BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 96 /2023/TT-BQP	*Hà Nội, ngày 29 tháng 11 năm 2023*

THÔNG TƯ

Ban hành "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"

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;

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 quy định 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.

Điều 1. Ban hành kèm theo Thông tư này 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.

Ký hiệu: QCVN 15:2023/BQP.

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 01 năm 2024

Điều 3. 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./.

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 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.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Nguyễn Tân Cương

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

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

National technical regulation on security of cryptographic used in civil cryptography products belong to data storage security product group

HÀ NỘI – 2023

MỤC LỤC

Lời nói đầu

QCVN 15:2023/BQP do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã – 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 ..... /2023/TT-BQP ngày ... tháng ....năm 2023.

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

National technical regulation on security of cryptographic used in civil cryptography products belong to data storage security product group

1 QUY ĐỊNH CHUNG

1.1 Phạm vi điều chỉnh

Quy chuẩn này quy định mức giới hạn các đặc tính kỹ thuật mật mã của các sản phẩm bảo mật dữ liệu lưu giữ phục vụ bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

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 để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.3 Tài liệu viện dẫn

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*".

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 12853:2020 (ISO/IEC 18031:2011 With amendment 1:2017) "*Công nghệ thông tin - Các kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên*".

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*".

ISO/IEC 27040:2015 "*Information technology – Security techniques – Storage security*".

National Institute of Standards and Technology, FIPS 186-4 "*Digital Signature Standard (DSS)*", July 2013.

National Institute of Standards and Technology, FIPS 180-4 "*Secure Hash Standard (SHS)*", August 2015.

National Institute of Standards and Technology, FIPS 202 *"SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions"*, August 2015.

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.

Internet Engineering Task Force, *"IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices"*, October 2018.

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

[RFC 5832]: *"GOST R 34.10-2001: Digital Signature Algorithm"*, Internet Engineering Task Force (IETF), March 2010.

[RFC 7091]: *"GOST R 34.10-2012: Digital Signature Algorithm"*, Internet Engineering Task Force (IETF), December 2013.

[RFC 4868]: *"Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec"*, Internet Engineering Task Force (IETF), May 2007.

[RFC 9106]: *"Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications"*, Internet Engineering Task Force (IETF), September 2021.

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. Sản phẩm bảo mật dữ liệu lưu giữ

Là sản phẩm mật mã dân sự sử dụng các thuật toán mật mã, kỹ thuật mật mã để bảo vệ dữ liệu lưu giữ trên thiết bị.

1.4.6. Dữ liệu lưu giữ

Dữ liệu (thông tin) được lưu giữ (ghi) trong một phương tiện lưu trữ.

1.4.7. Kỹ thuật mật mã

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

1.4.8. Mã hóa

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

1.4.9. Giải mã

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

1.4.10. Khóa

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

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.

1.4.12. Mật mã phi đối xứng

Là mật mã trong đó khóa được sử dụng cho phép mã hóa hoặc giải mã gồm hai thành phần là khóa công khai và khóa riêng với đặc tính có thể dễ dàng tính toán được khóa công khai nếu biết khóa riêng nhưng không khả thi về mặt tính toán để tính được khóa riêng từ khóa công khai.

1.4.13. Thuật toán băm

Là thuật toán thực hiện quá trình biến đổi chuỗi dữ liệu đầu vào có độ dài bất kỳ thành một chuỗi dữ liệu đầu ra đặc trưng có độ dài cố định.

1.4.14. Thuật toán xác thực thông điệp

Là thuật toán biến đổi các chuỗi dữ liệu đầu vào và khóa bí mật thành các chuỗi dữ liệu đầu ra có độ dài cố định thỏa mãn các tính chất sau đây:

- Dễ dàng tính toán với bất kỳ khóa và chuỗi dữ liệu đầu vào nào;

- Với khóa cố định bất kỳ và không biết trước khóa, bằng tính toán không thể tính được giá trị chuỗi dữ liệu đầu ra với bất kỳ chuỗi dữ liệu đầu vào mới nào.

1.4.15. Mã HS

Là mã phân loại của hàng hóa, dùng để xác định thuế suất xuất nhập khẩu hàng hóa và các nghĩa vụ khác.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
Argon2	Tên gọi một hàm dẫn xuất khóa được thiết kế bởi Alex Biryukov, Daniel Dinu và Dmitry Khovratovich.	
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
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
EC	Elliptic Curve	Đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
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
Hash_DRBG	Hash Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên hàm băm
HDD	Hard Disk Drive	Ổ đĩa cứng
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
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
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

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 Việt Nam
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

1.6 Ký hiệu

Ký hiệu	Mô tả
nlen	Đối với thuật toán RSA: *nlen* là độ dài modulo theo bit; Đối với thuật toán ECDSA, GOST R 34.10-2012, GOST R 34.10-2001: *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

2 QUY ĐỊNH KĨ THUẬT

Các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ phải tuân thủ các quy định an toàn sau:

2.1 Quy định về thuật toán mật mã

2.1.1 Thuật toán mã hóa đối xứng

– 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	TDEA	[TCVN 11367-3], [TCVN 12213], [SP 800-38E], [SP 800-38D]
2	AES	
3	GOST R 34.12-2015	[TCVN 12213], [RFC 7801]

2.1.2 Thuật toán mật mã phi đối xứng

– Sử dụng thuật toán trong danh sách sau:

Bảng 2 - Danh mục thuật toán mật mã phi đối xứng được phép sử dụng

STT	Thuật toán	Tham chiếu
1	RSA	[FIPS 186-4], [SP 800-56B Rev. 2]
2	DSA	[FIPS 186-4]
3	ECDSA	
4	GOST R34.10-2001	[RFC 5832]
5	GOST R34.10-2012	[RFC7091]

2.1.3 Thuật toán băm

– Sử dụng thuật toán trong danh sách sau:

Bảng 3 - Danh mục thuật toán băm được phép sử dụng

STT	Thuật toán	Tham chiếu
1	SHA-256, SHA-384, SHA-512/256, SHA-512	[TCVN 11816-3], [FIPS 180-4]
2	SHA3-256, SHA3-384, SHA3-512	[FIPS 202]

2.1.4 Thuật toán xác thực thông điệp

– Sử dụng thuật toán trong danh sách sau:

Bảng 4 - Danh mục thuật toán xác thực thông điệp được phép sử dụng

STT	Thuật toán	Tham chiếu
1	HMAC_SHA_256_128	[RFC 4868]
2	HMAC_SHA_256	
3	HMAC_SHA_384_192	
4	HMAC_SHA_384	
5	HMAC_SHA_512_256	
6	HMAC_SHA_512	
7	HMAC_SHA3_256	[FIPS 198-1], [FIPS 202]
8	HMAC_SHA3_384	
9	HMAC_SHA3_512	

2.1.5 Hàm dẫn xuất khóa

– Sử dụng hàm dẫn xuất khóa trong danh sách sau:

Bảng 5 - Danh mục hàm dẫn xuất khóa được phép sử dụng

STT	Thuật toán	Tham chiếu
1	PBKDF2	[SP 800-132]
2	Argon2	RFC 9106

2.1.6 Bộ tạo số ngẫu nhiên

– Sử dụng bộ tạo số ngẫu nhiên trong danh sách sau:

Bảng 6 - Danh mục bộ tạo số ngẫu nhiên được phép sử dụng

STT	Thuật toán	Tham chiếu
1	Hash_DRBG	[TCVN 12853]
2	HMAC_DRBG	
3	CTR_DRBG(AES)	
4	XOR-NRBG	[SP 800-90C]
5	Oversampling-NRBG	

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

2.2.1 Thuật toán mã hóa đối xứng

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

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	TDEA	192	CBC	2025
2	AES	≥ 128	XTS, CCM, GCM, CBC, KW, KWP	2027
3	GOST R 34.12-2015	256	CCM, GCM, CBC	2027

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	2025
		nlen ≥ 3072	2027

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

2	DSA	$L = 2048$, $N = 256$	2025
		$L \geq 3072$, $N \geq 256$	2027
3	ECDSA	*nlen* ≥ 256	2027
4	GOST R 34.10-2012	*nlen* ≥ 256	2027
5	GOST R 34.10-2001		
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.			

2.2.3 Thuật toán băm

Việc sử dụng thuật toán băm phải tuân thủ các quy định sau:

Bảng 9 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán băm

STT	Thuật toán	Sử dụng đến năm
1	SHA-256, SHA-384, SHA-512/256, SHA-512	2027
2	SHA3-256, SHA3-384, SHA3-512	2027

2.2.4 Thuật toán xác thực thông điệp

Việc sử dụng thuật toán xác thực thông điệp phải tuân thủ các quy định sau:

Bảng 10 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán xác thực thông điệp

STT	Thuật toán	Sử dụng đến năm
1	HMAC_SHA_256_128	2027
2	HMAC_SHA_256	2027

Bảng 10 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán xác thực thông điệp (tiếp)

3	HMAC_SHA_384_192	2027
4	HMAC_SHA_384	2027
5	HMAC_SHA_512_256	2027
6	HMAC_SHA_512	2027
7	HMAC_SHA3_256_128	2027
8	HMAC_SHA3_256	2027
9	HMAC_SHA3_384_192	2027
10	HMAC_SHA3_384	2027
11	HMAC_SHA3_512_256	2027
12	HMAC_SHA3_512	2027

2.2.5 Hàm dẫn xuất khóa

Việc sử dụng hàm dẫn xuất khóa phải tuân thủ các quy định sau:

Bảng 11 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với hàm dẫn xuất khóa

STT	Thuật toán	Sử dụng đến năm
1	PBKDF2	2027
2	Argon2	2027

2.2.6 Bộ tạo số ngẫu nhiên

Việc sử dụng bộ tạo số ngẫu nhiên phải tuân thủ các quy định sau:

Bảng 12 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với bộ tạo số ngẫu nhiên

STT	Thuật toán	Sử dụng đến năm
1	Hash_DRBG	2027
2	HMAC_DRBG	2027
3	CTR_DRBG(AES)	2027
4	XOR-NRBG	2027
5	Oversampling-NRBG	2027

2.3 Quy định về an toàn trong sử dụng

- Trong mã hóa/giải mã dữ liệu bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: XTS, CCM, GCM, CBC.
- 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.
- Đối với dữ liệu lưu giữ dài hạn phải sử dụng các chế độ sau:
  + Chế độ XTS cho lưu giữ bằng ổ đĩa cứng (HDD).
  + Chế độ CCM, GCM cho lưu giữ bằng băng từ hoặc bộ nhớ flash.
  + Trong trường hợp các chế độ trên không khả dụng thì được phép sử dụng chế độ CBC.
- Đối với thuật toán RSA, chỉ được phép sử dụng lược đồ KTS-OAEP và KTS-KEM-KWS cho vận chuyển khóa.
- Trong mã hóa dữ liệu được truyền tải, áp dụng hai giao thức IPSec và TLS (phiên bản TLS 1.2 và TLS 1.3) để cung cấp khả năng bảo vệ bổ sung (nếu có).

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.

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./.

PHỤ LỤC

(Quy định)

Quy định về mã HS của sản phẩm bảo mật dữ liệu lưu giữ

STT	Tên sản phẩm, hàng hóa theo QCVN	Mã HS	Mô tả sản phẩm hàng hóa
01	Sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	8471.30.90	Sản phẩm có chức năng mã hóa dữ liệu lưu giữ
02		8471.41.90	
03		8471.49.90	
04		8471.50.90	
05		8471.70.20	
06		8471.70.99	
07		8517.69.00	
08		8517.70.29	
09		8517.70.39	
10		8517.70.99	
11		8523.51.11	
12		8523.51.19	
13		8523.51.21	
14		8523.51.29	
15		8523.51.30	
16		8523.51.91	
17		8523.51.92	
18		8523.51.99	
19		8523.52.00	
20		8542.31.00	

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 800-56B Revision 2 *"Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography"*, March 2019.

[5]. National Institute of Standards and Technology, Special Publication 800-90A *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*, June 2015.

[6]. 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.

[7]. 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.

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

[9]. National Institute of Standards and Technology, Special Publication 800-90C (Second Draft) *"Recommendation for Random Bit Generator (RBG) Constructions"*, April 2016.

[10]. Storage Networking Industry Association (SNIA), "*TLS Specification for Storage Systems Version 1.0*", December 2013.