: + L ≥ 3072, N ≥ 256. + Áp dụng DH để phân phối khóa và DSA để ký.
		PKCS #1	RSA Cryptography Standard	
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
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	

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 *(nếu có)*.
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	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		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 mô-đun an toàn phần cứng

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mã HS	Mô tả sản phẩm hàng hóa
01	Sản phẩm mật mã dân sự thuộc nhóm sản phẩm sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã.	8471.30.90	Sản phẩm sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã.
02		8471.41.90	
03		8471.49.90	
04		8471.80.90	

Giải thích chữ viết tắt và ký hiệu:

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CBC	Cipher Block Chaining Mode	Chế độ móc xích khối mã
CCM	Counter with Cipher Block Chaining Message Authentication Code	Bộ đếm với mã xác thực thông báo khối mã hóa
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
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
GCM	Galois/Counter Mode	Chế độ Galois/Bộ đếm
Hash_DRBG	Hash Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định 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

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
HS	Harmonized Commodity Description and Coding System	Hệ thống hài hòa mô tả và mã hóa hàng hóa
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định bậc hai đa biến
MS_DRBG	Micali-Schnorr Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định Micali Schnorr
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật 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
Oversampling-NRBG	Bộ tạo bit ngẫu nhiên bất định theo cấu trúc Oversampling. Được trình bày trong tài liệu SP 800-90C của NIST.	
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn xuất khóa dựa trên mật khẩu 2
PKCS	Public Key Cryptography Standards	Các tiêu chuẩn mật mã khóa công khai
QCVN		Quy chuẩn kỹ thuật quốc gia
RSA	Rivest - Shamir - Adleman	Tên của hệ mã do ba nhà toán học Rivest, Shamir và

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
		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
TDEA	Triple Data Encryption Algorithm	Thuật toán mã hóa dữ liệu Triple-DES
XOR-NRBG	Bộ tạo bit ngẫu nhiên bất định theo cấu trúc XOR. Được trình bày trong tài liệu SP 800-90C của NIST.	
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối hẹp

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