

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 IOT

NATIONAL TECHNICAL REGULATION ON CRYPTOGRAPHY IN THE FIELD OF CIVIL CRYPTOGRAPHY FOR IOT SYSTEMS

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu *4*
1. QUY ĐỊNH CHUNG *5*
1.1. Phạm vi điều chỉnh **5**
1.2. Đối tượng áp dụng **5**
1.3. Tài liệu viện dẫn **6**
1.4. Giải thích từ ngữ **7**
1.5 Ký hiệu **9**
1.6. Từ viết tắt **9**
2. QUY ĐỊNH KỸ THUẬT *10*
2.1 Yêu cầu chung **10**
2.1.1 Yêu cầu về bảo vệ dữ liệu 10
2.1.2 Kênh truyền dữ liệu 10
2.1.3 Quản lý khóa 10
2.2 Yêu cầu về kỹ thuật mật mã đối với lớp thiết bị **11**
2.2.1 Mật mã đối xứng 11
2.2.2 Mật mã phi đối xứng 13
2.2.3. Mật mã hạng nhẹ(*) 15
2.2.3.1 Mã khối hạng nhẹ 15
2.2.3.2 Mã dòng hạng nhẹ 15
2.2.3.3 Hàm băm 15
2.2.3.4 Mã xác thực thông điệp 16
2.2.3.5 Thuật toán mật mã phi đối xứng hạng nhẹ 16
2.2.4 Bộ sinh số ngẫu nhiên 16
2.3 Yêu cầu về mật mã đối với lớp mạng **16**
2.4 Yêu cầu về mật mã đối với lớp hỗ trợ ứng dụng và hỗ trợ dịch vụ **16**
2.5 Yêu cầu về mật mã đối với lớp ứng dụng **16**
3. QUY ĐỊNH VỀ QUẢN LÝ *17*
4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN *17*
5. TỔ CHỨC THỰC HIỆN *17*

Danh mục bảng biểu

Bảng 1: Danh mục các thuật toán mã khối, mã dòng được phép sử dụng 11
Bảng 2: Danh mục các chế độ mã khối được phép sử dụng 11
Bảng 3- Danh mục các hàm băm được phép sử dụng 12
Bảng 4- Danh mục các thuật toán mã xác thực thông báo được phép sử dụng 12
Bảng 5- Danh mục các thuật toán dẫn xuất khóa được phép sử dụng 13
Bảng 6- Danh mục các thuật toán mã hóa phi đối xứng được phép sử dụng 13
Bảng 7- Danh mục các lược đồ chữ ký số được phép sử dụng 14
Bảng 8- Danh mục các cơ chế thỏa thuận, thiết lập khóa được phép sử dụng 14
Bảng 9- Danh mục các thuật toán mã khối hạng nhẹ được phép sử dụng 15
Bảng 10- Danh sách thuật toán mã dòng hạng nhẹ được phép sử dụng 15
Bảng 11- Danh sách thuật hàm băm được phép sử dụng 15
Bảng 12- Danh mục mã xác thực thông điệp hạng nhẹ được phép sử dụng 16
Bảng 13- Danh sách thuật toán sinh số ngẫu nhiên 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 – Ban Cơ yếu Chính phủ 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 IOT

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

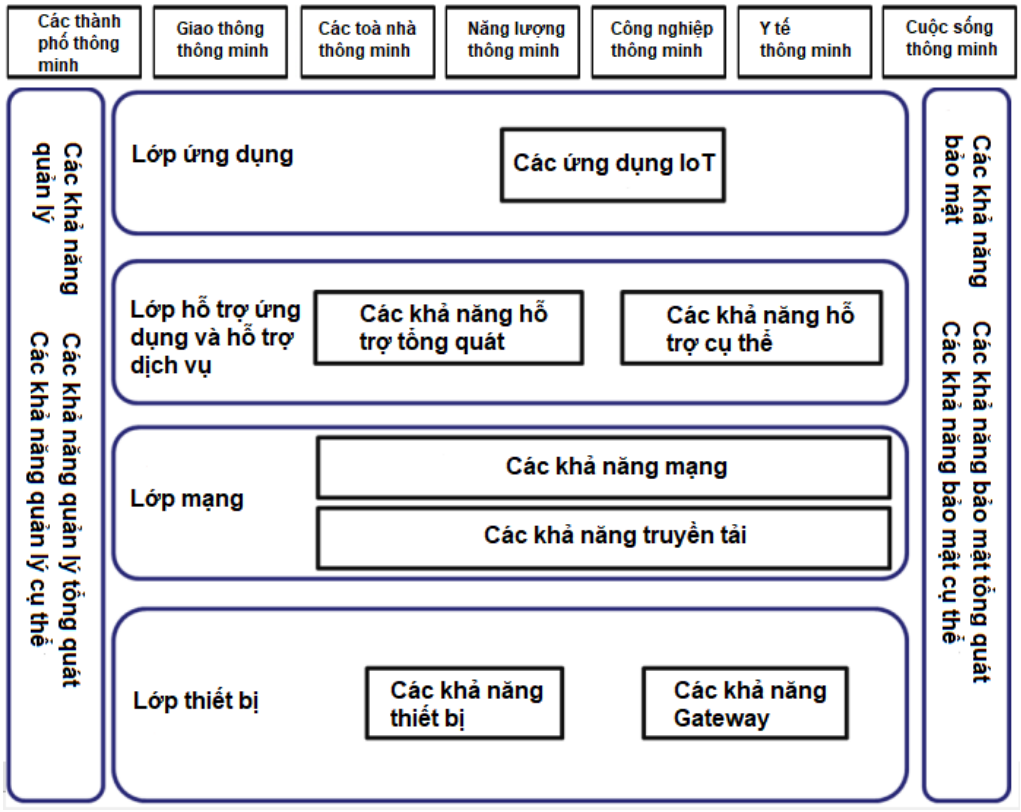
Quy chuẩn kỹ thuật này quy định các thuật toán mật mã được phép áp dụng trong hệ thống IoT sử dụng để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.2. Đối tượng áp dụng

Các yêu cầu về kỹ thuật mật mã trong quy chuẩn này được quy định áp dụng cho:

- Bảo mật dữ liệu trên các thiết bị;

- Bảo mật dữ liệu trên kênh truyền giữa các thiết bị trong cùng lớp hoặc giữa các lớp trong mô hình tham chiếu kiến trúc (hình 1).



Hình 1- Mô hình tham chiếu kiến trúc IoT (TCVN 13115:2020)

Đối tượng áp dụng của Quy chuẩn này bao gồm:

a) Cơ quan, tổ chức, doanh nghiệp xây dựng, thiết kế, triển khai hệ thống IoT.

b) Tổ chức, cá nhân sản xuất, nhập khẩu, phân phối thiết bị IoT.

c) Các phòng thử nghiệm, đơn vị kiểm định thiết bị IoT.

d) Các tổ chức đánh giá sự phù hợp theo quy định của pháp luật.

1.3. Tài liệu viện dẫn

TCVN 13115:2020: Internet vạn vật (IoT) - Các yêu cầu chung.

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

TCVN 12854-1:2020 (ISO/IEC 29192-1:2012): Công nghệ thông tin - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 1: Tổng quan.

TCVN 12854-2:2020: Công nghệ thông tin (ISO/IEC 29192-2:2012) - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 2: Mã khối.

TCVN 12854-3:2020 (ISO/IEC 29192-3:2012): Công nghệ thông tin - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 3: Mã dòng.

TCVN 12854-4:2020 (ISO/IEC 29192-4:2015): Công nghệ thông tin - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 4: Các cơ chế sử dụng kỹ thuật phi đối xứng.

TCVN 12849-5:2020 (ISO/IEC 29192-5:2016): Công nghệ thông tin - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 5: Hàm băm.

ISO/IEC 29192-6:2019 – TCVN 13952:2023: Công nghệ thông tin — Kỹ thuật an toàn — Mật mã hạng nhẹ — Phần 6: Mã xác thực thông điệp (MAC).

FIPS 197, Advanced Encryption Standard (AES).

NIST SP 800-56A Rev.3 – *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*; National Institute of Standards and Technology (NIST), 2018.

NIST SP 800-56B Rev.2 – *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*; NIST, 2019.

NIST SP 800-56C Rev.2 – *Recommendation for Key Derivation through Extraction-then-Expansion*; NIST, 2020.

NIST SP 800-90A Rev.1 – *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*; NIST, 2015.

NIST SP 800-90B – *Recommendation for the Entropy Sources Used for Random Bit Generation*; NIST, 2018.

NIST SP 800-90C – *Recommendation for Random Bit Generator (RBG) Constructions*; NIST, 2018.

NIST SP 800-108 – *Recommendation for Key Derivation Using Pseudorandom Functions (KDFs)*; NIST, 2009.

NIST SP 800-185 – *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*; NIST, 2016.

NIST SP 800-232 – *Recommendation for Lightweight Authenticated Encryption: ASCON*; NIST, 2020.

FIPS PUB 180-4 – *Secure Hash Standard (SHS)*; Federal Information Processing Standards, NIST, 2015.

FIPS PUB 202 – *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*; NIST, 2015.

RFC 8439 – *ChaCha20 and Poly1305 for IETF Protocols*; IETF, 2018.

RFC 8032 – *Edwards-Curve Digital Signature Algorithm (EdDSA)*: Ed25519 and Ed448; IETF, 2017.

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

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

ISO/IEC 14888-3:2016 – *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*; ISO/IEC, 2016.

NIST SP 800-213A: IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog, 2021.

NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

1.4. Giải thích từ ngữ

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

1.4.1 Internet vạn vật (IoT)

Cơ sở hạ tầng toàn cầu cho xã hội thông tin, cho phép các dịch vị tiên tiến bằng cách kết nối mọi vật (vật lý và ảo) dựa trên công nghệ thông tin và truyền thông tương thích hiện có và đang phát triển.

[4.77, TCVN 13116:2020]

1.4.2 Constrained device

Thiết bị hạn chế tài nguyên
Thiết bị hạn chế về đặc tính, chẳng hạn như hạn chế về năng lực xử lý, dung lượng bộ nhớ nhỏ, công suất pin hữu hạn, kết nối cự ly ngắn, tốc độ thấp.

[4.36, TCVN 13116:2020]

1.4.4 Mật mã hạng nhẹ

Mật mã được thiết kế riêng cho việc triển khai trong một số môi trường hạn chế.

[TCVN 12854-1:2020]

1.4.5 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.

1.4.6 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.

1.4.7 Hàm 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.

1.4.8 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 xác định;

- 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.

1.4.9 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.

1.4.10 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

1.4.11 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

1.4.12 Bộ sinh số ngẫu nhiên

Thuật toán sinh giá trị số ngẫu nhiên hoặc gần ngẫu nhiên dùng trong thuật toán mật mã, sinh khóa, nonce.

1.4.13 Độ an toàn

Số được liên kết với số lượng công việc (nghĩa là số hoạt động) được yêu cầu để phá vỡ một thuật toán mật mã hoặc hệ thống mật mã.

[TCVN 11367-1:2016]

CHÚ THÍCH 1 Độ an toàn của n là lượng công việc được yêu cầu để phá vỡ hệ thống mật mã tương đương với *2n* thực thi của hệ thống mật mã.

CHÚ THÍCH 2 Độ an toàn được đặc tả theo bit, như 80, 112, 128, 192, và 256 trong quy chuẩn này.

1.4.14 Kênh an toàn

Là kênh truyền thông giữa các thực thể trong hệ thống/mạng IoT được thiết lập và bảo vệ bằng các cơ chế mật mã nhằm bảo đảm thông tin truyền qua kênh được bảo vệ về tính bí mật, toàn vẹn và xác thực.

CHÚ THÍCH:

- Các giao thức thiết lập kênh truyền trên thiết bị IoT được nhà sản xuất tích hợp dựa trên mô hình triển khai, nhu cầu, cũng như khả năng đáp ứng tài nguyên của thiết bị.

- Một số giao thức phổ biến hiện nay trên thiết bị IoT có thể kể đến như: LoRaWAN, NB-IoT / LTE-M, Zigbee, BLE, MQTT + TLS, CoAP + DTLS, HTTPS…

1.5 Ký hiệu

$nlen$	Độ dài modulo theo bit sử dụng trong thuật toán RSA;
$\|p\|$	Độ dài tính theo bit của p với p là mô-đun của trường hữu hạn nguyên tố $\mathbb{F}_p$ của đường cong EC
L	Độ dài của tham số miền p theo bit sử dụng trong thuật toán DH
N	Độ dài của tham số miền q theo bit sử dụng trong thuật toán DH

1.6. Từ viết tắt

Chữ viết tắt	Tên đây đủ	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
DRBG	Deterministic Random Bit Generator	Bộ sinh bit ngẫu nhiên
ECDH	Elliptic Curve Diffie-Hellman	Diffi-Hellman trên đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số trên đường cong Elliptic
EdDSA	Edwards-Curve Digital Signature Algorithm	Thuật toán chữ ký số trên đường cong Edwards
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang
HKDF	HMAC-based Key Derivation Function	Hàm dẫn xuất khóa dựa trên HMAC
HSM	Hardware Security Module	Mô-đun bảo mật phần cứng
IoT	Internet of Things	Internet vạn vật
KWP	Key Wrapping with Padding	Thuật toán bọc khóa với bộ đệm Padding
KW	Key Wrapping	Thuật toán bọc khóa
MAC	Message Authentication Code	Mã xác thực thông điệp
MKV		Mã Khối Việt Nam
PBKDF	Password-Based Key Derivation Function	Hàm dẫn xuất khóa dựa trên mật khẩu
RSA	Rivest-Shamir-Adleman	Thuật toán mật mã khóa công khai RSA
SE	Secure Element	Phần tử bảo mật
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
TPM	Trusted Platform Module	Mô-đun nền tảng tin cậy

2. QUY ĐỊNH KỸ THUẬT

2.1 Yêu cầu chung

2.1.1 Yêu cầu về bảo vệ dữ liệu

a. Các giá trị mật khẩu, định danh, các dữ liệu xác thực, dữ liệu thông tin thu thập và dữ liệu sao lưu của thiết bị phải được lưu trữ có mã hóa trên thiết bị hoặc vùng nhớ truy cập từ xa.

b. Sử dụng phân vùng nhớ riêng biệt cho dữ liệu hệ thống và dữ liệu được sinh hoạt động của thiết bị.

c. Các kỹ thuật mật mã áp dụng cho cơ chế bảo vệ dữ liệu được quy định tại mục 2.2.

2.1.2 Kênh truyền dữ liệu

a. Sử dụng kênh an toàn trong giao tiếp giữa các thiết bị trong một lớp hoặc giữa các lớp trong mô hình kiến trúc tham chiếu IoT.

b. Các kỹ thuật mật mã sử dụng trong giao thức thiết lập kênh truyền tuân thủ theo quy định tại mục 2.2.

2.1.3 Quản lý khóa

2.1.3.1 Yêu cầu về sinh khóa

a. Thiết bị phải có khả năng sinh khóa (bao gồm cả các thành phần khóa) phục vụ cho các hoạt động mật mã trên thiết bị.

b. Các thuật toán sinh số giả ngẫu nhiên sử dụng trong sinh khóa được quy định tại mục 2.2.4.

2.1.3.2 Yêu cầu về lưu trữ khóa

Các giá trị khóa bí mật phải được lưu trữ dưới dạng mã hóa trên bộ nhớ của thiết bị hoặc được lưu trữ tại các modun riêng biệt: HSM, TPM, SE.

2.1.3.3 Sử dụng khóa

a. Không sử dụng trùng khóa với các mục đích, dịch vụ mã mật mã khác nhau.

Ví dụ: mã hóa dữ liệu, ký số, bọc khóa, xác thực, định danh thiết bị…

b. Khóa mặc định trên thiết bị chỉ được phép sử dụng trong quá trình thiết lập, tham gia hệ thống ban đầu. Sau khi thiết lập hoàn tất, giá trị khóa mặc định phải bị vô hiệu hóa hoặc thay đổi. Không sử dụng khóa mặc định với mục đích khác.

c. Các thành phần trong hệ thống IoT phải bảo đảm các khóa mật mã được kiểm soát trong đúng phạm vi được ủy quyền, không được phép truy cập, sao chép, trích xuất, xuất khẩu, thay đổi hoặc sử dụng khóa mật mã ngoài quyền hạn được cấp. Việc sử dụng khóa bởi hệ thống bên ngoài phải được kiểm soát, ghi nhận và có khả năng thu hồi hoặc luân chuyển khi cần thiết.

2.1.3.4 Yêu cầu về phân phối, thỏa thuận khóa

a. Có cơ chế cập nhật, thay khóa bí mật trên thiết bị IoT thông qua giao diện vật lý của thiết bị hoặc kênh truyền từ xa.

b. Kênh truyền sử dụng trong cập nhật, thay đổi khóa từ xa đáp ứng các yêu cầu tại 2.1.2.

c. Thuật toán thỏa thuận khóa được quy định tại mục 2.2.2.3.

2.1.3.5 Yêu cầu về hủy khóa

a. Việc huỷ khoá phải đảm bảo huỷ bỏ được tất cả các bản ghi khoá, bao gồm cả các bản sao dự phòng, sao cho không thể khôi phục được bất kì thông tin khoá nào dù bằng bất kì phương

tiện nào. Đồng thời không để bất kì khoá nào bị huỷ bỏ trước thời hạn nhằm đảm bảo khả năng giải mã khi dữ liệu hết thời hạn bảo mật.

b. Nếu khoá bị lộ, nghi ngờ bị lộ hoặc có sự thay đổi chủ sở hữu thì phải thực hiện thu hồi khoá để vô hiệu hoá nguy cơ bị lộ hoặc mất an toàn.

2.2 Yêu cầu về kỹ thuật mật mã đối với lớp thiết bị[1]

- Các yêu cầu từ 2.2.1 đến 2.2.4 quy định các kỹ thuật mật mã được phép sử dụng đối với bảo mật dữ liệu trên đường truyền và dữ liệu trên thiết bị.
- Đối với các thiết bị IoT không hạn chế tài nguyên chỉ sử dụng các kỹ thuật mật mã hạng nhẹ (tại mục 2.2.3) để giao tiếp với các thiết bị IoT hạn chế tài nguyên.
- Đối với các thiết bị hạn chế tài nguyên sử dụng các kỹ thuật mật mã hạng nhẹ tại muc 2.2.3

2.2.1 Mật mã đối xứng

2.2.1.1 Thuật toán mã hóa đối xứng

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

STT	Tên thuật toán	Kích thước khóa theo bit	Sử dụng đến năm	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	
		384 bit	2040	
		512 bit	2045	
3	ChaCha20-Poly1305	256 bit	2035	RFC 8439

Bảng 2: Danh mục các chế độ mã khối được phép sử dụng

STT	Chế độ hoạt động	Tham chiếu

[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

1	CBC	NIST SP 800-38A
2	CFB	
3	CTR	
4	OFB	
5	CBC-CS1	SP 800-38A Addendum
6	CBC-CS2	
7	CBC-CS3	
8	CCM	NIST SP 800-38C
9	GCM	NIST SP 800-38D
10	XTS	NIST SP 800-38E
11	KW, KWP	NIST SP 800-38F
12	FF1	NIST SP 800-38G

2.2.1.2 Hàm băm

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

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
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	

2.2.1.3 Mã xác thực thông báo

Bảng 4- Danh mục các thuật toán mã xác thực thông báo được phép sử dụng

STT	Thuật toán MAC	Nguyên thủy mật mã	Sử dụng đến năm	Tham chiếu
1	HMAC	SHA-256, SHA-384, SHA3-256, SHA3-384	2030	NIST SP 800-107
		SHA-512, SHA3-512	2035	
2	CMAC	AES MKV	Tuân thủ theo quy định về năm sử dụng	NIST SP 800-38B NIST SP 800-38D

4	GMAC	AES MKV	đối với thuật toán mã khối tại bảng 1	FIPS 197 TCVN 14263:2024
5	KMAC	KMAC128	2035	NIST SP 800-185
		KMAC256	2040	

2.2.2.4 Dẫn xuất khóa

Bảng 5- Danh mục các thuật toán 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 NIST SP 800-132
2	PBKDF			
3	BCKDF	AES MKV		FIPS 197 TCVN 14263:2024 NIST SP 800-108 NIST SP 800-38B

2.2.2 Mật mã phi đối xứng

2.2.2.1 Thuật toán mã hóa

Bảng 6- Danh mục các 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 NIST SP 800-56B Rev. 2
2	ECIES	$256\ bit \leq \lvert p \rvert$ < 384 bit	2030	ISO/IEC 18033-2
		$384\ bit \leq \lvert p \rvert$	2035	
3	ML-KEM-512	Tuân thủ theo tham số tại FIPS 203	2030	FIPS 203
	ML-KEM-768		2035	

	ML-KEM-1024		2040	

2.2.2.2 Chữ ký số

Bảng 7- Danh mục các lược đồ chữ ký số được phép sử dụng

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	$256\ bit \leq \lvert p\rvert <$ 384 bit	2030	[FIPS 186-5] [NIST SP 800-186]
		$384\ bit \leq \lvert p\rvert <$ 512 bit	2030	
		$\lvert p\rvert \geq$ 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	

2.2.2.3 Thỏa thuận và thiết lập khóa

Bảng 8- Danh mục các cơ chế thỏa thuận, thiết lập khóa được phép sử dụng

STT	Lược đồ	Tham số	Năm sử dụng	Tham chiếu
1	DH/DHE, MQV	$L \geq 3072$ $N \geq 256$	2035	NIST SP 800-56A

2	ECDH/ECDHE, ECMQV	$\|p\| \geq 256$	2035	NIST SP 800-56A
3	Thỏa thuận khóa RSA KAS1, KAS2	*nlen* ≥ 3072	2035	NIST SP 800-56B

2.2.3. Mật mã hạng nhẹ(*)[2]

2.2.3.1 Mã khối hạng nhẹ

Bảng 9- Danh mục các thuật toán mã khối hạng nhẹ được phép sử dụng

STT	Tên thuật toán	Tham chiếu
1	Ascon-AEAD128	NISP 800-232
2	PRESENT	TCVN 12854-2 :2020 ISO/IEC 29192-2
3	CLEFIA	
4	LEA	
5	Grain-128a	ISO/IEC 29192-8

2.2.3.2 Mã dòng hạng nhẹ

Bảng 10- Danh sách thuật toán mã dòng hạng nhẹ được phép sử dụng

STT	Tên thuật toán	Tham chiếu
1	Trivium	TCVN 12854-3 :2020 ISO/IEC 29192-3: 2012
2	Enocoro-128v2	

2.2.3.3 Hàm băm

Bảng 11- Danh sách thuật hàm băm được phép sử dụng

STT	Thuật toán	Tham chiếu
1	Ascon-Hash256.	SP 800-232
2	Ascon-XOF128, Ascon-CXOF128.	
3	PHOTON	TCVN 12854-5 :2020 ISO/IEC 29192-5: 2016
4	SPONGENT	
5	Lesamnta-LW	

[2] QCVN này không quy định năm sử dụng đối với các thuật toán mật mã hạng nhẹ

2.2.3.4 Mã xác thực thông điệp

Bảng 12- Danh mục mã xác thực thông điệp hạng nhẹ được phép sử dụng

STT	Thuật toán	Tài liệu viện dẫn
1	LightMAC	ISO/IEC 29192-6:2019
2	Chaskey-12	
3	Tsudik's Keymode	

2.2.3.5 Thuật toán mật mã phi đối xứng hạng nhẹ

Sử dụng các cơ chế mật mã được quy định tài TCVN 12854-4:2020 (ISO/IEC 29192-4:2013):

- Cơ chế xác thực một chiều: cryptoGPS, ELLI_193.1
- Cơ chế trao đổi khóa xác thực một chiều dựa trên mã hóa: ALIKE.
- Cơ chế ký số dựa trên định danh: IBS.

2.2.4 Bộ sinh số ngẫu nhiên

Bảng 13- Danh sách thuật toán sinh số ngẫu nhiên được phép sử dụng

STT	Thuật toán	Nguyên thủy mật mã	Năm sử dụng	Tài liệu viện dẫn
1	CTR-DRBG	AES, MKV	Năm sử dụng được tính bằng năm sử dụng của các nguyên thủy mật mã tương ứng	FIPS 192 TCVN 14263:2024 NIST SP 800-90A NIST 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			

2.3 Yêu cầu về mật mã đối với lớp mạng

a. Đối với kết nối giữa lớp thiết bị và lớp mạng: tuân thủ các yêu cầu tại mục 2.2.

b. Đối với kết nối giữa lớp mạng và lớp hỗ trợ ứng dụng và hỗ trợ dịch vụ tuân thủ theo quy định tại tiêu chuẩn về khung bảo mật cho đô thị thông minh.

c. Đối với năm sử dụng của các kỹ thuật mật mã, tuân thủ quy định tại mục 2.2.

2.4 Yêu cầu về mật mã đối với lớp hỗ trợ ứng dụng và hỗ trợ dịch vụ

Tuân thủ theo quy định tại tại tiêu chuẩn về khung bảo mật cho đô thị thông minh.

2.5 Yêu cầu về mật mã đối với lớp ứng dụng

Tuân thủ theo quy định tại tiêu chuẩn về khung bảo mật cho đô thị thông minh.

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./.