DỰ THẢO

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN XXXX:2021/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ YÊU CẦU 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 requirements used in civil cryptography products under IP security products group with IPsec an TLS

HÀ NỘI – 2021

MỤC LỤC

Lời nói đầu

QCVN XXXX:2021/BQP do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã – Ban Cơ yếu Chính phủ biên soạn, Bộ Khoa học và Công nghệ thẩm định, Ban Cơ yếu Chính phủ trình duyệt và được ban hành theo Quyết định số /2021/QĐ-BQP ngày tháng năm 2021 của Bộ trưởng Bộ Quốc phòng.

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 sản phẩm bảo mật luồng IP sử dụng công nghệ TLS VPN, IPSec VPN 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. Giải thích từ ngữ

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

1.3.1. "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.

1.3.2. "Mật mã" là 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.

1.3.3. "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.

1.3.4. "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.

1.3.5. "Sản phẩm bảo mật luồng IP" là sản phẩm mật mã dân sự sử dụng các thuật toán mật mã, kỹ thuật mật mã để tạo kênh truyền bảo mật giữa hai đầu trên môi trường mạng IP.

1.3.6. "Kỹ thuật mật mã" là phương pháp, phương tiện có ứng dụng mật mã để bảo vệ thông tin.

1.3.7. "Mã hóa" là phép biến đổi khả nghịch dữ liệu bởi thuật toán mật mã để tạo ra bản mã, nhằm mục đích che giấu nội dung thông tin của dữ liệu.

1.3.8. "Giải mã" là phép toán ngược với phép mã hóa tương ứng

1.3.9. "Mã khối" là thuật toán mã hóa thao tác trên khối bản rõ, nghĩa là trên xâu bít có độ dài xác định, kết quả cho ra khối bản mã.

1.3.10. "Khóa" là dãy các ký tự sử dụng trong một phép biến đổi mật mã (ví dụ phép mã hóa, giải mã).

1.3.11. "Chữ ký số" là một chuỗi số, kết quả của phép biến đổi mật mã trên thông điệp dữ liệu nhằm cung cấp một phương tiện để kiểm tra tính xác thực của nguồn gốc thông điệp dữ liệu, tính toàn vẹn của dữ liệu và tính không thể chối bỏ của người đã ký.

1.3.12. Chữ viết tắt

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CAST	Carlisle Adams - Stafford Tavares	Tên của hệ mã do ba nhà toán học phát minh Carlisle Adams và Stafford Tavares
CBC	Cipher Block Chaining Mode	Chế độ hoạt động móc xích khối mã
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 bít ngẫu nhiên tất định dựa trên bộ đếm
DH	Diffie-Hellman	Giao thức thỏa thuận khóa Diffie-Hellman
DRBG	Deterministic Random Bit Generator	Bộ tạo bít 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
GOST	Russian National Standard	Tiêu chuẩn Quốc gia Liên bang Nga
Hash_DRBG	Hash Deterministic Random Bit Generator	Bộ tạo bít 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 bít ngẫu nhiên tất định dựa trên HMAC
IKE	Internet Key Exchange	Giao thức trao đổi khóa
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
NRBG	Non-deterministic Random Bit Generator	Bộ tạo bít ngẫu nhiên bất định
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
PRF	Pseudo Random Function	Hàm giả ngẫu nhiên

RFC	Request for Comments	Đề nghị duyệt thảo và bình luận
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
TDES	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

1.3.13. Giải thích tham số

Chữ viết tắt	**Tên tiếng anh**	**Tên tiếng việt**
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CAST	Carlisle Adams - Stafford Tavares	Tên của hệ mã do ba nhà toán học phát minh Carlisle Adams và Stafford Tavares
CBC	Cipher Block Chaining Mode	Chế độ hoạt động móc xích khối mã
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 bít ngẫu nhiên tất định dựa trên bộ đếm
DH	Diffie-Hellman	Giao thức thỏa thuận khóa Diffie-Hellman
DRBG	Deterministic Random Bit Generator	Bộ tạo bít 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
GOST	Russian National Standard	Tiêu chuẩn Quốc gia Liên bang Nga
Hash_DRBG	Hash Deterministic Random Bit Generator	Bộ tạo bít 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 bít ngẫu nhiên tất định dựa trên HMAC
IKE	Internet Key Exchange	Giao thức trao đổi khóa
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 bít ngẫu nhiên bất định
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
PRF	Pseudo Random Function	Hàm giả ngẫu nhiên
RFC	Request for Comments	Đề nghị duyệt thảo và bình luận
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
TCVN		Tiêu chuẩn quốc gia Việt Nam
TDES	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

2. QUY ĐỊNH KỸ THUẬT

2.1. Yêu cầu kỹ thuật sản phẩm sử dụng công nghệ IPsec VPN

2.1.1. Yêu cầu về sử dụng giao thức và thuật toán mật mã

- Sử dụng một trong các giao thức xác thực và trao đổi khóa sau:

STT	Giao thức xác thực và trao đổi khóa
1	IKEv1
2	IKEv2

- Sử dụng một trong các thuật toán mã khối sau:

STT	Thuật toán mã khối
1	AES
2	TDEA
3	Camellia
4	CAST
5	SEED
6	GOST R 34.12-2015

- Sử dụng một trong các thuật toán ký số sau:

STT	Thuật toán ký số
1	RSASSA-PSS
2	DSA
3	ECDSA
4	GOST R34.10-2001
5	GOST R34.10-2012

- Sử dụng một trong các thuật toán trao đổi khóa sau:

STT	Thuật toán
1	DH

2	ECDH

- Sử dụng một trong các thuật toán hàm băm sau:

STT	Thuật toán
1	SHA-256, SHA-512/256, SHA3-256
2	SHA-384, SHA3-384
3	SHA-512, SHA3-512

- Sử dụng một trong các thuật toán mã xác thực thông báo sau:

STT	Thuật toán
1	HMAC_SHA1_96
2	AES_XCBC_96
3	AES_CMAC_96
4	HMAC_SHA_256_128
5	HMAC_SHA_256
6	HMAC_SHA_384_192
7	HMAC_SHA_384
8	HMAC_SHA_512_256
9	HMAC_SHA_512
10	HMAC_SHA3_256_128
11	HMAC_SHA3_256
12	HMAC_SHA3_384_192
13	HMAC_SHA3_384
14	HMAC_SHA3_512_256
15	HMAC_SHA3_512

- Sử dụng một trong các thuật toán mật mã dùng trong hàm giả ngẫu nhiên (PRF) sau:

STT	Thuật toán
1	AES128_XCBC
2	AES128_CMAC
3	HMAC_SHA1
4	HMAC_SHA_256
5	HMAC_SHA_384
6	HMAC_SHA_512
7	HMAC_SHA3_256
8	HMAC_SHA3_384
9	HMAC_SHA3_512

- Sử dụng một trong các bộ tạo số ngẫu nhiên sau:

STT	Thuật toán
1	Hash_DRBG
2	HMAC_DRBG
3	CTR_DRBG
4	OFB_DRBG
5	MS_DRBG
6	MQ_DRBG
7	XOR – NRBG
8	Oversampling-NRBG Construction

2.1.2. Yêu cầu về an toàn giao thức và tham số mật mã

- Yêu cầu về thời gian sử dụng và chế độ hoạt động của giao thức xác thực và trao đổi khóa như sau:

STT	Xác thực và trao đổi khóa	Chế độ hoạt động	Sử dụng đến năm

1	IKEv1	Main Mode và Aggressive Mode	2025
2	IKEv2	Main Mode, Aggressive Mode và Quick Mode	2027

- Yêu cầu an toàn tham số mật mã đối với thuật toán mã khối như sau:

STT	Thuật toán	Chế độ hoạt động của mã khối	Kích thước khóa theo bít	Sử dụng đến năm	Tham chiếu
1	AES	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥ 128	2027	[TCVN 11367-3], [TCVN 12213], [SP 800-38D], [RFC2612], [RFC4309], [RFC8247]
2	TDEA	CBC, CFB, OFB hoặc CTR	192	2027	
3	Camellia	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥ 128	2027	
4	CAST	CBC, CFB, OFB hoặc CTR	≥ 128	2027	
5	SEED	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥ 128	2027	
6	GOST R 34.12-2015	CTR, CFB	256	2027	[RFC7801]

- Yêu cầu an toàn tham số mật mã đối với thuật toán ký số như sau:

STT	Thuật toán	Độ dài tham số theo bít	Sử dụng đến năm	Tham chiếu
1	RSASSA-PSS	*nlen* = 2048	2025	[TCVN 12214-2], [FIPS PUB 186-4], [SP 800-131A]
2		*nlen* ≥ 3072	2027	
3	DSA	*L* = 2048, *N* = 224	2025	[TCVN 12214-3],

Comment [Ma1]: Cho thuật toán AES, 3DES, Camelia

Comment [Ma2]: Các chế độ hoạt động ECB, CBC, CTR, OFB, CFB

Comment [Ma3]: Cho thuật toán CAST

Comment [Ma4]: Chế độ CCM

Comment [Ma5]: Các thuật toán sử dụng trong ipsec

Comment [Ma6]: Thuật toán GOST R34

Comment [Ma7]: Cơ chế phân tích số nguyên

Comment [Ma8]: ECDSA, DSA, RSA

Comment [Ma9]: Khuyến nghị về sử dụng kh

Comment [Ma10]: DSA và ECDSA

4		$L = 2048, N = 256$	2025	[FIPS PUB 186-4], [SP 800-131A]
5		$L \geq 3072, N \geq 256$	2027	
6	ECDSA	$n \geq 256$	2027	
7	GOST R34.10-2001	$q = 256$	2027	[RFC7091]
8	GOST R34.10-2012	$256 \leq q \leq 512$	2027	

Comment [Ma11]: ECDSA, DSA

Comment [Ma12]: Khuyến nghị về sử dụng khóa

Comment [Ma13]: Thuật toán GOST

- Yêu cầu an toàn tham số mật mã đối với thuật toán trao đổi khóa như sau:

STT	Thuật toán	Độ dài tham số theo bít	Sử dụng đến năm	Tham chiếu
1	DH	$L = 2048, N = 224$	2025	[SP 800-56A], [RFC2631]
2		$L = 2048, N = 256$	2025	
3		$L \geq 3072, N \geq 256$	2027	
4	ECDH	$n \geq 256$	2027	[SP 800-56A], [RFC6090]

Comment [Ma14]: DH, ECC

Comment [Ma15]: DH, ECC

- Yêu cầu đối với tham số khởi tạo khóa:

STT	Thuật toán	Độ dài tham số (bít)
1	RSA	• p, q là các số nguyên tố được sinh ngẫu nhiên • Số mũ công khai e: $65,537 \leq e < 2^{nlen-2security\_strength}$.
2	DSA	• p là một số nguyên tố, sao cho $2^{L-1} < p < 2^{L}$. • q là ước nguyên tố của $(p - 1)$, sao cho $2^{N-1} < p < 2^{N}$.
3	ECDSA	• n là bậc của điểm G và phải là một số nguyên tố.
4	GOST R34.10-2001	• $q$là bậc của điểm P và phải là một số nguyên tố.
5	GOST R34.10-2012	
6	DH	• p là một số nguyên tố, sao cho $2^{L-1} < p < 2^{L}$

		• *q* là ước nguyên tố của (*p* - 1), sao cho $2^{N-1}<p<2^{N}$
7	ECDH	• *n* là bậc của điểm G và phải là một số nguyên tố.

– Độ an toàn *security_strength* theo bít:

Security strength	RSA	DSA	ECDSA	Tham chiếu
112	2048	2048	224-255	SP 800-57
128	3072	3072	256-383	
192	7680	7680	384-511	
256	15360	15360	512+	

- Yêu cầu an toàn sử dụng đối với thuật toán thuật toán hàm băm như sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	SHA-256, SHA-512/256, SHA3-256	2027	[TCVN 11816-3], [FIPS PUB 180-4] [FIPS PUB 202],
2	SHA-384, SHA3-384	2027	
3	SHA-512, SHA3-512	2027	

Comment [Ma16]: Hàm băm chuyên dụng

Comment [Ma17]: SHA-2

Comment [Ma18]: Tiêu chuẩn SHA3

- Yêu cầu an toàn sử dụng đối với thuật toán đảm bảo tính toàn vẹn của thông điệp như sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	HMAC_SHA1_96	2023	[RFC7296]
2	AES_XCBC_96	2027	[RFC7296]
3	AES_CMAC_96	2027	[RFC4494]
4	HMAC_SHA_256_128	2027	[FIPS PUB 202], [RFC4868]
5	HMAC_SHA_256	2027	
6	HMAC_SHA_384_192	2027	
7	HMAC_SHA_384	2027	
8	HMAC_SHA_512_256	2027	
9	HMAC_SHA_512	2027	
10	HMAC_SHA3_256_128	2027	
11	HMAC_SHA3_256	2027	

Comment [Ma19]: HMAC_SHA1_96

Comment [Ma20]: AES_XCBC_96

Comment [Ma21]: AES-CMAC-96

Comment [Ma22]: Tiêu chuẩn SHA3

Comment [Ma23]: HMAC-SHA256 đến 512 trong IPsec

12	HMAC_SHA3_384_192	2027	
13	HMAC_SHA3_384	2027	
14	HMAC_SHA3_512_256	2027	
15	HMAC_SHA3_512	2027	

- Yêu cầu an toàn sử dụng đối với thuật toán mật mã dùng trong hàm giả ngẫu nhiên (PRF) như sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	AES128_XCBC	2027	[RFC7296], [RFC8247]
2	AES128_CMAC	2027	[RFC4615], [RFC8247]
3	HMAC_SHA1	2027	[RFC2104], [RFC8247]
4	HMAC_SHA_256	2027	[FIPS PUB 202], [RFC4868], [RFC8247]
5	HMAC_SHA_384	2027	
6	HMAC_SHA_512	2027	
7	HMAC_SHA3_256	2027	
8	HMAC_SHA3_384	2027	
9	HMAC_SHA3_512	2027	

Comment [Ma24]: PRF_AES_XCBC trong IKEv2

Comment [Ma25]: PRF, Các thuật toán sử dụ trong IKE

Comment [Ma26]: PRF_AES_CMAC

Comment [Ma27]: PRF, Các thuật toán sử dụ trong ipsec

Comment [Ma28]: Mã xác thực thông điệp – HMAC-SHA1

Comment [Ma29]: PRF, Các thuật toán sử dụ trong ipsec

Comment [Ma30]: Tiêu chuẩn SHA3

Comment [Ma31]: HMAC-SHA256 đến 512 trong IPsec

Comment [Ma32]: PRF, Các thuật toán sử dụ trong ipsec

- Yêu cầu an toàn sử dụng đối với các bộ tạo số ngẫu nhiên sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	Hash_DRBG	2027	[TCVN 12853], [SP 800-90A], [SP 800-131A],
2	HMAC_DRBG	2027	
3	CTR_DRBG	2027	
4	OFB_DRBG	2027	
5	MS_DRBG	2027	

Comment [Ma33]: Bộ tạo bít ngẫu nhiên

Comment [Ma34]: Tiêu chuẩn về tạo bít ngẫu nhiên của NIST

Comment [Ma35]: Khuyến nghị của NIST về thời gian sử dụng khóa

6	MQ_DRBG	2027	
7	XOR – NRBG	2027	[SP 800-90C], [SP 800-203]
8	Oversampling-NRBG Construction	2027	

Comment [Ma36]: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf

2.2. Yêu cầu kỹ thuật sản phẩm sử dụng công nghệ TLS VPN

2.2.1. Yêu cầu về sử dụng giao thức và thuật toán mật mã

- Sử dụng một trong các giao thức tạo kênh bảo mật sau:

STT	Giao thức
1	TLS 1.2
2	TLS 1.3

- Sử dụng một trong các thuật toán mã khối sau:

STT	Thuật toán
1	AES
2	TDEA
3	Camellia
4	CAST
5	SEED
6	GOST R 34.12-2015

- Sử dụng một trong các phương thức xác thực sau:

STT	Thuật toán
I	**Sử dụng mật mã khóa công khai**
1	RSASSA-PSS
3	DSA
6	ECDSA
7	GOST R34.10-2001

8	GOST R34.10-2012
II	**Sử dụng khóa bí mật chia sẻ trước**
1	PSK

- Sử dụng một trong các thuật toán sau cho trao đổi khóa:

STT	Thuật toán
1	DH
2	ECDH

- Sử dụng một trong các thuật toán băm sau:

STT	Thuật toán
1	SHA-256, SHA-512/256, SHA3-256
2	SHA-384, SHA3-384
3	SHA-512, SHA3-512

- Sử dụng một trong các bộ tạo số ngẫu nhiên sau:

STT	Thuật toán
1	Hash_DRBG
2	HMAC_DRBG
3	CTR_DRBG
4	OFB_DRBG
5	MS_DRBG
6	MQ_DRBG
7	XOR-NRBG Construction
8	Oversampling-NRBG Construction

- Sử dụng một trong các thuật toán mật mã dùng trong hàm giả ngẫu nhiên (PRF).

STT	Thuật toán

1	AES128_XCBC
2	AES128_CMAC
3	HMAC_SHA1
4	HMAC_SHA_256
5	HMAC_SHA_384
6	HMAC_SHA_512
7	HMAC_SHA3_256
8	HMAC_SHA3_384
9	HMAC_SHA3_512

2.2.2. Yêu cầu về an toàn giao thức và tham số mật mã

- Yêu cầu về thời gian sử dụng giao thức tạo kênh bảo mật như sau:

STT	Giao thức	Sử dụng đến năm
1	TLS 1.2	2027
2	TLS 1.3	2027

- Yêu cầu an toàn tham số mật mã đối với thuật toán mã khối như sau:

STT	Thuật toán	Chế độ hoạt động của mã khối	Kích thước khóa theo bít	Sử dụng đến năm	Tham chiếu
1	AES	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥ 128	2027	[TCVN 11367-3], [TCVN 12213], [SP 800-38D], [RFC4309], [RFC8247], [RFC2612]
2	TDEA	CBC, CFB, OFB hoặc CTR	192	2027	
3	Camellia	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥ 128	2027	
4	CAST	CBC, CFB, OFB hoặc CTR	≥ 128	2027	
5	SEED	CBC, CFB, OFB,	≥ 128	2027	

Comment [Ma37]: Cho thuật toán AES, 3DE Camelia

Comment [Ma38]: Các chế độ hoạt động EC CBC, CTR, OFB, CFB

Comment [Ma39]: Chế độ CCM

Comment [Ma40]: Các thuật toán sử dụng tr ipsec

Comment [Ma41]: Cho thuật toán CAST

		GCM, CCM hoặc CTR			
6	GOST R 34.12-2015	CTR, CFB	256	2027	[RFC7801]

- Yêu cầu an toàn tham số mật mã đối với các phương thức xác thực như sau:

STT	Thuật toán	Độ dài tham số theo bít	Sử dụng đến năm	Tham chiếu
I	**Sử dụng mật mã khóa công khai**			
1	RSASSA-PSS	*nlen* = 2048	2025	[TCVN 12214-2], [FIPS PUB 186-4], [SP 800-131A]
2		*nlen* ≥ 3072	2027	
3	DSA	$L = 2048, N = 224$	2025	[TCVN 12214-3], [FIPS PUB 186-4], [SP 800-131A]
4		$L = 2048, N = 256$	2025	
5		$L \geq 3072, N \geq 256$	2027	
6	ECDSA	$n \geq 256$	2027	
7	GOST R34.10-2001	$q = 256$	2027	[RFC7091]
8	GOST R34.10-2012	$256 \leq q \leq 512$	2027	
II	**Sử dụng khóa bí mật chia sẻ trước**			
1	PSK	- Đáp ứng các yêu cầu về tham số mật mã sử dụng.	2027	[SP 800-52], [RFC4279], RFC5487], [RFC5489]

- Yêu cầu an toàn tham số mật mã đối với thuật toán trao đổi khóa như sau:

STT	Thuật toán	Độ dài tham số theo bít	Sử dụng đến năm	Tham chiếu
1	RSA	*nlen* = 2048	2025	[TCVN 12214-2],

Comment [Ma42]: Cơ chế phân tích số nguyê

Comment [Ma43]: ECDSA, DSA, RSA

Comment [Ma44]: Khuyến nghị về sử dụng khóa

Comment [Ma45]: DSA và ECDSA

Comment [Ma46]: ECDSA, DSA

Comment [Ma47]: Khuyến nghị về sử dụng khóa

Comment [Ma48]: Thuật toán GOST

Comment [Ma49]: Cơ chế phân tích số nguyê

2		$nlen \geq 3072$	2027	[FIPS PUB 186-4], [SP 800-131A]
3	DH	$L = 2048, N = 224$	2025	[SP 800-56A], [RFC2631]
4		$L = 2048, N = 256$	2025	
5		$L \geq 3072, N \geq 256$	2027	
6	ECDH	$n \geq 256$	2027	[SP 800-56A], [RFC6090]

Comment [Ma50]: ECDSA, DSA, RSA

Comment [Ma51]: Khuyến nghị về sử dụng khóa

Comment [Ma52]: DH, ECC

Comment [Ma53]: Trao đổi khóa DH

Comment [Ma54]: DH, ECC

Comment [Ma55]: Mô tả về ECDH

- Yêu cầu đối với tham số khởi tạo khóa:

STT	Thuật toán	Độ dài tham số (bít)
1	RSA	• *p*, *q* là các số nguyên tố được sinh ngẫu nhiên • Số mũ công khai e: $65,537 \leq e < 2^{nlen-2security\_strength}$.
2	DSA	• *p* là một số nguyên tố, sao cho $2^{L-1} < p < 2^{L}$. • *q* là ước nguyên tố của (*p* - 1), sao cho $2^{N-1} < p < 2^{N}$.
3	ECDSA	• *n* là bậc của điểm G và phải là một số nguyên tố.
4	GOST R34.10-2001	• *q*là bậc của điểm P và phải là một số nguyên tố.
5	GOST R34.10-2012	
6	DH	• *p* là một số nguyên tố, sao cho $2^{L-1} < p < 2^{L}$. • *q* là ước nguyên tố của (*p* - 1), sao cho $2^{N-1} < p < 2^{N}$.
7	ECDH	• *n* là bậc của điểm G và phải là một số nguyên tố.

– Độ an toàn *security_strength* theo bít:

Security strength	RSA	DSA	ECDSA	Tham chiếu
112	2048	2048	224-255	SP 800-57
128	3072	3072	256-383	
192	7680	7680	384-511	
256	15360	15360	512+	

- Yêu cầu an toàn sử dụng đối với thuật toán thuật toán hàm băm như sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	SHA-256, SHA-512/256, SHA3-256	2027	[TCVN 11816-3], [FIPS PUB 180-4], [FIPS PUB 202],
2	SHA-384, SHA3-384	2027	
3	SHA-512, SHA3-512	2027	

Comment [Ma56]: Hàm băm chuyên dụng

Comment [Ma57]: SHA-2

Comment [Ma58]: Tiêu chuẩn SHA3

- Yêu cầu an toàn sử dụng đối với thuật toán mật mã dùng trong hàm giả ngẫu nhiên (PRF) như sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	AES128_XCBC	2027	[RFC7296], [RFC8247]
2	AES128_CMAC	2027	[RFC4615], [RFC8247]
3	HMAC_SHA1	2027	[RFC2104], [RFC8247]
4	HMAC_SHA_256	2027	[FIPS PUB 202], [RFC4868], [RFC8247]
5	HMAC_SHA_384	2027	
6	HMAC_SHA_512	2027	
7	HMAC_SHA3_256	2027	
8	HMAC_SHA3_384	2027	
9	HMAC_SHA3_512	2027	

Comment [Ma59]: PRF_AES_XCBC trong IKEv2

Comment [Ma60]: PRF, Các thuật toán sử dụ trong IKE

Comment [Ma61]: PRF_AES_CMAC

Comment [Ma62]: PRF, Các thuật toán sử dụ trong ipsec

Comment [Ma63]: Mã xác thực thông điệp – HMAC-SHA1

Comment [Ma64]: PRF, Các thuật toán sử dụ trong ipsec

Comment [Ma65]: Tiêu chuẩn SHA3

Comment [Ma66]: HMAC-SHA256 đến 512 trong IPsec

Comment [Ma67]: PRF, Các thuật toán sử dụ trong ipsec

- Yêu cầu an toàn sử dụng đối với các bộ tạo số ngẫu nhiên sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	Hash_DRBG	2027	[TCVN 12853], [SP 800-90A], [SP 800-131A],
2	HMAC_DRBG	2027	
3	CTR_DRBG	2027	
4	OFB_DRBG	2027	

Comment [Ma68]: Bộ tạo bít ngẫu nhiên

Comment [Ma69]: Tiêu chuẩn về tạo bít ngẫu nhiên của NIST

Comment [Ma70]: Khuyến nghị của NIST về thời gian sử dụng khóa

5	MS_DRBG	2027	
6	MQ_DRBG	2027	
7	XOR – NRBG	2027	[SP 800-90C], [SP 800-203]
8	Oversampling-NRBG Construction	2027	

Comment [Ma71]: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf

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 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 theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 và 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, 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 được cơ quan quản lý nhà nước có thẩm quyền tiến hành định kỳ hàng năm hoặc đột xuất.

3.4. Các quy định trong trong Quy chuẩn được rà soát lạihằng năm để sửa đổi, bổ sung Quy chuẩn này để đảm bảo phù hợp với thực tiễn và đáp ứng yêu cầu quản lý.

4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Cơ quan, tổ chức cá nhân hoạt động kinh doanh và sử dụng sản phẩm bảo mật luồng IP phải đảm bảo chất lượng phù hợp với Quy chuẩn này, thực hiện công bố hợp quy theo Quy định về chứng nhận hợp chuẩn, chứng nhận hợp quy và công bố hợp chuẩn, công bố hợp quy ban hành kèm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 và 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 và theo quy định tại Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 và chịu sự kiểm tra thường xuyên, đột xuất 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

TT	Tên sản phẩm, hàng hóa theo QCVN	Mã số 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 8471.41.90 8471.49.90 8471.80.90 8517.62.10 8517.62.21 8517.62.29 8517.62.30 8517.62.41 8517.62.42 8517.62.49 8517.62.51 8517.62.52 8517.62.53 8517.62.59 8517.62.61 8517.62.69 8517.62.91 8517.62.92 8517.62.99 8525.50.00 8525.60.00 8528.71.11 8528.71.19 8528.71.91 8528.71.99	Sản phẩm có tính năng bảo mật luồng IP sử dụng công nghệ IPSec hoặc TLS

TÀI LIỆU THAM KHẢO

1. NIST Special Publication 800-77 *"Guide to IPsec VPNs"*, 2020.
2. NIST Special Publication 800-113 *"Guide to SSL VPNs"*, 2008.
3. NIST Special Publication 800-52 *"Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"*, August 2019.
4. Technical Guideline TR-02102-2 *"Cryptographic Mechanisms:Recommendations and Key Lengths"*, Federal Office for Information Security, 2021.
5. Technical Guideline TR-02102-3 *"Cryptographic Mechanisms: Recommendations and KeyLengths"*, Federal Office for Information Security, 2021.
6. NIST Special Publication 800-90A *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*,June 2015.
7. NIST Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths"*, March 2019.
8. NIST Special Publication 800-90C (Second Draft) "*Recommendation for Random Bit Generator (RBG) Constructions*", National Institute of Standards and Technology, April 2016.
9. NIST SP 800-57 Part 1 Rev. 5 "*Recommendation for Key Management: Part 1 – General*", National Institute of Standards and Technology, May 2020.
10. SP 800-203 *"2017 NIST/ITL Cybersecurity Program Annual Report"*, National Institute of Standards and Technology, July 2018.
11. FIPS PUB 186-4 *"Digital Signature Standard (DSS)"*, Federal Information Processing Standards Publication, July 2013.
12. FIPS PUB 202 *"SHA-3 Standard: Permutation-Based Hash andExtendable-Output Functions"*, National Institute of Standards and Technology, August 2015.
13. NIST Special Publication 800-38D *"Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC",*November, 2007.
14. FIPS PUB 180-4 *"Secure Hash Standard (SHS)"*, Federal Information Processing Standards Publication, August 2015.
15. NIST Special Publication 800-56A *"Recommendation for Pair-Wise Key Establishment Schemes UsingDiscrete Logarithm Cryptography"*, May 2013.
16. RSA Laboratories. *PKCS#1 v2.1: RSA Cryptography Standard*. June 2002. (Phòng thí nghiệm RSA. *PKCS#1 v2.1: Tiêu chuẩn mật mã RSA*. Tháng 6năm 2002).
17. [RFC2612]: *The CAST-256 Encryption Algorithm*, Internet Engineering Task Force (IETF), June 1999.
18. [RFC4309]:*Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*, Internet Engineering Task Force (IETF), December 2005.
19. [RFC8247]: *Algorithm Implementation Requirements and Usage Guidancefor the Internet Key Exchange Protocol Version 2 (IKEv2)*, Internet Engineering Task Force (IETF), September 2017.
20. [RFC7801]: *GOST R 34.12-2015: Block Cipher "Kuznyechik"*, Internet Engineering Task Force (IETF),March 2016.

21. [RFC7296]*: Internet Key Exchange Protocol Version 2 (IKEv2)*, Internet Engineering Task Force (IETF), October 2014.
22. [RFC4615]: *The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)*, Internet Engineering Task Force (IETF), October 2014.
23. [RFC2104]: *HMAC: Keyed-Hashing for Message Authentication*, Internet Engineering Task Force (IETF), February 1997.
24. [RFC4868]: *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*, Internet Engineering Task Force (IETF), May 2007.
25. [RFC3526]: *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*, Internet Engineering Task Force (IETF), May 2003.
26. [RFC5114]: *Additional Diffie-Hellman Groups for Use with IETF Standards*, Internet Engineering Task Force (IETF), January 2008.
27. [RFC5903]: *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*, Internet Engineering Task Force (IETF), June 2010.
28. [RFC6954]: *Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)*, Internet Engineering Task Force (IETF), July 2013.
29. [RFC4753]: *ECP Groups for IKE and IKEv2*, Internet Engineering Task Force (IETF), January 2007.
30. [RFC4754]: *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*, Internet Engineering Task Force (IETF), January 2007.
31. [RFC7427]: *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*, Internet Engineering Task Force (IETF), January 2015.
32. [RFC4055]: *Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF), June 2005.
33. [RFC7091]: *GOST R 34.10-2012: Digital Signature Algorithm*, Internet Engineering Task Force (IETF), December 2013.
34. [RFC2404]: *The Use of HMAC-SHA-1-96 within ESP and AH*, Internet Engineering Task Force (IETF), November 1998.
35. [RFC3566] *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*, Internet Engineering Task Force (IETF), September 2003.
36. [RFC4494]: *The AES-CMAC-96 Algorithm and Its Use with IPsec*, Internet Engineering Task Force (IETF), June 2006.
37. [RFC2631] *Diffie-Hellman Key Agreement Method*, Internet Engineering Task Force (IETF), June 1999.
38. [RFC6090]: *Fundamental Elliptic Curve Cryptography Algorithms*, Internet Engineering Task Force (IETF), February 2011.
39. [RFC4357]: *Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms*, Internet Engineering Task Force (IETF), January 2006.

40. [RFC4279]:*Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, Internet Engineering Task Force (IETF),December 2005.
41. [RFC5487]: *Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode*, Internet Engineering Task Force (IETF),March 2009.
42. [RFC5489]: ECDHE_PSK Cipher Suites for Transport Layer Security (TLS), Internet Engineering Task Force (IETF),March 2009.
43. [RFC8446]: *The Transport Layer Security (TLS) Protocol Version 1.3*, Internet Engineering Task Force (IETF),August 2018.
44. [RFC7919]: *Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)*, Internet Engineering Task Force (IETF),August 2016.
45. [RFC8422]: *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*, Internet Engineering Task Force (IETF),August 2018.
46. [RFC7027]: *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)*, Internet Engineering Task Force (IETF),October 2013.
47. [RFC8734]: *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS) Version 1.3*, Internet Engineering Task Force (IETF),February 2020.
48. [RFC4434]: *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*, Internet Engineering Task Force (IETF),February 2006.
49. 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.
50. 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.
51. TCVN 12853:2020 Công nghệ thông tin - Các kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên.
52. TCVN 11816 (ISO/IEC 10118) Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng.
53. TCVN 12214-2:2018 Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số kèm phụ lục – Phần 2: Các cơ chế dựa trên phân tích số nguyên.
54. TCVN 12214-3:2018 Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số kèm phụ lục – Phần 3: Các cơ chế dựa trên logarit rời rạc.
55. TCVN 7635:2007 Kỹ thuật mật mã – Chữ ký số.
56. TCVN 7876:2007 Công nghệ thông tin – Kỹ thuật mật mã – Thuật toán mã dữ liệu AES.
57. TCVN 11367-2:2016 (ISO/IEC 18033-2:2006) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng.
58. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) Công nghệ thông tin – Các kỹ thuật an toàn- Mã xác nhận thông điệp.