

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN XXXX : 2026/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MẬT MÃ TRONG LĨNH VỰC MẬT MÃ DÂN SỰ CHO HỆ THỐNG QUẢN LÝ ĐỊNH DANH VÀ XÁC THỰC

NATIONAL TECHNICAL REGULATION ON CRYPTOGRAPHY IN THE FIELD OF CIVIL CRYPTOGRAPHY FOR IDENTITY AND AUTHENTICATION MANAGEMENT SYSTEMS

HÀ NỘI – 2026

MỤC LỤC

Danh mục bảng biểu *3*
Lời nói đầu *4*
1. QUY ĐỊNH CHUNG *5*
1.1. Phạm vi điều chỉnh 5
1.2. Đối tượng áp dụng 5
1.4. Giải thích từ ngữ 6
1.5 Ký hiệu 8
1.6. Từ viết tắt 8
2. QUY ĐỊNH KỸ THUẬT *10*
2.1 Các yêu cầu chung 10
2.2 Các yêu cầu về mã hóa dữ liệu 10
2.2.1 Các thuật toán mã hóa đối xứng 10
2.2.2 Các chế độ hoạt động 11
2.2.3 Thuật toán mã hóa phi đối xứng 11
2.3 Các yêu cầu về chữ ký số 11
2.3.1 Các yêu cầu về hàm băm 11
2.3.2 Thuật toán mã xác thực thông điệp 12
2.3.3 Thuật toán chữ ký số 13
2.4 Các yêu cầu về quản lý khóa 14
2.4.1 Yêu cầu chung 14
2.4.2 Sinh khóa 14
2.4.3 Phân phối và trao đổi khóa 14
2.4.4 Lưu trữ khóa 14
2.4.5 Thay thế, Thu hồi, Hủy khóa 14
2.4.6 Bộ sinh số ngẫu nhiên 14
2.4.7 Hàm dẫn xuất khóa 15
2.4.8 Cơ chế thỏa thuận khóa 15
2.5 Yêu cầu về giao thức 16
2.5.1 Yêu cầu chung 16
2.5.2 Yêu cầu đối với giao thức TLS 16
2.5.3 Yêu cầu đối với giao thức HTTPS 17
2.5.4 Yêu cầu đối với giao thức *OPENAPI/API* 17
2.5.5 Yêu cầu đối với giao thức VPN 17
3. QUY ĐỊNH VỀ QUẢN LÝ *17*
4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN *18*
5. TỔ CHỨC THỰC HIỆN *18*
THƯ MỤC TÀI LIỆU THAM KHẢO *19*

Danh mục bảng biểu

Bảng 1: Danh mục thuật toán mã hóa đối xứng được phép sử dụng 10
Bảng 2: Danh mục thuật toán mã hóa phi đối xứng được phép sử dụng 11
Bảng 3: Danh mục các hàm băm được phép sử dụng 12
Bảng 4: Danh mục các thuật toán xác thực thông điệp được phép sử dụng 12
Bảng 5: Danh mục thuật toán chữ ký số được phép sử dụng 13
Bảng 6: Danh mục các bộ sinh số ngẫu nhiên được phép sử dụng 15
Bảng 7: Danh mục hàm dẫn xuất khóa được phép sử dụng 15
Bảng 8: Danh mục cơ chế thỏa thuận khóa được phép sử dụng 15
Bảng 9: Danh mục các giao thức được phép sử dụng 16

Lời nói đầu

QCVN XXX : 2026/BQP do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định và được ban hành theo Thông tư số /2026/TT-BQP ngày / /2026 của Bộ trưởng Bộ Quốc phòng.

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MẬT MÃ TRONG LĨNH VỰC MẬT MÃ DÂN SỰ CHO HỆ THỐNG QUẢN LÝ ĐỊNH DANH VÀ XÁC THỰC

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định các yêu cầu về mã dữ liệu, chữ ký số, xác thực thông điệp, quản lý khóa và các giao thức được sử dụng trong hệ thống quản lý định danh và xác thực điện tử để 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:

a) Cơ quan quản lý nhà nước về định danh và xác thực điện tử;

b) Tổ chức, doanh nghiệp, cá nhân xây dựng, phát triển, cung cấp, tích hợp hoặc vận hành hệ thống định danh và xác thực điện tử có sử dụng kỹ thuật mật mã;

c) Tổ chức đánh giá, kiểm định, chứng nhận sản phẩm, mô-đun hoặc giải pháp mật mã được sử dụng trong hệ thống định danh và xác thực điện tử;

d) Các cơ quan, tổ chức, cá nhân khác có liên quan đến việc ứng dụng, triển khai, quản lý hoặc khai thác các thành phần kỹ thuật mật mã phục vụ định danh và xác thực điện tử.

1.3. Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây là cần thiết cho việc áp dụng Quy chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

- FIPS 197, Advanced Encryption Standard (AES).

- FIPS 180-4, Secure Hash Standard (SHS).

- FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

- FIPS 186-5, Digital Signature Standard (DSS).

- FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA).

- FIPS 205, Stateless Hash-Based Digital Signature Standard (SLH-DSA).

- NIST SP 800-90A Rev.1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators.

- NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation.

- NIST SP 800-232, Ascon-Based Lightweight Cryptography Standards for Constrained Devices.

- RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF).

- RFC 7748, Elliptic Curves for Security.

- RFC 8032, Edwards-Curve Digital Signature Algorithm (EdDSA).

- RFC 8439, ChaCha20 and Poly1305 for IETF Protocols.

- RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3.

- TCVN 11367, Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã hóa khối AES.

- TCVN 14263:2024, Công nghệ thông tin - Thuật toán mã hóa khối MKV.

1.4. Giải thích từ ngữ

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

1.4.1 Hệ thống định danh và xác thực điện tử

Hệ thống dùng để xác lập và xác thực danh tính của người sử dụng hoặc thiết bị thông qua phương tiện điện tử.

[Điều 3, Nghị định 69/2024/NĐ-CP]

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.

[1.4.2, QCVN 07:2026/BQP]

1.4.3 Kỹ thuật mật mã

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

[1.4.5, QCVN 07:2026/BQP]

1.4.4 Khóa

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

[3.16, TCVN 11717-1:2017]

1.4.5 Hàm băm

Hàm mà ánh xạ một xâu bit tới một xâu bit có độ dài xác định thỏa mãn 2 tính chất sau:

- Không thể tìm được một giá trị đầu vào và ứng với một giá trị đầu ra cho trước;

- Không thể tìm được một đầu vào thứ 2 khác với đầu vào cho trược mà có cùng đầu ra.

[3.4 TCVN 11816-1:2017]

1.4.6 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.

1.4.7 Chữ ký số

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.

1.4.8 Toàn vẹn dữ liệu

Tính chất của dữ liệu đã không bị thay đổi hay bị làm hư hại theo một cách trái phép.

1.4.9 Mã xác thực thông điệp

Chuỗi các bit là đầu ra của một thuật toán MAC.

[3.9 TCVN 11495-1:2016]

1.4.10 Thuật toán mã xác thực thông điệp

Thuật toán để tính ra một hàm ánh xạ các chuỗi bit và một khóa bí mật thành các chuỗi bit có chiều dài cố định, thỏa mãn hai tính chất sau:

- Đối với khóa bất kỳ và chuỗi đầu vào bất kỳ, hàm có thể tính được một cách hiệu quả;

- Đối với khóa có định bất kỳ, khi không cho biết thông tin về khóa trước về mặt tính toàn là không thể tính ra giá trị của hàm trên bất kỳ chuỗi đầu vào mới nào, thậm chí khi đã biết thông tin về tập chuỗi đầu vào và các giá trị hàm tương ứng, trong đó giá trị của chuỗi đầu vào thứ i có thể được chọn sau khi quan sát i-1 giá trị hàm đầu tiên (đối với số nguyên i>1).

[3.10 TCVN 11495-1:2016]

1.4.11 Quản lý khóa

Tập hợp các hoạt động quản trị và sử dụng dữ liệu khóa trong toàn bộ vòng đời khóa, bao gồm sinh, đăng ký, chứng nhận, phân phối, cài đặt, lưu trữ, lưu trữ dài hạn, dẫn xuất, thu hồi và hủy bỏ, phù hợp với chính sách an toàn.

1.4.12 Thiết lập khoá

Quá trình đảm bảo sự khả dụng một khoá bí mật dùng chung cho một hoặc nhiều thực thể. Thiết lập khoá bao gồm thoả thuận khoá và vận chuyển khoá

1.4.13 Thoả thuận khoá

Tiến trình kiến tạo một khoá bí mật dùng chung giữa hai thực thể theo cách mà không có bên nào có thể định trước giá trị cho khoá

1.4.14. Xác thực điện tử

Là hoạt động xác thực, xác nhận, khẳng định, chứng nhận, cung cấp danh tính điện tử, tài khoản định danh điện tử hoặc thông tin khác thuộc Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu căn cước, Cơ sở dữ liệu quốc gia về xuất nhập cảnh qua Hệ thống định danh và xác thực điện tử, nền tảng định danh và xác thực điện tử.

[Khoản 6, Điều 3, Nghị định 69/2024/NĐ-CP]

1.4.15. Sinh số ngẫu nhiên

Quá trình tạo ra giá trị số ngẫu nhiên hoặc gần ngẫu nhiên dùng trong thuật toán mật mã, sinh khóa, nonce.

1.4.16 Mã hóa có xác thực

Phép biến đổi dữ liệu bằng thuật toán mã hóa để tọa ra bản mã không thể bị truy xuất bởi thực thể trái phép mà không bị phát hiện, tức là nó cung cấp bảo vệ tính bí mật dữ liệu, tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu (có tính đảo ngược).

[3.10 TCVN 12197:2018]

1.4.17 Bảo mật kênh truyền

Tập hợp các biện pháp nhằm bảo đảm thông tin truyền qua kênh không bị nghe lén, giả mạo hoặc sửa đổi.

1.5 Ký hiệu

$nlen$	Độ dài modulo theo bit;
$\|p\|$	Độ dài tính theo bit của p với p là mô-đun của trường hữu hạn nguyên tố $\mathbb{F}_p$
L	Độ dài của tham số miền p theo bit
N	Độ dài của tham số miền q theo bit

1.6. Từ viết tắt

Chữ viết tắt	Tên đầy đủ	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CCM	Counter with CBC-MAC	Chế độ đếm kết hợp mã xác thực CBC
DRBG	Deterministic Random Bit Generator	Bộ sinh bit ngẫu nhiên xác định
ECDH	Elliptic Curve Diffie-Hellman	Trao đổi khóa Diffie–Hellman trên đường cong elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số đường cong elliptic
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ
GCM	Galois/Counter Mode	Chế độ đếm kết hợp Galois
HKDF	HMAC-based Key Derivation Function	Hàm dẫn xuất khóa dựa trên HMAC
KDF	Key Derivation Function	Hàm dẫn xuất khóa
KWP	Key Wrapping with Padding	Thuật toán đóng gói khóa có đệm

KW	Key Wrapping	Thuật toán đóng gói khóa
MAC	Message Authentication Code	Mã xác thực thông điệp
PBKDF	Password-Based Key Derivation Function	Hàm dẫn xuất khóa từ mật khẩu
RSA	Rivest-Shamir-Adleman	Thuật toán mật mã khóa công khai RSA
SHA	Secure Hash Algorithm	Thuật toán băm an toàn

2. QUY ĐỊNH KỸ THUẬT[1]

2.1 Các yêu cầu chung

1. Hệ thống định danh và xác thực điện tử chỉ được phép sử dụng các thuật toán mật mã, cơ chế mật mã và tham số mật mã tương ứng quy định tại Quy chuẩn này để bảo vệ thông tin.
2. Việc lựa chọn thuật toán mật mã, cơ chế mật mã và tham số tương ứng phải phù hợp với chức năng an toàn cần bảo đảm và mục đích sử dụng.
3. Thuật toán mật mã, cơ chế mật mã và các tham số tương ứng phải bảo đảm mức an toàn tối thiểu tương đương 128 bit.
4. Khóa mật mã phải được quản lý trong suốt vòng đời, bao gồm sinh khóa, phân phối, lưu trữ, sử dụng, thay thế, thu hồi và hủy bỏ theo yêu cầu được quy định tại Quy chuẩn này bảo đảm ngăn chặn việc truy cập, sử dụng hoặc thay đổi trái phép.

2.2 Các yêu cầu về mã hóa dữ liệu

2.2.1 Các thuật toán mã hóa đối xứng

Sử dụng các thuật toán mã hóa dưới đây.

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

STT	Tên thuật toán	Kích thước khóa theo bit	Thời gian sử dụng	Tài liệu tham chiếu
1	AES	128 bit	2030	[FIPS 197], [TCVN 11367]
		192 bit	2030	
		256 bit	2035	
2	MKV-128	128 bit	2030	[TCVN 14263:2024]
		192 bit	2030	
		256 bit	2035	
	MKV-256	256 bit	2035	[TCVN 14263:2024]
		384bit	2040	
		512 bit	2045	
3	ASCON-AEAD	128 bit	2030	[SP 800-232]
4	ChaCha20-Poly1305	256 bit	2035	[RFC 8439]

[1] Áp dụng tham chiếu đến tiêu chuẩn mới nhất trường hợp các tham chiếu đến trong mục này đã được sửa đổi, bổ sung, thay thế

2.2.2 Các chế độ hoạt động

1. Cho phép sử dụng các chế độ hoạt động sau:

a) CBC;

b) CTR;

c) GCM;

d) CCM;

e) XTS;

f) KW;

g) KWP.

2. Việc sử dụng các chế độ hoạt động phải đáp ứng các yêu cầu sau:

a) Đối với chế độ CBC, chỉ được phép sử dụng để giải mã dữ liệu cũ, không dùng để mã hóa dữ liệu mới kể từ thời điểm quy chuẩn này có hiệu lực.

b) Chế độ XTS chỉ được sử dụng để bảo vệ dữ liệu lưu trữ.

c) Chế độ GCM và CCM được sử dụng như cơ chế mã hóa có xác thực.

d) Chế độ KW và KWP được sử dụng để bảo vệ hoặc vận chuyển khóa.

2.2.3 Thuật toán mã hóa phi đối xứng

Sử dụng các thuật toán mật mã phi đối xứng sau:

Bảng 2: Danh mục thuật toán mã hóa phi đối xứng được phép sử dụng

STT	Tên thuật toán	Tham số	Sử dụng đến năm	Tham chiếu
1	RSA-OAEP	nlen ≥ 3072 bit	2030	[ISO/IEC 18033-2], [SP 800-56B Rev. 2]
2	ECIES	$256\ bit \leq \lvert p \rvert$ < 384 bit	2030	[ISO/IEC 18033-2]
		$384\ bit \leq \lvert p \rvert$ < 512 bit	2035	
		$\lvert p \rvert \geq$ 512 bit	2035	
3	ML-KEM	ML-KEM-512	2030	FIPS 203; NIST SP 800-227
		ML-KEM-768	2035	
		ML-KEM-1024	2040	

2.3 Các yêu cầu về chữ ký số

2.3.1 Các yêu cầu về hàm băm

Sử dụng các hàm băm dưới đây.

Bảng 3: Danh mục các hàm băm được phép sử dụng

STT	Thuật toán	Sử dụng đến năm	Tài liệu viện dẫn
1	SHA-256	2030	[FIPS 180-4] [FIPS 202]
	SHA-512/256		
	SHA-384	2030	
	SHA-512	2035	
2	SHA3-256	2030	[FIPS 202] [NIST IR 8547]
	SHA3-384	2030	
	SHA3-512	2035	
3	SHAKE128	2035	
	SHAKE256	2040	
4	Ascon-Hash256	2030	NIST SP 800-232

2.3.2 Thuật toán mã xác thực thông điệp

Sử dụng các thuật toán mã xác thực thông điệp dưới đây.

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

STT	Thuật toán	Sử dụng đến năm	Tài liệu viện dẫn
1	HMAC-SHA-256	2030	[FIPS 198-1]
2	HMAC-SHA-384	2030	
3	HMAC-SHA-512	2035	
4	HMAC-SHA3-256	2030	[SP 800-107 Rev.1]
5	HMAC-SHA3-384	2030	
6	HMAC-SHA3-512	2035	
7	AES-128-CMAC	2030	[NIST SP 800-38B]; [RFC 4493]
8	AES-256-CMAC	2030	
9	KMAC128	2035	[NIST SP 800-185]
10	KMAC256	2040	

12	Poly1305	2035	[RFC 8439]

2.3.3 Thuật toán chữ ký số

Sử dụng các thuật toán chữ ký số dưới đây.

Bảng 5: Danh mục thuật toán chữ ký số được phép sử dụng[2]

STT	Thuật toán	Tham số	Sử dụng đến năm	Tài liệu viện dẫn
1	RSASSA-PSS	3072 bit $\leq nlen <$ 7680 bit	2030	[FIPS 186-5], [RFC 8017]
		$nlen \geq 7068$ bit	2035	
2	ECDSA	$256\ bit \leq \|p\| <$ 384 bit	2030	[FIPS 186-5] [NIST SP 800-186]
		$384\ bit \leq \|p\| <$ 512 bit	2030	
		$\|p\| \geq$ 512 bit	2035	
3	EdDSA	Ed25519	2030	[RFC 8032], [FIPS 186-5]
		Ed448	2035	
4	ML-DSA	ML-DSA-44;	2030	[FIPS 204]
		ML-DSA-65;	2035	
		ML-DSA-87	2040	
5	SLH-DSA	SLH-DSA-SHA2-128[s/f]; SLH-DSA-SHAKE-128[s/f]	2035	[FIPS 205] [NIST IR 8547]
		SLH-DSA-SHA2-192[s/f]; SLH-DSA-SHAKE-192[s/f]	2035	
		SLH-DSA-SHA2-256[s/f]; SLH-DSA-SHAKE-256[s/f]	2040	

[2] Khuyến khích nghiên cứu, áp dụng mô hình mật mã lai kết hợp thuật toán mật mã khóa công khai truyền thống (như RSA, ECDSA, ECDH) với thuật toán mật mã hậu lượng tử (như ML-KEM, ML-DSA) nhằm tăng cường khả năng bảo đảm an toàn thông tin trước nguy cơ tấn công bằng máy tính lượng tử khi chưa hoàn toàn thay thế được các thuật toán truyền thống. Việc kết hợp phải bảo đảm phù hợp với chức năng của từng thuật toán, sử dụng cơ chế kết hợp khóa hoặc chữ ký số được tiêu chuẩn hóa, không làm suy giảm mức độ an toàn mật mã và tuân thủ các quy định pháp luật có liên quan.

2.4 Các yêu cầu về quản lý khóa

2.4.1 Yêu cầu chung

a. Khóa phải được quản lý trong toàn bộ vòng đời, bao gồm sinh khóa, phân phối, lưu trữ, sử dụng, thay thế, thu hồi và hủy bỏ.
b. Mỗi khóa chỉ được sử dụng cho một mục đích/ một ngữ cảnh được xác định, không được dùng chung cho nhiều chức năng.
c. Khóa phải được bảo vệ chống truy cập, sử dụng, sửa đổi hoặc tiết lộ trái phép trong suốt vòng đời của khóa.

2.4.2 Sinh khóa

a. Khóa phải được sinh bằng các bộ sinh số ngẫu nhiên được quy định tại mục 2.4.6 Quy chuẩn này hoặc phần cứng tin cậy cảu thiết bị cung cấp có độ an toàn tương ứng.

b. Trường hợp khóa được sinh từ mật khẩu hoặc thông tin bí mật được chia sẻ phải sử dụng hàm dẫn xuất khóa được quy định tại mục 2.4.7 Quy chuẩn này.

c. Thuật toán và độ dài khóa phải phù hợp chính sách mật mã do hệ thống định danh và xác thực điện tử quy định.

d. Không được sử dụng khóa mặc định, khóa cố định hoặc khóa được xác định trước.

2.4.3 Phân phối và trao đổi khóa

Việc phân phối khóa, trao đổi khóa phải sử dụng các cơ chế thỏa thuận khóa được quy định tại mục 2.4.8 quy chuẩn này hoặc thông qua kênh truyền có mã hóa và xác thực được quy định tại mục 2.5 Quy chuẩn này.

2.4.4 Lưu trữ khóa

a. Khóa phải được lưu trữ trong vùng bảo mật do hệ điều hành hoặc mô đun mật mã (phần cứng của ứng dụng cung cấp)

b. Trường hợp lưu trữ bên ngoài mô đun mật mã các tham số này phải được bảo vệ bằng cơ chế mật mã được phép sử dụng theo Quy chuẩn này.

2.4.5 Thay thế, Thu hồi, Hủy khóa

a. Khóa phải được thay thế trước khi hết thời hạn sử dụng hoặc khi không còn đáp ứng yêu cầu an toàn quy định tại Quy chuẩn này.

b. Khóa phải được thu hồi khi có dấu hiệu bị lộ, bị sửa đổi trái phép, bị mất quyền kiểm soát hoặc không còn được phép sử dụng.

c. Khóa đã bị thu hồi không được sử dụng để thực hiện các tác vụ mới.

d. Việc hủy khóa phải bảo đảm khóa không thể được khôi phục hoặc tái tạo bằng các biện pháp kỹ thuật thông thường.

e. Khi hủy khóa, các bản ghi khóa bao gồm cả bản sao dự phòng phải được xóa hoặc vô hiệu hóa tương ứng.

2.4.6 Bộ sinh số ngẫu nhiên

Sử dụng các bộ sinh số ngẫu nhiên dưới đây.

Bảng 6: Danh mục các bộ sinh số ngẫu nhiên được phép sử dụng

STT	Thuật toán	Nguyên thủy mật mã	Sử dụng đến năm	Tài liệu viện dẫn
1	CTR-DRBG	AES-128, AES-192, AES-256	Năm sử dụng được tính bằng năm sử dụng của các nguyên thủy mật mã tương ứng	[SP 800-90A] [SP 800-90B]
2	Hash-DRBG	SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256		
3	HMAC-DRBG			

2.4.7 Hàm dẫn xuất khóa

Sử dụng các hàm dẫn xuất khóa dưới đây.

Bảng 7: Danh mục hàm dẫn xuất khóa được phép sử dụng

STT	Thuật toán	Nguyên thủy mật mã	Năm an toàn sử dụng	Tài liệu viện dẫn
1	HKDF	SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256	Năm sử dụng được tính bằng năm sử dụng của các nguyên thủy mật mã tương ứng	[RFC 5869], [NIST SP 800-56C]
2	PBKDF			[NIST SP 800-132]

2.4.8 Cơ chế thỏa thuận khóa

Sử dụng các thuật toán mã hóa dưới đây.

Bảng 8: Danh mục cơ chế thỏa thuận khóa được phép sử dụng

STT	Cơ chế	Tham số	Năm an toàn sử dụng	Tài liệu viện dẫn
1	ECDH/ECDHE	$256\ bit \leq \lvert p \rvert$ < 384 bit	2030	[NIST SP 800-56A]
		$384\ bit \leq \lvert p \rvert$< 512 bit	2035	

		$\|p\| \geq 512$ bit	2040	
2	DH/DHE	$L \geq 3072$ $N \geq 256\ bit$	2035	[NIST SP 800-56A]

2.5 Yêu cầu về giao thức

2.5.1 Yêu cầu chung

a. Hệ thống định danh và xác thực điện tử phải sử dụng các giao thức được quy định tại Quy chuẩn này để bảo vệ dữ liệu trong quá trình truyền thông.

b. Giao thức bảo mật phải sử dụng các thuật toán mật mã, cơ chế thiết lập khóa và tham số an toàn được quy định tại Quy chuẩn này.

c. Không được sử dụng các phiên bản giao thức hoặc bộ mật mã không đáp ứng yêu cầu an toàn quy định tại Quy chuẩn này.

2.5.2 Yêu cầu đối với giao thức TLS

1. Hệ thống định danh và xác thực điện tử được phép sử dụng các phiên bản giao thức TLS sau:

Bảng 9: Danh mục các giao thức được phép sử dụng

STT	Giao thức	Sử dụng đến năm	Tài liệu viện dẫn
1	TLS 1.2	2030	RFC 5246
2	TLS 1.3	2035	RFC 8446

2. Đối với các triển khai mới, phải ưu tiên sử dụng TLS 1.3.

3. Giao thức TLS 1.2 chỉ được sử dụng với các bộ mật mã sau:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256;

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384;

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256;

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384;

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256;

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256;

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256;

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384;

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256;

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384;

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256;

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384;

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256;

TLS_DHE_RSA_WITH_AES_256_CBC_SHA384;

4. Đối với giao thức TLS 1.3:

+ 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.

2.5.3 Yêu cầu đối với giao thức HTTPS

a. Giao thức HTTPS phải tuân thủ RFC 2818 và sử dụng giao thức TLS được quy định tại mục 2.5.2 quy chuẩn này.

b. Chứng thư số sử dụng trong HTTPS phải tuân thủ RFC 5280 và được cấp bởi tổ chức chứng thực tin cậy và phải còn hiệu lực.

2.5.4 Yêu cầu đối với giao thức

a. Các giao diện lập trình ứng dụng trong hệ thống định danh và xác thực điện tử phải được định nghĩa và được cung cấp qua giao thức HTTPS.

b. Cơ chế xác thực và ủy quyền truy cập API.

c. Đối với các giao dịch API truyền, nhận dữ liệu định danh sinh trắc học, dữ liệu xác thực hoặc thông tin nhạy cảm, hệ thống phải áp dụng các biện pháp bảo mật phù hợp nhằm bảo đảm tính bí mật, tính toàn vẹn, xác thực nguồn gốc dữ liệu và phòng, chống giả mạo, phát lại bản tin. Trường hợp giao dịch yêu cầu khả năng chống chối bỏ, phải sử dụng cơ chế chữ ký số và quản lý bằng chứng đáp ứng các yêu cầu kỹ thuật, pháp lý có liên quan.

2.5.5 Yêu cầu đối với giao thức VPN

Tuân thủ các yêu cầu tại Thông tư 23/2022/TT-BQP ngày 04/4/2022 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 và Thông tư số 07/2026/TT-BQP ngày 20/01/2026 ban hành, sửa đổi quy chuẩn kỹ thuật quốc gia và danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc trong lĩnh vực mật mã dân sự.

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1 Các mức giới hạn của đặc tính kỹ thuật mật mã quy định tại quy chuẩn này là các chỉ tiêu an toàn phục vụ quản lý theo quy định về quản lý chất lượng sản phẩm mật mã dân sự được quy định tại Luật An ninh mạng ngày 10 tháng 12 năm 2025.

3.2 Công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật theo Thông tư số 14/2026/TT-BKHCN ngày 09/4/2026 với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 5 hoặc phương thức 7; 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 Ban Cơ yếu Chính phủ xem xét thừa nhận kết quả đánh giá sự phù hợp do tổ chức đánh giá sự phù hợp nước ngoài thực hiện đối với các sản phẩm mật mã dân sự thuộc trách nhiệm quản lý theo quy định.

4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

4.1 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.

4.2 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.

5.4 Trong trường hợp các văn bản quy phạm pháp luật quy định tại quy chuẩn kỹ thuật này có sự thay đổi, bổ sung hoặc được thay thế thì thực hiện theo các văn bản mới. Trong trường hợp các tiêu chuẩn được viện dẫn trong quy chuẩn này có sự thay đổi, bổ sung, thay thế thì thực hiện theo hướng dẫn của Bộ Quốc phòng./.

THƯ MỤC TÀI LIỆU THAM KHẢO

[1]QCVN 01:2022/BQP, Quy chuẩn kỹ thuật quốc gia về sản phẩm mật mã dân sự.

[2] QCVN 05:2016/BQP, Quy chuẩn kỹ thuật quốc gia về trao đổi khóa mật mã.

[3] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques.

[4] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.

[5] NIST SP 800-56A Rev.3 (hoặc Rev.4), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

[6] NIST SP 800-56C Rev.2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes.

[7] NIST SP 800-107 Rev.1, Recommendation for Applications Using Approved Hash Algorithms.

[8] NIST SP 800-132, Recommendation for Password-Based Key Derivation.

[9] NIST SP 800-185, SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash.

[10] NIST SP 800-186, Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters.

[11] NIST IR 8547, Transition to Post-Quantum Cryptography Standards.

[12] RFC 4493, The AES-CMAC Algorithm.

[13] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2.

[14] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2.

[15] Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử.

[16] ETSI TS 119 312, Cryptographic Suites.

[17] EN 319 401, General Policy Requirements for Trust Service Providers.

[18] EN 319 411-1, Policy and Security Requirements for Trust Service Providers Issuing Certificates.