BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /2025/TT-BQP	*Hà Nội, ngày tháng năm 2025*

DỰ THẢO

THÔNG TƯ

Sửa đổi, bổ sung một số Thông tư của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia, Danh mục tiêu chuẩn kỹ thuật áp dụng bắt buộc trong lĩnh vực mật mã dân sự

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 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật; được sửa đổi, bổ sung một số điều tại Nghị định số 78/2018/NĐ-CP ngày 16 tháng 5 năm 2018 của Chính phủ;

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; Nghị định số 03/2025/NĐ-CP ngày 28 tháng 02 năm 2025 của Chính phủ sửa đổi, bổ sung 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;

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

Bộ trưởng Bộ Quốc phòng ban hành Thông tư Sửa đổi, bổ sung một số Thông tư của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia, Danh mục tiêu chuẩn kỹ thuật áp dụng bắt buộc trong lĩnh vực mật mã dân sự.

Điều 1. Sửa đổi, bổ sung Thông tư số 87/2024/TT-BQP ngày 26/10/2024 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

Thay thế "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" ban hành kèm theo Thông tư số 87/2024/TT-BQP bằng "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" ban hành tại Phụ lục kèm theo Thông tư này.

Điều 2. Ban hành kèm theo Thông tư này 02 sửa đổi quy chuẩn kỹ thuật quốc gia gồm:

1. Sửa đổi 1:2025 QCVN 15:2023/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;

2. Sửa đổi 1:2025 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.

Điều 3. Ban hành kèm theo Thông tư này QCVN 04:2025/BQP Quy chuẩn kỹ thuật quốc gia mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng.

Điều 4. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày … tháng … năm 2025.

2. QCVN 04:2016/BQP Quy chuẩn kỹ thuật quốc gia mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng ban hành kèm theo Thông tư số 161/2016/TT-BQP ngày 21/10/2016 của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng hết hiệu lực kể từ ngày Thông tư này có hiệu lực.

Điều 5. Tổ chức thực hiện

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

2. Trong quá trình thực hiện, nếu phát sinh vướng mắc, cơ quan, tổ chức, cá nhân kịp thời phản ánh bằng văn bản về Ban Cơ yếu Chính phủ (qua Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã) để được hướng dẫn hoặc nghiên cứu sửa đổi, bổ sung cho phù hợp./.

Nơi nhận:
- Thủ tướng, các Phó Thủ tướng Chính phủ (để b/c);
- 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 Tiêu chuẩn - Đo lường - Chất lượng/BTTM;
- Cục Kiểm tra văn bản QPPL Bộ Tư pháp;
- Công báo, Cổng TTĐTCP;
- Vụ Pháp chế/BQP;
- Cổng TTĐTBQP
- Lưu: VT, BCY. BN110.

BỘ TRƯỞNG

Đại tướng Phan Văn Giang

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

(Ban hành kèm theo Thông tư số /2025/TT-BQP ngày tháng năm 2025 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
Tiêu chuẩn về đặc tính kỹ thuật mật mã				
1	Mật mã đối xứng và chế độ hoạt động	TCVN 14263:2024	Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.	- Áp dụng ít nhất một trong hai tiêu chuẩn TCVN 14263:2024, 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 ba thuật toán MKV, AES hoặc TDEA. - Đối với thuật toán MKV: + Sử dụng khóa k có độ dài là 128 bit, 192 bit hoặc 256 bit; + Sử dụng một trong các chế độ: CBC, CFB, OFB, GCM, CCM, CTR. - Đối với thuật toán AES: + Sử dụng khóa có kích thước là 128 bit, 192 bit hoặc 256 bit;
		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.	
		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	Recommendation for Block	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		Publication 800-38E	Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices	+ 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.
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: + 2048 ≤ nlen ≤ 3072 + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký. - Đối với thuật toán ECDSA, ECDH: + 256 ≤ nlen ≤ 384 + Áp dụng ECDH để phân phối khóa và ECDSA để ký. - Đối với thuật toán DSA, DH: + 2048 ≤ L ≤ 3072, 256 ≤ N ≤ 384. + 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)	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
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.
		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

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		NIST SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	sau: Hash_DRBG, HMAC_DRBG, CTR_DRBG(AES), MS_DRBG, MQ_DRBG, XOR-NRBG, Oversampling-NRBG.
		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 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	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
	Generator	
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
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
MKV		Mã khối Việt
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định bậc hai đa biến

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
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 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

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
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

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

DỰ THẢO

SỬA ĐỔI 01:2025 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

Amendment 1:2025 QCVN 12:2022/BQP

National technical regulation on cryptographic technical specification used in civil cryptography products under IP security products group with IPsec and TLS

HÀ NỘI – 2025

Lời nói đầu

SỬA ĐỔI 01:2025 QCVN 12:2022/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số ..... /2025/TT-BQP ngày … tháng ….năm 2025.

Sửa đổi 01:2025 QCVN 12:2022/BQP chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 12:2022/BQP. Các nội dung không được nêu tại Sửa đổi 01:2025 này thì tiếp tục áp dụng QCVN 12:2022/BQP ban hành kèm theo Thông tư số 23/2022/TT-BQP ngày 04/4/2022 của Bộ trưởng Bộ Quốc phòng.

SỬA ĐỔI 01:2025 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

Amendment 1:2025 QCVN 12:2022/BQP National technical regulation on cryptographic technical specification used in civil cryptography products under IP security products group with IPsec and TLS

Bổ sung tại mục *1.3 Tài liệu viện dẫn* tài liệu sau vào phần đầu tiên sau tiêu đề mục 1.3*:*

TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*"

Bổ sung tại mục *1.5 Chữ viết tắt* dòng sau:

Chữ viết tắt	**Tên tiếng anh**	**Tên tiếng việt**
MKV		Mã khối Việt

Bổ sung tại mục *1.6 Ký hiệu* dòng sau:

Ký hiệu	**Mô tả**
k	Khóa của thuật toán mã hóa đối xứng MKV

Thay thế mục 2.2.1.1 như sau:

2.2.1.1 Thuật toán mật mã đối xứng

- Sử dụng thuật toán trong danh sách sau:

STT	**Thuật toán**	**Tham chiếu**
1	MKV	[TCVN 14263:2024], [TCVN 12213]
2	AES	[TCVN 11367-3], [TCVN 12213], [SP 800-38D], [RFC 4309]
3	TDEA	[TCVN 11367-3], [TCVN 12213]
4	Camellia	
5	SEED	
6	CAST	[TCVN 11367-3], [RFC 2612]
7	GOST R 34.12-2015	[TCVN 12213], [RFC 7801]

Thay thế mục 2.2.2.1 như sau:

2.2.2.1 Thuật toán mật mã đối xứng

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
2	AES	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
3	TDEA	192	CBC, CFB, OFB, CTR	2030
4	Camellia	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
5	SEED	128	CBC, CFB, OFB, GCM, CCM, CTR	2027
6	CAST	128	CBC, CFB, OFB, CTR	2027
		256		2030
7	GOST R 34.12-2015	256	CCM, GCM, CBC	2030

Thay thế mục 2.2.2.2 như sau:

2.2.2.2 Thuật toán mật mã phi đối xứng

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
1	RSA	*nlen* = 2048	2027
		2048 < *nlen* ≤ 3072	2030
2	DSA, DH	*L* = 2048, *N* = 256	2027
		2048 < *L* ≤ 3072, *256* < *N* ≤ 384	2030
3	ECDH	256 < nlen ≤ 384	2030
4	ECDSA		

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
5	GOST R 34.10-2001	*256 < nlen ≤ 384*	2030
6	GOST R 34.10-2012		
CHÚ THÍCH: Các tiêu chuẩn cho tham số an toàn, các thuật toán sinh, các bộ tham số cụ thể cho các thuật toán RSA, DSA, ECDSA trong quy chuẩn này áp dụng theo tiêu chuẩn FIPS 186-4. Các bộ tham số cụ thể cho thuật toán GOST R 34.10-2001, GOST R 34.10-2012 trong quy chuẩn này áp dụng theo RFC 5832 và RFC 7091.			

Thay thế thời gian được phép sử dụng tại cột "**Sử dụng đến năm**" trong các bảng tại mục 2.2.2.3 và mục 2.2.2.4 như sau:

Sửa năm "2027" thành năm "2030".

Bổ sung mục 3.4 như sau:

3.4 Chấp nhận kết quả thử nghiệm của tổ chức thử nghiệm trong nước được chỉ định và tổ chức thử nghiệm nước ngoài được công nhận phù hợp với tiêu chuẩn ISO/IEC 17025 theo các yêu cầu kỹ thuật tương ứng trong Quy chuẩn này. 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.

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

DỰ THẢO

SỬA ĐỔI 01:2025 QCVN 15:2023/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

Amendment 1:2025 QCVN 15:2023/BQP
National technical regulation on security of cryptographic used in civil cryptography products belong to data storage security product group

HÀ NỘI – 2025

Lời nói đầu

SỬA ĐỔI 01:2025 QCVN 15:2023/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số ..... /2025/TT-BQP ngày … tháng ….năm 2025.

Sửa đổi 01:2025 QCVN 15:2023/BQP chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 15:2023/BQP. Các nội dung không được nêu tại Sửa đổi 01:2025 này thì tiếp tục áp dụng QCVN 15:2023/BQP ban hành kèm theo Thông tư số 96/2023/TT-BQP ngày 21/11/2023 của Bộ trưởng Bộ Quốc phòng.

SỬA ĐỔI 01:2025 QCVN 15:2023/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

Amendment 1:2025 QCVN 15:2023/BQP National technical regulation on security of cryptographic used in civil cryptography products belong to data storage security product group

Bổ sung tại mục *1.3 Tài liệu viện dẫn* tài liệu sau vào dòng sau tài liệu viện dẫn *QCVN 12:2022/BQP:*

TCVN 14263:2024 “Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV”

Bổ sung tại mục *1.5 Chữ viết tắt* dòng sau:

Chữ viết tắt	**Tên tiếng anh**	**Tên tiếng việt**
MKV		Mã khối Việt

Bổ sung tại mục *1.6 Ký hiệu* dòng sau:

Ký hiệu	**Mô tả**
k	Khóa của thuật toán mã hóa đối xứng MKV

Thay thế Bảng 1 Mục 2.1.1 bằng:

Bảng 1 - Danh mục thuật toán mã hóa đối xứng được phép sử dụng

STT	**Thuật toán**	**Tham chiếu**
1	MKV	[TCVN 14263:2024]
2	TDEA	[TCVN 11367-3], [TCVN 12213], [SP 800-38E], [SP 800-38D]
3	AES	
4	GOST R 34.12-2015	[TCVN 12213], [RFC 7801]

Thay thế Bảng 7 mục 2.2.1 bằng:

Bảng 7 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mã hóa đối xứng

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
2	TDEA	192	CBC	2030
3	AES	128, 192 hoặc 256	XTS, CCM, GCM, CBC, KW, KWP	2030
4	GOST R 34.12-2015	256	CCM, GCM, CBC	2030

Thay thế mục 2.2.2 như sau:

2.2.2 Thuật toán mật mã phi đối xứng

Việc sử dụng thuật toán mật mã phi đối xứng phải tuân thủ các quy định sau:

Bảng 8 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mật mã phi đối xứng

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
1	RSA	*nlen* = 2048	2027
		2048 < *nlen* ≤ 3072	2030
2	DSA, DH	*L* = 2048, *N* = 256	2027
		2048 < *L* ≤ 3072, *256* < *N* ≤ 384	2030
3	ECDH	256 < nlen ≤ 384	2030
4	ECDSA		
5	GOST R 34.10-2001	*256 < nlen ≤ 384*	2030
6	GOST R 34.10-2012		

CHÚ THÍCH:

Các tiêu chuẩn cho tham số an toàn, các thuật toán sinh, các bộ tham số cụ thể cho các thuật toán RSA, DSA, ECDSA trong quy chuẩn này áp dụng theo tiêu chuẩn FIPS 186-4.

Các bộ tham số cụ thể cho thuật toán GOST R 34.10-2001, GOST R 34.10-2012 trong quy chuẩn này áp dụng theo RFC 5832 và RFC 7091.

Thay thế thời gian được phép sử dụng tại cột "**Sử dụng đến năm**" trong các bảng 9 mục 2.2.3, bảng 10 mục 2.2.4, bảng 11 mục 2.2.5 và bảng 12 mục 2.2.6 như sau:

Sửa năm "2027" thành năm "2030".

Thay thế mục 3.4 bằng:

3.4 Chấp nhận kết quả thử nghiệm của tổ chức thử nghiệm trong nước được chỉ định và tổ chức thử nghiệm nước ngoài được công nhận phù hợp với tiêu chuẩn ISO/IEC 17025 theo các yêu cầu kỹ thuật tương ứng trong Quy chuẩn này. 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.

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

DỰ THẢO

QCVN 4:2025/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

HÀ NỘI – 2025

MỤC LỤC

Lời nói đầu

QCVN 4:2025/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số ..... /2025/TT-BQP ngày … tháng …. năm 2025.

QCVN 04:2025/BQP thay thế QCVN 04:2016/BQP Quy chuẩn kỹ thuật quốc gia mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng ban hành kèm theo Thông tư số 161/2016/TT-BQP ngày 21/10/2016 của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

1 QUY ĐỊNH CHUNG

1.1 Phạm vi điều chỉnh

Quy chuẩn kỹ thuật quốc gia này quy định mức giới hạn các đặc tính kỹ thuật mật mã của các thuật tóa mã hóa dữ liệu dùng trong các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

1.2 Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các tổ chức, cá nhân sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự trong lĩnh vực ngân hàng; các tổ chức tín dụng (trừ quỹ tín dụng nhân dân cơ sở có tài sản dưới 10 tỷ đồng, tổ chức tài chính vi mô) sử dụng sản phẩm, dịch vụ mật mã dân sự.

1.3 Tài liệu viện dẫn

TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

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"*.

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"*.

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

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

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.

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.

[RFC7801]: "GOST R 34.12-2015: Block Cipher "Kuznyechik"", Internet Engineering Task Force (IETF), March 2016.

1.4 Giải thích từ ngữ

Trong Quy chuẩn này, các từ ngữ dưới đây được hiểu như sau:

1.4.1. Thông tin không thuộc phạm vi bí mật nhà nước

Là thông tin không thuộc nội dung tin "tuyệt mật", "tối mật" và "mật" được quy định tại Luật bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018.

1.4.2. Mật mã

Là những quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin nhằm bảo đảm bí mật, xác thực, toàn vẹn của nội dung thông tin.

1.4.3. Mật mã dân sự

Là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

1.4.4. Sản phẩm mật mã dân sự

Là các tài liệu, trang thiết bị kỹ thuật và nghiệp vụ mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.4.5. Kỹ thuật mật mã

Là phương pháp, phương tiện có ứng dụng mật mã để bảo vệ thông tin.

1.4.6. Mã hóa

Là quá trình dùng kỹ thuật mật mã để thay đổi hình thức biểu hiện thông tin.

1.4.7. Giải mã

Là phép biến đổi ngược của quá trình mã hóa tương ứng.

1.4.8. Mã khối

Hệ mật đối xứng với tính chất là thuật toán mã hóa thao tác trên một khối của bản rõ, nghĩa là trên một xâu bit có độ dài xác định, kết quả cho ra một khối của bản mã.

1.4.9. Mã dòng

Hệ mật đối xứng với tính chất là thuật toán mã hóa bao gồm tổ hợp một dãy các ký tự của bản rõ với dãy các ký tự của khóa dòng, mỗi lần một ký tự, sử dụng một hàm khả nghịch.

1.4.10. Khóa

Là dãy ký tự điều khiển hoạt động của biến đổi mật mã.

1.4.11. Khóa dòng

Là dãy các ký tự giả ngẫu nhiên bí mật, được sử dụng bởi các thuật toán mã hóa và giải mã của mã dòng.

1.4.11. Mật mã đối xứng

Là mật mã trong đó khóa được sử dụng cho các phép mã hóa, giải mã là trùng nhau hoặc dễ dàng tính toán được khóa mã hóa khi biết khóa giải mã và ngược lại.

1.5 Chữ viết tắt

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 hoạt động 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
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
FIPS PUB	Federal Information Processing Standards Publication	Công bố 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
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm
MKV		Mã khối Việt
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
QCVN		Quy chuẩn quốc gia Việt Nam
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF (Internet Engineering Task Force) công bố
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
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối hẹp

1.6 Ký hiệu

Ký hiệu	Mô tả
k	Khóa của thuật toán mã hóa đối xứng MKV

2 QUY ĐỊNH KĨ THUẬT

Các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng tuân thủ các quy định về thuật tóa mã hóa đối xứng sau:

2.1 Quy định về thuật toán mật mã

Sử dụng thuật toán trong danh sách sau:

Bảng 1 - Danh mục thuật toán mã hóa đối xứng được phép sử dụng

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024], [TCVN 12213]
2	TDEA	[TCVN 11367-3], [TCVN 12213], [SP 800-38E], [SP 800-38D]
3	AES	
4	Camellia	
5	GOST R 34.12-2015	[TCVN 12213], [RFC 7801]

2.2 Quy định về đặc tính kỹ thuật và thời gian sử dụng

Việc sử dụng thuật toán mã hóa đối xứng phải tuân thủ các quy định sau:

Bảng 2 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mã hóa đối xứng

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
2	TDEA	192	CBC	2030
3	AES	128, 192 hoặc 256	XTS, CCM, GCM, CBC, CFB, OFB, KW, KWP	2030
4	Camellia	128, 192 hoặc 256	CBC, CFB, OFB, GCM, CCM, CTR	2030
5	GOST R 34.12-2015	256	CCM, GCM, CBC	2030

2.3 Quy định về an toàn trong sử dụng

- Trong bọc khóa bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: KW, KWP, CCM, GCM, CBC.
- Các khóa mật mã chỉ được sử dụng cho một mục đích, không được phép sử dụng chung khóa để mã hóa khóa và mã hóa dữ liệu.

3 QUY ĐỊNH VỀ QUẢN LÝ

3.1 Các mức giới hạn của đặc tính kỹ thuật mật mã nêu tại Quy chuẩn này là các chỉ tiêu chất lượng phục vụ quản lý theo quy định về quản lý chất lượng sản phẩm mật mã dân sự được quy định tại Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm, khắc phục hậu quả khi bị xử phạt vi phạm hành chính theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật, trong Quy chuẩn này được thực hiện theo phương thức 1; Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012; Nghị định số 126/2021/NĐ-CP ngày ngày 30 tháng 12 năm 2021 của Chính phủ sửa đổi, bổ sung một số điều của các nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực sở hữu công nghiệp; tiêu chuẩn, đo lường và chất lượng sản phẩm, hàng hóa; hoạt động khoa học và công nghệ, chuyển giao công nghệ; năng lượng nguyên tử; Thông tư số 06/2020/TT-BKHCN ngày 10/12/2020 của Bộ Khoa học và Công nghệ quy định chi tiết và biện pháp thi hành một số điều Nghị định số 132/2008/NĐ-CP ngày 31 tháng 12 năm 2008, Nghị định số 74/2018/NĐ-CP ngày 15 tháng 5 năm 2018, Nghị định số 154/2018/NĐ-CP ngày 09 tháng 11 năm 2018 và Nghị định số 119/2017/NĐ-CP ngày 01 tháng 11 năm 2017 của Chính phủ và các văn bản quy phạm pháp luật có liên quan. Quản lý công bố hợp quy dựa trên kết quả chứng nhận của tổ chức chứng nhận được chỉ định theo quy định của pháp luật.

3.3 Dấu hợp quy được sử dụng trực tiếp trên sản phẩm hoặc trên bao gói hoặc trên nhãn gắn trên sản phẩm hoặc trong chứng chỉ chất lượng, tài liệu kỹ thuật của sản phẩm.

3.4 Chấp nhận kết quả thử nghiệm của tổ chức thử nghiệm trong nước được chỉ định và tổ chức thử nghiệm nước ngoài được công nhận phù hợp với tiêu chuẩn ISO/IEC 17025 theo các yêu cầu kỹ thuật tương ứng trong Quy chuẩn này. 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.

3.5 Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã - Ban Cơ yếu Chính phủ là cơ quan tiếp nhận công bố hợp quy, kiểm tra nhà nước về chất lượng sản phẩm mật mã dân sự.

4 TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Các tổ chức, cá nhân có hoạt động sản xuất, kinh doanh sản phẩm mật mã dân sự thuộc phạm vi điều chỉnh của quy chuẩn này có trách nhiệm thực hiện các quy định về chứng nhận, công bố hợp quy và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định hiện hành.

5 TỔ CHỨC THỰC HIỆN

5.1 Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng rà soát, sửa đổi, bổ sung hoặc ban hành thay thế Quy chuẩn này để đảm bảo phù hợp với thực tiễn và đáp ứng yêu cầu quản lý.

5.2 Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã - Ban Cơ yếu Chính phủ có trách nhiệm hướng dẫn, tổ chức triển khai quản lý kỹ thuật mật mã theo Quy chuẩn này.

5.3 Thanh tra, kiểm tra sản phẩm mật mã dân sự được cơ quan quản lý nhà nước có thẩm quyền tiến hành định kỳ hàng năm hoặc đột xuất./.

TÀI LIỆU THAM KHẢO

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

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

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

[4]. 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.

[5]. National Institute of Standards and Technology, Special Publication 800-38F*, "Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping"*, December 2012.