BỘ QUỐC PHÒNG	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 23 /2022/TT-BQP	*Hà Nội, ngày 04 tháng 4 năm 2022*

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 luồng IP sử dụng công nghệ IPsec và TLS"

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 164/2017/NĐ-CP ngày 30 tháng 12 năm 2017 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 luồng IP sử dụng công nghệ IPsec và TLS.

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 luồng IP sử dụng công nghệ IPsec và TLS.

Ký hiệu: QCVN 01 :2022/BQP.

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày 20 tháng 5 năm 2022.

Điều 3. 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./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Nguyễn Tân Cương

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 01 :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

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

HÀ NỘI – 2022

MỤC LỤC

Lời nói đầu .....
1 QUY ĐỊNH CHUNG .....
1.1 Phạm vi điều chỉnh .....
1.2 Đối tượng áp dụng .....
1.3 Tài liệu viện dẫn .....
1.4 Giải thích từ ngữ .....
1.5 Chữ viết tắt .....
1.6 Ký hiệu .....
2 QUY ĐỊNH KỸ THUẬT .....
2.1 Quy định chung .....
2.2 Quy định về đặc tính kỹ thuật mật mã .....
2.2.1 Quy định về thuật toán mật mã .....
2.2.2 Quy định về an toàn, thời gian sử dụng .....
2.3 Quy định về an toàn sử dụng trong giao thức .....
2.3.1 Quy định về an toàn sử dụng trong giao thức IPsec .....
2.3.2 Quy định về an toàn sử dụng trong giao thức TLS .....
3 QUY ĐỊNH VỀ QUẢN LÝ .....
4 TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN .....
5 TỔ CHỨC THỰC HIỆN .....
PHỤ LỤC A .....
TÀI LIỆU THAM KHẢO .....

QCVN 01 :2022/BQP

Lời nói đầu

QCVN 01 :2022/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 kèm theo Thông tư số 23. /2022/TT-BQP ngày 04. tháng 4. năm 2022.

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

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

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 luồng IP sử dụng công nghệ IPsec và TLS 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 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

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*".

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 198-1 "*The Keyed-Hash Message Authentication Code (HMAC)*", July 2008.

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

[RFC 4309]: *"Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)"*, Internet Engineering Task Force (IETF), December 2005.

[RFC 2612]: *"The CAST-256 Encryption Algorithm"*, Internet Engineering Task Force (IETF), June 1999.

[RFC 7801]: *"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 3566]: *"The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec"*, Internet Engineering Task Force (IETF), September 2003.

[RFC 4494]: *"The AES-CMAC-96 Algorithm and Its Use with IPsec"*, Internet Engineering Task Force (IETF), June 2006.

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

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 luồng IP

Là sản phẩm mật mã sử dụng các kỹ thuật, công nghệ mật mã để đảm bảo an toàn, bảo mật cho dữ liệu truyền, nhận trên môi trường mạng IP.

1.4.6 Kỹ thuật mật mã

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

1.4.7 Mã hóa

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

1.4.8 Giải mã

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

1.4.9 Khóa

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

1.4.10 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.

1.4.11 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.

1.4.12 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.

1.4.13 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.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
AH	Authentication Header	Xác thực thông tin điều khiển gói IP
CAST	Carlisle Adams - Stafford Tavares	Tên của hệ mã do hai nhà toán học Carlisle Adams và Stafford Tavares phát minh
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
DH	Diffie-Hellman	Thuật toán trao đổi khóa Diffie-Hellman
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
ESP	Encapsulating Security Payload	Đóng gói an toàn dữ liệu
FIPS	Federal Information Processing Standards	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
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
IKE	Internet Key Exchange	Giao thức trao đổi khóa trên Internet
IP	Internet Protocol	Giao thức Internet
IPsec	Internet Protocol Security	Giao thức bảo mật mạng IP
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 Công nghệ 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
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
TLS	Transport Layer Security	Bảo mật tầng giao vận
VPN	Virtual Private Network	Mạng riêng ảo

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 ECDH, 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, 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

2 QUY ĐỊNH KỸ THUẬT

2.1 Quy định chung

- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ IPsec VPN được phép sử dụng giao thức trao đổi khóa IKEv1 và IKEv2, giao thức đóng gói ESP.

- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ TLS VPN được phép sử dụng giao thức TLS 1.2 và TLS 1.3.

2.2 Quy định về đặc tính kỹ thuật mật mã

2.2.1 Quy định về thuật toán mật mã

Các sản phẩm mật mã dân sự sử dụng công nghệ IPsec VPN, TLS VPN yêu cầu đáp ứng các quy định 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	AES	[TCVN 11367-3], [TCVN 12213], [SP 800-38D], [RFC 4309]
2	TDEA	[TCVN 11367-3], [TCVN 12213]
3	Camellia	
4	SEED	
5	CAST	[TCVN 11367-3], [RFC 2612]
6	GOST R 34.12-2015	[TCVN 12213], [RFC 7801]

2.2.1.2 Thuật toán mật mã phi đối xứng

- Sử dụng thuật toán trong danh sách sau:

STT	Thuật toán	Tham chiếu
1	RSA	[FIPS 186-4], [SP 800-56B Rev. 2]
2	DSA	[FIPS 186-4]
3	ECDSA	

4	DH	[FIPS 186-4], [SP 800-56A Rev. 3]
5	ECDH	
6	GOST R 34.10-2001	[RFC 5832]
7	GOST R 34.10-2012	[RFC7091]

2.2.1.3 Thuật toán băm

- Sử dụng thuật toán trong danh sách sau:

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]

2.2.1.4 Thuật toán xác thực thông điệp

- Sử dụng thuật toán trong danh sách sau:

STT	Thuật toán	Tham chiếu
1	AES-XCBC-96	[RFC 3566]
2	AES-CMAC-96	[RFC 4494]
3	HMAC-SHA-256-128	[RFC 4868]
4	HMAC-SHA-256	
5	HMAC-SHA-384-192	
6	HMAC-SHA-384	
7	HMAC-SHA-512-256	
8	HMAC-SHA-512	
9	HMAC-SHA3-256	[FIPS 198-1] [FIPS 202]
10	HMAC-SHA3-384	
11	HMAC-SHA3-512	

2.2.1.5 Bộ tạo số ngẫu nhiên

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

STT	Thuật toán	Tham chiếu
1	Hash_DRBG	[TCVN 12853]
2	HMAC_DRBG	
3	CTR_DRBG	
4	OFB_DRBG	
5	MS_DRBG	
6	MQ_DRBG	
7	XOR – NRBG	[SP 800-90C]
8	Oversampling-NRBG Construction	

2.2.2 Quy định về an toàn, thời gian sử dụng

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	AES	≥ 128	CBC, CFB, OFB, GCM, CCM, CTR	2027
2	TDEA	192	CBC, CFB, OFB, CTR	2025
3	Camellia	≥ 128	CBC, CFB, OFB, GCM, CCM, CTR	2027
4	SEED	≥ 128	CBC, CFB, OFB, GCM, CCM, CTR	2027
5	CAST	≥ 128	CBC, CFB, OFB, CTR	2027
6	GOST R 34.12-2015	256	CTR, CFB	2027

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

2.2.2.3 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

2.2.2.4 Thuật toán xác thực thông điệp

STT	Thuật toán	Sử dụng đến năm
1	AES-XCBC-96	2027
2	AES-CMAC-96	2027

3	HMAC-SHA-256-128	2027
4	HMAC-SHA-256	2027
5	HMAC-SHA-384-192	2027
6	HMAC-SHA-384	2027
7	HMAC-SHA-512-256	2027
8	HMAC-SHA-512	2027
9	HMAC-SHA3-256	2027
10	HMAC-SHA3-384	2027
11	HMAC-SHA3-512	2027

2.3 Quy định về an toàn sử dụng trong giao thức

2.3.1 Quy định về an toàn sử dụng trong giao thức IPsec

- Không được phép sử dụng chế độ Aggressive trong giao thức IKEv1, giao thức IKEv1 được phép sử dụng đến năm 2025.
- Không được phép sử dụng giao thức AH.
- Không được phép sử dụng giao thức ESP chỉ có cơ chế xác thực dữ liệu.
- Sử dụng giải pháp bảo vệ khóa được lưu trữ dạng tệp trên thiết bị (nếu có).

2.3.2 Quy định về an toàn sử dụng trong giao thức TLS

- Không được phép trao đổi khóa dựa trên thuật toán Diffie-Hellman sử dụng khóa cố định (Static Diffie-Hellman).
- Không được phép cài đặt các mở rộng cho phép sử dụng những phiên bản trước TLS 1.2 trên máy chủ TLS.
- Sử dụng định dạng chứng thư số X.509 v3 cho TLS (nếu có).
- Sử dụng giải pháp bảo vệ khóa được lưu trữ dạng tệp trên thiết bị (nếu có).
- Không được phép sử dụng phần mở rộng Heartbeat.
- Yêu cầu bổ sung đối với phiên bản TLS 1.3:
  + Không được phép sử dụng chế độ CBC trong mã hóa đối xứng.
  + Không được phép sử dụng chế độ MAC-then-Encrypt (Non-AHEAD Ciphers).
  + Không được phép trao đổi khóa sử dụng thuật toán RSA.
  + Không được phép sử dụng lược đồ ký số/ xác thực RSASSA-PKCS1-v1_5.

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, Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012, Thông tư số 06/2020/TT-BKHCN ngày 10/12/2020. 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 Hoạt động kiểm tra, đánh giá chất lượng 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.

4 TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Các tổ chức, cá nhân có hoạt động 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

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.

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

PHỤ LỤC A

(Quy định)

Quy định về mã HS của sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS

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 luồng IP và bảo mật kênh.	8471.30.90	Sản phẩm sử dụng công nghệ IPsec VPN hoặc TLS VPN để đảm bảo an toàn, bảo mật cho dữ liệu truyền nhận trên môi trường mạng IP.
02		8471.41.90	
03		8471.49.90	
04		8471.80.90	
05		8517.62.10	
06		8517.62.21	
07		8517.62.29	
08		8517.62.30	
09		8517.62.41	
10		8517.62.42	
11		8517.62.49	
12		8517.62.51	
13		8517.62.52	
14		8517.62.53	
15		8517.62.59	
16		8517.62.61	
17		8517.62.69	
18		8517.62.91	
19		8517.62.92	
20		8517.62.99	

21		8525.50.00	
22		8525.60.00	
23		8528.71.11	
24		8528.71.19	
25		8528.71.91	
26		8528.71.99	

TÀI LIỆU THAM KHẢO

1. National Institute of Standards and Technology, "*Guide to IPsec VPNs*", June 2020.
2. National Institute of Standards and Technology, *"Guide to SSL VPNs"*, July 2008.
3. National Institute of Standards and Technology, *"Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"*, August 2019.
4. Federal Office for Information Security, Technical Guideline TR-02102-2 *"Cryptographic Mechanisms: Recommendations and Key Lengths"*, 2021.
5. Federal Office for Information Security, Technical Guideline TR-02102-3 *"Cryptographic Mechanisms: Recommendations and KeyLengths"*, 2021.
6. National Institute of Standards and Technology, Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths"*, March 2019.
7. National Institute of Standards and Technology, Special Publication 800-90A *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*, June 2015.
8. National Institute of Standards and Technology, Special Publication 800-90C (Second Draft) *"Recommendation for Random Bit Generator (RBG) Constructions"*, April 2016.
9. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General"*, May 2020.
10. National Institute of Standards and Technology, Special Publication 800-203 *"2017 NIST/ITL Cybersecurity Program Annual Report"*, July 2018.
11. National Institute of Standards and Technology, Special Publication 800-56A *"Recommendation for Pair-Wise Key Establishment Schemes UsingDiscrete Logarithm Cryptography"*, May 2013.
12. National Institute of Standards and Technology, Special Publication 800-56B Revision 2 *"Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography"*, March 2019.
13. 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.
14. RSA Laboratories, "*PKCS#1 v2.1: RSA Cryptography Standard*", June 2002.
15. [RFC 8247]: "*Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*", Internet Engineering Task Force (IETF), September 2017.

16. [RFC 7427]: "*Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*", Internet Engineering Task Force (IETF), January 2015.
17. [RFC 4754]: "*IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*", Internet Engineering Task Force (IETF), January 2007.
18. [RFC 8446]: "*The Transport Layer Security (TLS) Protocol Version 1.3*", Internet Engineering Task Force (IETF), August 2018.
19. [RFC 8422]: "*Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*", Internet Engineering Task Force (IETF), August 2018.
20. [RFC 8734]: "*Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS) Version 1.3*", Internet Engineering Task Force (IETF), February 2020.
21. National Institute of Standards and Technology, Information Technology Laboratory "*National Vulnerability Database*". https://nvd.nist.gov/vuln/search.