BỘ QUỐC PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 07/2026/TT-BQP

Hà Nội, ngày 20 tháng 01 năm 2026

THÔNG TƯ
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

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật số 70/2025/QH15;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Nghị định số 01/2022/NĐ-CP được sửa đổi, bổ sung bởi Nghị định số 03/2025/NĐ-CP 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 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

Căn cứ Nghị định số 22/2026/NĐ-CP của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Tiêu chuẩn và quy chuẩn kỹ thuật;

Theo đề nghị của Trưởng ban Ban Cơ yếu Chính phủ;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư 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.

Điều 1. Ban hành kèm theo Thông tư này gồm:

1. Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng (QCVN 4:2026/BQP) kèm theo Thông tư này thay thế Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng (QCVN 4:2016/BQP) ban hành kèm theo Thông tư số 161/2016/TT-BQP ngày 21 tháng 10 năm 2016 của Bộ trưởng Bộ Quốc phòng;

2. Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử tại Phụ lục ban hành kèm theo Thông tư này thay thế Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử tại Phụ lục ban hành kèm theo Thông tư số 87/2024/TT-BQP ngày 26 tháng 10 năm 2024 của Bộ trưởng Bộ Quốc phòng;

Điều 2. Sửa đổi kèm theo Thông tư này gồm:

1. Sửa đổi, bổ sung một số nội dung của Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ ban hành kèm theo Thông tư số 96/2023/TT-BQP ngày 29 tháng 11 năm 2023 của Bộ trưởng Bộ Quốc phòng (Sửa đổi 1:2026 QCVN 15:2023/BQP kèm theo Thông tư này);

2. Sửa đổi, bổ sung một số nội dung của 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 ban hành kèm theo Thông tư số 23/2022/TT-BQP ngày 04 tháng 4 năm 2022 của Bộ trưởng Bộ Quốc phòng (Sửa đổi 1:2026 QCVN 12:2022/BQP kèm theo Thông tư này).

Điều 3. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 06 tháng 3 năm 2026.

2. Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng (QCVN 4:2016/BQP) ban hành kèm theo Thông tư số 161/2016/TT-BQP ngày 21 tháng 10 năm 2016 của Bộ trưởng Bộ Quốc phòng và Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử ban hành kèm theo Thông tư số 87/2024/TT-BQP ngày 26 tháng 10 năm 2024 của Bộ trưởng Bộ Quốc phòng hết hiệu lực kể từ ngày Thông tư này có hiệu lực.

Điều 4. Tổ chức thực hiện

1. Trưởng ban Ban Cơ yếu Chính phủ có trách nhiệm theo dõi, hướng dẫn, kiểm tra, đôn đốc việc thực hiện Thông tư này.

2. Thủ trưởng các cơ quan, đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này./.

Nơi nhận:
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Đ/c Bộ trưởng (để báo cáo);
- Ban Cơ yếu Chính phủ;
- Các Cục: Pháp chế/BQP; Cơ yếu/BTTM, Tiêu chuẩn - Đo lường - Chất lượng/BTTM;
- Lưu: VT, NCTH. LTr60.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Đại tướng Nguyễn Tân Cương

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 4:2026/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

QCVN 4:2026/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số 07/2026/TT-BQP ngày 20 tháng 01 năm 2026.

QCVN 4:2026/BQP thay thế QCVN 4:2016/BQP Quy chuẩn kỹ thuật quốc gia mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng ban hành kèm theo Thông tư số 161/2016/TT-BQP ngày 21/10/2016 của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

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 thuật toán mã hóa dữ liệu dùng trong các sản phẩm, dịch vụ mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

1.2 Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các tổ chức kinh doanh, sử dụng sản phẩm, dịch vụ mật mã dân sự trong lĩnh vực ngân hàng.

1.3 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng quy chuẩn này. Trường hợp các tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất.

TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

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*".

[RFC 7801]: "*GOST R 34.12-2015: Block Cipher "Kuznyechik"*", Internet Engineering Task Force (IETF), March 2016.

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. Kỹ thuật mật mã

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

1.4.6. Mã hóa

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

1.4.7. Giải mã

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

1.4.8. Mã khối

Hệ mật đối xứng với tính chất là thuật toán mã hóa thao tác trên một khối của bản rõ, nghĩa là trên một xâu bit có độ dài xác định, kết quả cho ra một khối của bản mã.

1.4.9. Mã dòng

Hệ mật đối xứng với tính chất là thuật toán mã hóa bao gồm tổ hợp một dãy các ký tự của bản rõ với dãy các ký tự của khóa dòng, mỗi lần một ký tự, sử dụng một hàm khả nghịch.

1.4.10. Khóa

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

1.4.11. Khóa dòng

Là dãy các ký tự giả ngẫu nhiên bí mật, được sử dụng bởi các thuật toán mã hóa và giải mã của mã dòng.

1.4.12. 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.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CBC	Cipher Block Chaining Mode	Chế độ móc xích khối mã

CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC
CFB	Cipher Feedback Mode	Chế độ phản hồi bản mã
CTR	Counter Mode	Chế độ bộ đếm
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
FIPS PUB	Federal Information Processing Standards Publication	Công bố tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois
GOST	Gosudarstvennyy Standart	Tiêu chuẩn quốc gia Liên bang Nga
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm dữ liệu
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
QCVN		Quy chuẩn quốc gia Việt Nam
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF (Internet Engineering Task Force) công bố
SP	Special Publication	Ấn phẩm đặc biệt (Viện Tiêu chuẩn và Kỹ thuật quốc gia Hoa Kỳ)
TCVN		Tiêu chuẩn quốc gia
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối XTS

2 QUY ĐỊNH KỸ THUẬT

Các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng tuân thủ các quy định về thuật toán mã hóa đối xứng sau:

2.1 Quy định về thuật toán mật mã

Sử dụng thuật toán trong danh sách sau:

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

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015] [RFC 7801]

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

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

Bảng 2 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mã hóa đối xứng

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128	XTS, CTR, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
2	AES	128	XTS, CTR, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
3	Kuznyechik	256	XTS, CTR, MGM	2030
			CBC (chỉ để giải mã)	2028
CHÚ THÍCH: Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo TCVN 14263:2024.				

Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo TCVN 11367-3:2016. Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801). Các chế độ hoạt động của mã khối trong quy chuẩn này áp dụng theo TCVN 12213:2018, SP 800-38C, SP 800-38D, SP 800-38E, SP 800-38F, RFC 9058.

2.3 Quy định về an toàn trong sử dụng

– Trong bọc khóa bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: KW, KWP, CCM, GCM.

– Các khóa mật mã chỉ được sử dụng cho một mục đích, không được phép sử dụng chung khóa để mã hóa khóa và mã hóa dữ liệu.

– Đối với chế độ CBC, chỉ được phép sử dụng để giải mã dữ liệu cũ, không dùng để mã hóa dữ liệu mới.

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, dịch vụ mật mã dân sự.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp và Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 1; 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 sử dụng sản phẩm, dịch vụ mật mã dân sự có trách nhiệm đảm bảo tuân thủ quy chuẩn này và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định của pháp luật hiện hành.

4.3 Các tổ chức có hoạt động sản xuất, kinh doanh sản phẩm, dịch vụ 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 của pháp luật 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, dịch vụ 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./.

TÀI LIỆU THAM KHẢO

[1]. QCVN 4:2016/BQP "*Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng*".

[2]. 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*".

[3]. 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*".

[4]. 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*".

[5]. TCVN 11816 (ISO/IEC 10118) "*Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng*".

[6]. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "*Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác nhận thông điệp*".

[7]. ISO/IEC 27040:2015 "*Information technology - Security techniques - Storage security*".

[8]. Federal Office for Information Security, BSI TR-02102-1 *"Cryptographic Mechanisms: Recommendations and Key Lengths"*, January 2022.

[9]. National Information Assurance Partnership, *"PP-Module for File Encryption Enterprise Management v1.0"*, 2019.

[10]. Common Criteria, "*collaborative Protection Profile for USB Portable Storage Devices Version: 1.0*", January 2015.

[11]. Common Criteria, "*collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0*", September 2016.

[12]. National Institute of Standards and Technology, Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths"*, March 2019.

[13]. National Institute of Standards and Technology, Special Publication 800-132 *"Recommendation for Password-Based Key Derivation: Part 1: Storage Applications"*, December 2010.

[14]. National Institute of Standards and Technology, Special Publication 800-38E "*Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*", January 2010.

[15]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General"*, May 2020.

[16]. National Institute of Standards and Technology, Special Publication 800-56B Revision 2 *"Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography"*, March 2019.

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

[18]. 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.

[19]. National Institute of Standards and Technology, Special Publication 800-38C "*Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality"*, July 2007.

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

PHỤ LỤC

DANH MỤC TIÊU CHUẨN KỸ THUẬT MẬT MÃ ÁP DỤNG BẮT BUỘC CHO MÔ-ĐUN AN TOÀN PHẦN CỨNG TRONG HOẠT ĐỘNG ĐỊNH DANH VÀ XÁC THỰC ĐIỆN TỬ

(Kèm theo Thông tư số 07/2026/TT-BQP ngày 20 tháng 01 năm 2026 của Bộ trưởng Bộ Quốc phòng)

I. Quy định Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
Tiêu chuẩn về đặc tính kỹ thuật mật mã				
1	Mật mã đối xứng và chế độ hoạt động	TCVN 14263:2024	Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.	- Áp dụng ít nhất một trong hai tiêu chuẩn TCVN 14263:2024, TCVN 11367-3:2016 (ISO/IEC 18033-3:2010) và ít nhất một trong ba tiêu chuẩn về chế độ hoạt động của mã khối. - Sử dụng một trong các thuật toán MKV, AES, Kuznyechik. - Đối với thuật toán MKV: + Sử dụng khóa có kích thước là 128 bit, 192 bit hoặc 256 bit; + Sử dụng một trong các chế độ: CFB, OFB, GCM, CCM, CTR, XTS. - Đối với thuật toán AES: + Sử dụng khóa có kích thước là 128 bit, 192 bit hoặc 256 bit; + Sử dụng một trong các chế độ: CFB, OFB, GCM, CCM, CTR, XTS.
		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 trong CNTT.	
		RFC 7801	GOST R 34.12-2015: Block Cipher "Kuznyechik"	
		RFC 9058	Multilinear Galois Mode (MGM)	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		ISO/IEC 19772:2020	An toàn thông tin - Mã hóa có sử dụng xác thực (Information security - Authenticated encryption)	- Đối với thuật toán Kuznyechik: + Sử dụng khóa có kích thước là 256 bit; + Sử dụng một trong các chế độ: CFB, OFB, MGM, CTR.
		NIST Special Publication 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices	
2	Mật mã phi đối xứng và chữ ký số	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	Áp dụng một trong các thuật toán mật mã sau: - Đối với thuật toán RSA: + $2048 \leq nlen \leq 3072$ + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký. - Đối với thuật toán ECDSA, ECDH và ECIES: + $250 \leq nlen \leq 384$ + Áp dụng ECDH để phân phối khóa, ECDSA để ký và ECIES để mã hóa dữ liệu. - Đối với thuật toán FFDH: + $2048 \leq L \leq 3072$, + $256 \leq N \leq 384$. + Áp dụng FFDH để phân phối khóa.
		PKCS #1	RSA Cryptography Standard	
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3	Thuật toán băm	TCVN 11816-3:2017	Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng	Sử dụng một trong các thuật toán sau: SHA-256, SHA-384, SHA-512-256, SHA-512, SHA3-256, SHA3-384, SHA3-512, GOST R 34.11-2012.
		FIPS PUB 202	SHA-3 Standard: Permutation - Based Hash and Extendable - Output Functions	
		RFC 6986	GOST R 34.11-2012: Hash Function	
4	Thuật toán xác thực thông điệp	TCVN 11495-1:2016	Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC) - Phần 2: Cơ chế sử dụng hàm băm chuyên dụng.	Sử dụng một trong các thuật toán sau: HMAC-SHA-256-128, HMAC-SHA-256, HMAC-SHA-384-192, HMAC-SHA-384, HMAC-SHA-512-256, HMAC-SHA-512, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512.
		FIPS PUB 202	SHA-3 Standard: Permutation - Based Hash and Extendable-Output Functions	
5	Hàm dẫn xuất khóa	NIST SP 800-132	Recommendation for Password -Based Key Derivation Part 1: Storage Applications	Áp dụng PBKDF2, phiên bản 2.0 trở lên (nếu có).
6	Bộ tạo bit ngẫu nhiên	TCVN 12853:2020	Các kỹ thuật an toàn - Bộ tạo bit ngẫu nhiên	Áp dụng một trong bốn tiêu chuẩn và sử dụng một trong các bộ tạo bit ngẫu nhiên sau: Hash_DRBG, HMAC_DRBG, CTR_DRBG (AES), MS_DRBG, MQ_DRBG, XOR-NRBG, Oversampling-NRBG.
		NIST SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		NIST SP 800-90C	Recommendation for Random Bit Generator (RBG) Constructions	
		AIS-31	A proposal for: Functionality classes for random number generators	
7	Lưu trữ các tham số an toàn	SP800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	Các tham số an toàn phải áp dụng AES chế độ KW hoặc KWP để mã hóa khi lưu giữ trên thiết bị.
8	Giao diện lập trình ứng dụng	PKCS#11	Cryptographic Token Interface Base Specification	Phiên bản 2.2 trở lên

II. Quy định về mã HS của mô-đun an toàn phần cứng

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
1	Sản phẩm mật mã dân sự thuộc nhóm sản phẩm sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã.	- Các sản phẩm trong hệ thống PKI sử dụng mật mã bao gồm: -- Module bảo mật phần cứng HSM (Hardware Security Module): có chức năng sinh khóa mật mã, lưu trữ và quản lý khóa	8471.30.90 8471.41.90 8471.49.90 8471.80.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; đầu đọc từ tính hoặc đầu đọc quang học, máy truyền dữ liệu lên các phương tiện truyền dữ liệu dưới dạng mã hóa và máy xử lý những dữ liệu này, chưa được chi tiết hoặc ghi ở nơi khác gồm:

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
		mật mã, chứng thư số, ký và kiểm tra chữ ký số. -- PKI Token (PKI USBToken, PKI Smartcard, SimPKI): có chức năng sinh khóa mật mã, lưu trữ và quản lý khóa mật mã, chứng thư số, ký và kiểm tra chữ ký số. - Các sản phẩm có chức năng sinh khóa mật mã, quản lý hoặc lưu trữ khóa mật mã không thuộc hệ thống PKI.		- Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống; - Loại khác của hàng hóa là các bộ máy khác của máy xử lý dữ liệu tự động.

Giải thích chữ viết tắt và ký hiệu:

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC
CFB	Cipher Feedback Mode	Chế độ phản hồi bản mã
CTR	Counter Mode	Chế độ bộ đếm

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
CTR_DRBG	Counter - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
ECIES	Elliptic Curve Integrated Encryption Scheme	Lược đồ mã hóa tích hợp đường cong Elliptic
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois
GOST	Gosudarstvenny 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
HS	Harmonized Commodity Description and Coding System	Hệ thống hài hòa mô tả và mã hóa hàng hóa
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm dữ liệu
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định đa biến bậc hai
MS_DRBG	Micali-Schnorr Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định Micali-Schnorr
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
NRBG	Non-deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên bất định
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
Oversampling-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc Oversampling. Được trình bày trong tài liệu SP 800-90C của NIST.
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn xuất khóa dựa trên mật khẩu 2
PKCS	Public Key Cryptography Standards	Các tiêu chuẩn mật mã khóa công khai
QCVN		Quy chuẩn kỹ thuật quốc gia
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

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
XOR-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc XOR. Được trình bày trong tài liệu SP 800-90C của NIST.
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối XTS

Ký hiệu	Mô tả
nlen	Đối với thuật toán RSA: *nlen* là độ dài modulo theo bit; Đối với thuật toán ECDSA: *nlen* là độ dài theo bit của cấp của phần tử sinh
L	Đối với thuật toán FFDH: L là độ dài của tham số miền p theo bit
N	Đối với thuật toán FFDH: N là độ dài của tham số miền q theo bit

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

SỬA ĐỔI 1:2026 QCVN 12:2022/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ ĐẶC TÍNH KỸ THUẬT MẬT MÃ SỬ DỤNG TRONG CÁC SẢN PHẨM MẬT MÃ DÂN SỰ THUỘC NHÓM SẢN PHẨM BẢO MẬT LUỒNG IP SỬ DỤNG CÔNG NGHỆ IPSEC VÀ TLS

Amendment 1:2026 QCVN 12:2022/BQP

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

HÀ NỘI – 2026

Lời nói đầu

SỬA ĐỔI 1:2026 QCVN 12:2022/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số 07/2026/TT-BQP ngày 20 tháng 01 năm 2026.

Sửa đổi 1:2026 QCVN 12:2022/BQP chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 12:2022/BQP. Các nội dung không được nêu tại Sửa đổi 1:2026 này thì tiếp tục áp dụng QCVN 12:2022/BQP ban hành kèm theo Thông tư số 23/2022/TT-BQP ngày 04/4/2022 của Bộ trưởng Bộ Quốc phòng.

SỬA ĐỔI 1:2026 QCVN 12:2022/BQP
QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ ĐẶC TÍNH KỸ THUẬT MẬT MÃ SỬ DỤNG TRONG CÁC SẢN PHẨM MẬT MÃ DÂN SỰ THUỘC NHÓM SẢN PHẨM BẢO MẬT LUỒNG IP SỬ DỤNG CÔNG NGHỆ IPSEC VÀ TLS

Amendment 1:2026 QCVN 12:2022/BQP

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

Thay thế mục 1.3 *Tài liệu viện dẫn* như sau:

"1.3 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng quy chuẩn này. Trường hợp các tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất.

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".*

QCVN 12:2022/BQP *"Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPSec và TLS."*

TCVN 14263:2024 *"Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.*

National Institute of Standards and Technology, FIPS 186-5 *"Digital Signature standard (DSS)"*, February 2023.

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

[RFC 6986]: *"GOST R 34.11-2012: Hash Function"*, Internet Engineering Task Force (IETF), December 2013.

[RFC 7801]: *"GOST R 34.12-2015: Block Cipher "Kuznyechik"*, Internet Engineering Task Force (IETF), March 2016.

[RFC 9058]: *"Multilinear Galois Mode (MGM)"*, Internet Engineering Task Force (IETF), June 2021.

[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."

Thay thế mục 1.5 *Chữ viết tắt* như sau:

"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 header
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC

CTR	Counter Mode	Chế độ bộ đếm
CTR_DRBG	Counter - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
EC	Elliptic Curve	Đường cong Elliptic
ECDH	Elliptic Curve Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên 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
FFDH	Finite-Field Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên trường hữu hạn
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois
GOST	Gosudarstvenny 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
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định đa biến bậc hai

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
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF 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)
TLS	Transport Layer Security	Bảo mật tầng giao vận
TCVN		Tiêu chuẩn quốc gia
VPN	Virtual Private Network	Mạng riêng ảo

"

Thay thế mục 1.6 *Ký hiệu* như sau:

"1.6 Ký hiệu

Ký hiệu	**Mô tả**
nlen	Độ dài modulo theo bit hoặc độ dài theo bit của cấp của phần tử sinh
L	Đối với thuật toán FFDH: L là độ dài của tham số miền p theo bit
N	Đối với thuật toán FFDH: N là độ dài của tham số miền q theo bit

"

2 QUY ĐỊNH KỸ THUẬT

Thay thế mục 2.1 như sau:

"2.1 Quy định chung

- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ IPsec VPN chỉ được phép sử dụng giao thức trao đổi khóa IKE phiên bản 2 (IKEv2) trở lên, giao thức đóng gói ESP.

- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ TLS VPN chỉ được phép sử dụng giao thức phiên bản TLS 1.2 trở lên."

Thay thế mục 2.2.1.1 như 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	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015], [RFC 7801]

"

Thay thế mục 2.2.1.2 như sau:

"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 186-5], [SP 800-56B Rev. 2]
2	FFDH	[SP 800-56A Rev. 3], [RFC 2631], [RFC 3526], [RFC 7919]
3	ECDSA	[FIPS 186-5], [RFC 6090], [SP 800-186]
4	ECDH	[FIPS 186-5], [SP 800-56A Rev. 3], [SP 800-56C Rev. 2]
5	GOST R34.10-2012	[RFC 7091]

"

Thay thế mục 2.2.1.3 như sau:

"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	[FIPS 180-4], [TCVN 11816-3]
2	SHA3-256, SHA3-384, SHA3-512	[FIPS 202]
3	GOST R 34.11-2012	[RFC 6986]

"

Thay thế mục 2.2.2.1 như sau:

"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	MKV	128	GCM, CCM, CTR	2028
		192, 256		2030
2	AES	128	GCM, CCM, CTR	2028
		192, 256		2030
3	Kuznyechik	256	MGM, CTR	2030

CHÚ THÍCH:

Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo TCVN 14263:2024.

Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo TCVN 11367-3:2016.

Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801).

Các chế độ hoạt động của mã khối trong quy chuẩn này áp dụng theo TCVN 12213:2018, SP 800-38C, SP 800-38D, SP 800-38E, SP 800-38F, RFC 9058.

"

Thay thế mục 2.2.2.2 như sau:

"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	$2048 \leq nlen < 3072$	2028
		$nlen = 3072$	2030
2	FFDH	$2048 \leq L \leq 3072$, $256 \leq N \leq 384$	2030
3	ECDH, ECDSA	$250 \leq nlen \leq 384$	2030
4	GOST R 34.10-2012	$nlen \geq 256$	2030

CHÚ THÍCH:

Đối với RSA và ECDSA, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo FIPS 186-5.

Đối với FFDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3.

Đối với ECDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3 và NIST SP 800-56C Rev. 2.

Đối với GOST R 34.10-2012, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.10-2012 (RFC 7091).

"

Thay thế mục 2.2.2.3 như sau:

"2.2.2.3 Thuật toán băm

STT	Thuật toán	Sử dụng đến năm
1	SHA-256, SHA-384, SHA-512/256, SHA-512	2030
2	SHA3-256, SHA3-384, SHA3-512	2030
3	GOST R 34.11-2012	2030

CHÚ THÍCH:

Đối với GOST R 34.11-2012, các tiêu chuẩn cho tham số an toàn và các bộ tham số cụ thể áp dụng theo GOST R 34.11-2012 (RFC 6986).

"

Sửa đổi mục 2.2.2.4 như sau:

Điều chỉnh thời hạn sử dụng từ năm "2027" thành năm "2030".

Thay thế mục 2.3.1 như sau:

"2.3.1 Quy định về an toàn sử dụng trong giao thức IPSec

"- 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)."

Thay thế mục 2.3.2 như sau:

"- Không được phép trao đổi khóa dựa trên thuật toán Diffie-Hellman trên trường hữu hạn sử dụng khóa cố định (Static Diffie-Hellman).

- 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 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

Thay thế mục 3 như sau:

"**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 của pháp luật.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp và Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 1; 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

Thay thế Điều 4 như sau:

"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

Thay thế Điều 5 như sau:

"**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./."

PHỤ LỤC A

Thay thế Phụ lục A như sau:

"PHỤ LỤC

(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	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
01	Sản phẩm bảo mật luồng IP	Sản phẩm sử dụng công nghệ VPN có bảo mật (IPSec VPN, TLS VPN) để đảm bảo an toàn, bảo mật cho dữ liệu truyền nhận trên môi trường mạng IP. Trong đó, sử dụng các thuật toán mã hóa đối xứng, thuật toán mã hóa phi đối xứng, thuật toán ký số, hàm băm mật mã để bảo mật, xác thực các thông tin truyền nhận trên môi trường mạng IP.	8471.30.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; máy truyền dữ liệu lên các phương tiện truyền dẫn dữ liệu dưới dạng hàng hóa và máy xử lý những dữ liệu này, chưa được chi tiết hay ghi ở nơi khác gồm: - Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống.
02			8471.41.90	
03			8471.49.90	
04			8517.62.42	Thiết bị dùng cho hệ thống hữu tuyến sóng mang hoặc hệ thống hữu tuyến kỹ thuật số của hàng hóa là máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Bộ tập trung hoặc bộ dồn kênh; - Bộ điều khiển và bộ thích ứng (adaptor), kể cả cổng nối, cầu nối, bộ định tuyến và các thiết bị tương tự
05			8517.62.43	
06			8517.62.49	

				được thiết kế để kết nối với máy xử lý dữ liệu tự động thuộc nhóm 84.71; - Loại khác.
07			8517.62.51	Thiết bị truyền dẫn khác kết hợp với thiết bị thu của hàng hóa máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Thiết bị mạng nội bộ không dây; - Thiết bị phát khác dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác.
08			8517.62.53	
09			8517.62.59	
10			8517.62.61	Thiết bị truyền dẫn khác của hàng hóa máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác với loại dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác là thiết bị thu xách tay để gọi, báo hiệu hoặc nhận tin và thiết bị cảnh báo bằng tin nhắn, kể cả máy nhắn tin; - Loại khác dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác với hàng hóa thuộc nhóm 8517.62.61, 8517.62.69, 8517.62.91, 8517.62.92.
11			8517.62.69	
12			8517.62.91	
13			8517.62.92	
14			8517.62.99	

"

TÀI LIỆU THAM KHẢO

Bổ sung tài liệu sau vào mục *Tài liệu tham khảo*:

"[22] National Institute of Standards and Technology, Special Publication 800-56A Revision 3 "Recommendation for Pair-Wise Key Establishment Using Schemes Using Discrete Logarithm Cryptography", April 2018.

[23] National Institute of Standards and Technology, Special Publication 800-56C Revision 2 "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", August 2020.

[24] National Institute of Standards and Technology, Special Publication 800-186 "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters", February 2023.

[25] Federal Office for Information Security, Technical Guideline TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths". 2025.

[26] Federal Office for Information Security, Technical Guideline TR-02102-2 "Cryptographic Mechanisms: Recommendations and Key Lengths". 2025.

[27] Federal Office for Information Security, Technical Guideline TR-02102-3 "Cryptographic Mechanisms: Recommendations and Key Lengths", 2025."

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

SỬA ĐỔI 1:2026 QCVN 15:2023/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ ĐẶC TÍNH KỸ THUẬT MẬT MÃ SỬ DỤNG TRONG CÁC SẢN PHẨM MẬT MÃ DÂN SỰ THUỘC NHÓM SẢN PHẨM BẢO MẬT DỮ LIỆU LƯU GIỮ

Amendment 1:2026 QCVN 15:2023/BQP

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

HÀ NỘI – 2026

Lời nói đầu

SỬA ĐỔI 1:2026 QCVN 15:2023/BQP do Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số 07/2026/TT-BQP ngày 20 tháng 01 năm 2026.

Sửa đổi 1:2026 QCVN 15:2023/BQP chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 15:2023/BQP. Các nội dung không được nêu tại Sửa đổi 1:2026 này thì tiếp tục áp dụng QCVN 15:2023/BQP ban hành kèm theo Thông tư số 96/2023/TT-BQP ngày 29/11/2023 của Bộ trưởng Bộ Quốc phòng.

SỬA ĐỔI 1:2026 QCVN 15:2023/BQP
QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ ĐẶC TÍNH KỸ THUẬT MẬT MÃ SỬ DỤNG TRONG CÁC SẢN PHẨM MẬT MÃ DÂN SỰ THUỘC NHÓM SẢN PHẨM BẢO MẬT DỮ LIỆU LƯU GIỮ

Amendment 1:2026 QCVN 15:2023/BQP

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

1 QUY ĐỊNH CHUNG

Thay thế mục *1.3 Tài liệu viện dẫn* như sau:

"1.3 Tài liệu viện dẫn

Các Tài liệu viện dẫn sau là cần thiết cho việc áp dụng Quy chuẩn này. Trường hợp các Tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất.

QCVN 12:2022/BQP *"Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS"*.

QCVN 15:2023/BQP "*Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ*".

TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

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 11816-3:2017 (ISO/IEC 10118-3 With Amendment 1:2006) "*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 - Phần 1: Cơ chế sử dụng mã khối*".

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

National Institute of Standards and Technology, FIPS 186-5 *"Digital Signature standard (DSS)"*, February 2023.

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

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

National Institute of Standards and Technology, Special Publication 800-38E *"Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on storage Devices"*, January 2010.

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

[RFC 7801]: *"GOST R 34.12-2015: Block Cipher "Kuznyechik""*, Internet Engineering Task Force (IETF), March 2016.

[RFC 9058]: *"Multilinear Galois Mode (MGM)"*, Internet Engineering Task Force (IETF), June 2021.

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

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

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

[RFC 2631]: "*Diffie-Hellman Key Agreement Method*", Internet Engineering Task Force (IETF), June 1999.

[RFC 3526]: "*More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*", Internet Engineering Task Force (IETF), May 2003.

[RFC 7919]: "*Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)*", Internet Engineering Task Force (IETF), August 2016.

[RFC 6090]: "*Fundamental Elliptic Curve Cryptography Algorithms*", Internet Engineering Task Force (IETF), February 2011.

[RFC 6986]: "*GOST R 34.11-2012: Hash Function*", Internet Engineering Task Force (IETF), August 2013."

Thay thế mục *1.5 Chữ viết tắt* như sau:

"1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
Argon2		Tên gọi một hàm dẫn xuất khóa được thiết kế bởi Alex Biryukov, Daniel Dinu và Dmitry Khovratovich
CBC	Cipher Block Chaining Mode	Chế độ móc xích khối mã
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với mã xác thực thông báo kiểu CBC
CTR	Counter Mode	Chế độ bộ đếm
CTR_DRBG	Counter - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
EC	Elliptic Curve	Đường cong Elliptic
ECDH	Elliptic Curve Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
FFDH	Finite-Field Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên trường hữu hạn
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
FIPS PUB	Federal Information Processing Standards Publication	Công bố tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ bộ đếm kiểu Galois
GOST	Gosudarstvennyy Standart	Tiêu chuẩn quốc gia Liên bang Nga
Hash_DRBG	Hash Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên hàm băm
HDD	Hard Disk Drive	Ổ đĩa cứng
HMAC	Hashed Message Authentication Code	Mã xác thực thông báo dựa trên hàm băm

HMAC_DRBG	HMAC - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên HMAC
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm dữ liệu
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định đa biến bậc hai
MS_DRBG	Micali-Schnorr Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định Micali Schnorr
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
NRBG	Non-deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên bất định
Oversampling-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc Oversampling. Được trình bày trong tài liệu SP 800-90C của NIST
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn xuất khóa dựa trên mật khẩu 2
QCVN		Quy chuẩn kỹ thuật quốc gia
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
XOR-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc XOR, Được trình bày trong tài liệu SP 800-90C của NIST.

XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối XTS

"

Thay thế mục *1.6 Ký hiệu* như sau:

"1.6 Ký hiệu

Ký hiệu	**Mô tả**
nlen	Độ dài modulo theo bit hoặc độ dài theo bit của cấp của phần tử sinh
L	Đối với thuật toán FFDH: *L* là độ dài của tham số miền *p* theo bit
N	Đối với thuật toán FFDH: *N* là độ dài của tham số miền *q* theo bit

"

2 QUY ĐỊNH KỸ THUẬT

Thay thế Bảng 1 mục 2.1.1 bằng:

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

STT	**Thuật toán**	**Tham chiếu**
1	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015], [RFC 7801]

"

Thay thế Bảng 2 mục 2.1.2 bằng:

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

STT	**Thuật toán**	**Tham chiếu**
1	RSA	[FIPS 186-5], [SP 800-56B Rev. 2]
2	FFDH	[SP 800-56A Rev. 3], [RFC 2631], [RFC 3526], [RFC 7919]

3	ECDSA	[FIPS 186-5], [RFC 6090], [SP 800-186]
4	ECDH	[SP 800-56A Rev. 3], [SP 800-56C Rev. 2]
5	GOST R 34.10-2012	[RFC 7091]

"

Thay thế Bảng 3 mục 2.1.3 bằng:

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

STT	Thuật toán	Tham chiếu
1	SHA-256, SHA-384, SHA-512/256, SHA-512	[TCVN 11816-3], [FIPS 180-4]
2	SHA3-256, SHA3-384, SHA3-512	[FIPS 202]
3	GOST R 34.11-2012	[RFC 6986]

"

Thay thế Bảng 7 mục 2.2.1 bằng:

"Bảng 7 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với 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	MKV	128	XTS, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
2	AES	128	XTS, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028

3	Kuznyechik	256	XTS, MGM	2030
			CBC (chỉ để giải mã)	2028
CHÚ THÍCH: Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo TCVN 14263:2024. Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo TCVN 11367-3:2016. Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801). Các chế độ hoạt động của mã khối trong quy chuẩn này áp dụng theo TCVN 12213:2018, SP 800-38C, SP 800-38D, SP 800-38E, SP 800-38F, RFC 9058.				

"

Thay thế Bảng 8 mục 2.2.2 bằng:

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

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
1	RSA	$2048 \leq \text{nlen} < 3072$	2028
		$nlen = 3072$	2030
2	FFDH	$2048 \leq L \leq 3072$, $256 \leq N \leq 384$	2030
3	ECDH, ECDSA	$250 \leq nlen \leq 384$	2030
4	GOST R 34.10-2012	$nlen \geq 256$	2030
CHÚ THÍCH: Đối với RSA và ECDSA, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo FIPS 186-5. Đối với FFDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3.			

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
Đối với ECDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3 và NIST SP 800-56C Rev. 2. Đối với GOST R 34.10-2012, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.10-2012 (RFC 7091).			

"

Thay thế Bảng 9 mục 2.2.3 bằng:

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

STT	Thuật toán	Sử dụng đến năm
1	SHA-256, SHA-384, SHA-512/256, SHA-512	2030
2	SHA3-256, SHA3-384, SHA3-512	2030
3	GOST R 34.11-2012	2030
CHÚ THÍCH: Đối với GOST R 34.11-2012, các tiêu chuẩn cho tham số an toàn và các bộ tham số cụ thể áp dụng theo trong quy chuẩn này áp dụng theo GOST R 34.11-2012 (RFC 6986).		

"

Thay thế thời gian được phép sử dụng tại cột "Sử dụng đến năm" trong các bảng 10 mục 2.2.4, bảng 11 mục 2.2.5 và bảng 12 mục 2.2.6 như sau:

Sửa năm "2027" thành năm "2030".

Thay thế các quy định tại mục *2.3 Quy định về an toàn trong sử dụng* như sau:

"- Trong mã hóa/giải mã dữ liệu bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: XTS, CCM, GCM, MGM.

- Trong bọc khóa bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: KW, KWP, CCM, GCM.

- Đối với chế độ CBC, chỉ được phép sử dụng để giải mã dữ liệu cũ, không dùng để mã hóa dữ liệu mới.

- Các khóa mật mã chỉ được sử dụng cho một mục đích, không được phép sử dụng chung khóa để mã hóa khóa và mã hóa dữ liệu

- Đối với thuật toán RSA, chỉ được phép sử dụng lược đồ KTS-OAEP và KTS-KEM-KWS cho vận chuyển khóa.

- Trong mã hóa dữ liệu được truyền tải, áp dụng hai giao thức IPSec và TLS (phiên bản TLS 1.2 và TLS 1.3) để cung cấp khả năng bảo vệ bổ sung (nếu có)."

3 QUY ĐỊNH VỀ QUẢN LÝ

Thay thế Điều 3 như sau:

"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 của pháp luật.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp và Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 1; 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

Thay thế Điều 4 như sau:

"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

Bổ sung mục 5.4 vào Điều 5 như sau:

"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."

PHỤ LỤC

Thay thế bằng *Phụ lục Quy định về mã HS của sản phẩm bảo mật dữ liệu lưu giữ* bằng:

"PHỤ LỤC

(Quy định)

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

STT	Tên sản phẩm	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả hàng hóa
01	Sản phẩm bảo mật dữ liệu lưu giữ	Sản phẩm sử dụng các thuật toán mật mã, kỹ thuật mật mã để bảo vệ dữ liệu lưu giữ trên thiết bị	8523.51.11	Các thiết bị lưu trữ bền vững, thể rắn của hàng hóa là đĩa, băng, các thiết bị lưu trữ bền vững, thể rắn, "thẻ thông minh" và các phương tiện lưu trữ thông tin khác để ghi âm thanh hoặc các nội dung, hình thức thể hiện khác, đã hoặc chưa ghi, kể cả bản khuôn mẫu và bản gốc để sản xuất ghi băng đĩa, nhưng không bao gồm các sản phẩm của vật liệu ảnh hoặc điện ảnh gồm: - Loại dùng cho máy vi tính của loại chưa ghi; - Loại dùng cho máy vi tính của loại để tái tạo các hiện tượng trừ âm thanh hoặc hình ảnh; - Loại khác với hàng hóa thuộc nhóm 8523.51.11, 8523.51.21.
02			8523.51.21	
03			8523.51.99	

04			8523.52.00	- "Thẻ thông minh".
05			8525.81.10	Thiết bị phát dùng cho phát thanh sóng vô tuyến hoặc truyền hình, có hoặc không gắn với thiết bị thu hoặc ghi hoặc tái tạo âm thanh; camera truyền hình, camera kỹ thuật số và camera ghi hình ảnh gồm: - Camera ghi hình ảnh; - Camera truyền hình; - Loại khác.
06			8525.81.20	
07			8525.81.90	
08			8542.32.00	Bộ nhớ của mạch điện tử tích hợp.
09			8471.30.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; đầu đọc từ tính hoặc đầu đọc quang học, máy truyền dữ liệu lên các phương tiện truyền dữ liệu dưới dạng mã hóa và máy xử lý những dữ liệu này, chưa được chi tiết hoặc ghi ở nơi khác gồm: - Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống; - Loại khác của hàng hóa là các bộ máy khác của máy xử lý dữ liệu tự động.
10			8471.41.90	
11			8471.49.90	
12			8471.80.90	

"

TÀI LIỆU THAM KHẢO

Bổ sung tài liệu sau vào mục *Tài liệu tham khảo*:

"[11] National Institute of Standards and Technology, Special Publication 800-56A Revision 3 "Recommendation for Pair-Wise Key Establishment Using Schemes Using Discrete Logarithm Cryptography", April 2018.

[12] National Institute of Standards and Technology, Special Publication 800-56C Revision 2 "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", August 2020.

[13] National Institute of Standards and Technology, Special Publication 800-186 "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters", February 2023."

BAN CƠ YẾU CHÍNH PHỦ

THUYẾT MINH

Dự thảo Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng thay thế QCVN 4:2016/BQP

Hà Nội, 2026

MỤC LỤC

1 Tên gọi và ký hiệu của QCVN

Tên gọi: Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng thay thế QCVN 4:2016/BQP.

Ký hiệu: QCVN 4:2026/BQP.

2 Đặt vấn đề

Tình hình thực tiễn

Quy chuẩn kỹ thuật quốc gia QCVN 4:2016/BQP ban hành và có hiệu lực từ ngày 09/12/2016. Tuy nhiên trong quá trình triển khai, Cơ quan quản lý chuyên ngành nhận thấy một số hạn chế như sau:

- Ngày 31/12/2024, Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quyết định số 3480/QĐ-BKHCN về việc công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV. Đây là thuật toán mã khối riêng của Việt Nam, do Ban Cơ yếu Chính phủ nghiên cứu, xây dựng, đề xuất ban hành. Thuật toán này hiện đang được cộng đồng doanh nghiệp quan tâm, nghiên cứu và tích hợp vào sản phẩm. Tuy nhiên trong quy chuẩn kỹ thuật quốc gia ban hành kèm theo Thông tư 161/2016/TT-BQP chưa cập nhật yêu cầu sử dụng với thuật toán mã khối MKV, cần thiết phải bổ sung đáp ứng yêu cầu thực tiễn sử dụng của xã hội;

- Một số nội dung kỹ thuật (*chế độ sử dụng, thời hạn sử dụng, kích thước khối*) trong quy chuẩn hiện hành đã không còn đáp ứng được các yêu cầu an toàn theo khuyến nghị từ các tổ chức quốc tế uy tín như NIST hay BSI, đặc biệt liên quan đến chế độ sử dụng và thời hạn sử dụng của sản phẩm hoặc hệ thống. Các quy định cũ có thể dẫn đến rủi ro cao hơn trong điều kiện vận hành thực tế, không đảm bảo an toàn thông tin.

- Bên cạnh đó, tại kỳ họp thứ 9 Quốc hội Khóa XIII thông qua Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó sửa đổi khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 với quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp như sau:

"2. Thừa nhận đơn phương kết quả đánh giá sự phù hợp được quy định như sau:

a) Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước;

b) Kết quả đánh giá sự phù hợp quy định tại điểm a khoản này phải được thực hiện bởi tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài được một trong các tổ chức công nhận là thành viên ký thỏa thuận thừa nhận lẫn nhau của Tổ chức Công nhận các phòng thử nghiệm Quốc tế (ILAC), Diễn đàn Công nhận Quốc tế (IAF), Tổ chức hợp tác Công nhận khu vực Châu Á Thái Bình Dương (APAC)

đánh giá và công nhận về năng lực đáp ứng tiêu chuẩn quốc tế, tiêu chuẩn quốc gia tương ứng;

Theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp quy định tại khoản này."

Căn cứ quy định trên, để phù hợp với yêu cầu thực tiễn của quản lý chất lượng sản phẩm mật mã dân sự tại Việt Nam, dự thảo Thông tư bổ sung quy định về thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức thử nghiệm nước ngoài đối với sản phẩm mật mã dân sự.

Do đó, việc thay thế và ban hành quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng là cần thiết để khắc phục các hạn chế, nâng cao chất lượng sản phẩm MMDS, đảm bảo an toàn và đồng bộ với các văn bản pháp luật liên quan. Quy chuẩn sửa đổi đáp ứng yêu cầu thực tiễn, phù hợp với tiến bộ khoa học kỹ thuật, thúc đẩy hội nhập quốc tế, nâng cao năng lực cạnh tranh của doanh nghiệp Việt Nam và bảo vệ lợi ích người tiêu dùng, góp phần xây dựng hệ thống tiêu chuẩn hóa bền vững theo Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

Tình hình tiêu chuẩn hóa tại Việt Nam

Quy chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên quy chuẩn	Ghi chú
1	QCVN 4 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng	Ban hành kèm theo Thông tư 161/2016/TT-BQP ngày 21/10/2016
2	QCVN 5 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về chữ ký số sử dụng trong lĩnh vực ngân hàng	
3	QCVN 6 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về quản lý khóa sử dụng trong lĩnh vực ngân hàng	
4	QCVN 12 : 2022/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS	Ban hành kèm theo Thông tư 23/2022/TT-BQP ngày 04/4/2022
5	QCVN 15 : 2023/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	Ban hành kèm theo Thông tư 96/2023/TT-BQP ngày 29/11/2023

Tiêu chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên tiêu chuẩn	Ghi chú
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	
2	TCVN 7816:2007	Công nghệ thông tin – Kỹ thuật mật mã thuật toán mã dữ liệu AES	Phiên bản mới nhất TCVN 11367-3:2016
3	TCVN 7817-1:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 11770-3:2021
4	TCVN 7817-2:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng	Phiên bản mới nhất ISO/IEC 11770-2:2018
5	TCVN 7817-3:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng	Phiên bản mới nhất ISO/IEC 11770-3:2021
6	TCVN 7817-4:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 4: Cơ chế dựa trên bí mật yếu	Phiên bản mới nhất ISO/IEC 11770-4:2017
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 18014-1:2008
8	TCVN 7818-2:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 2: Cơ chế token độc lập	Phiên bản mới nhất ISO/IEC 18014-2:2021
9	TCVN 7818-3:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 3: Cơ chế tạo thẻ liên kết	Phiên bản mới nhất ISO/IEC 18014-3:2009
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	
11	TCVN 11367-1:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 1: Tổng quan	Phiên bản mới nhất ISO/IEC 18033-1:2021

12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	
13	TCVN 11367-3:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối	
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	
16	TCVN 11816-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 2: Hàm băm sử dụng mã khối n-bit.	
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	
18	TCVN 11816-4:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 4: Hàm băm sử dụng số học đồng dư	
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	
20	TCVN 11817-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng	
21	TCVN 11817-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Cơ chế sử dụng kỹ thuật chữ ký số	
22	TCVN 12214-1:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan	
23	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	
24	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	

25	TCVN 11367-5:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật mã dựa trên định danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	
27	TCVN 12212:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô đun mật mã	
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	
29	TCVN 12852-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan	
30	TCVN 12852-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Các kỹ thuật tạo đường cong elliptic	
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	
32	TCVN 12855-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 2: Các cơ chế dựa trên phân tích số nguyên	
33	TCVN 12855-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 3: Các cơ chế dựa trên bài toán Logarit rời rạc	
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ -Phần 1: Tổng quan	
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	
36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	

37	TCVN 12854-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng	
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	
39	TCVN 11817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Cơ chế sử dụng kỹ thuật tri thức không	
40	TCVN 11817-6:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Cơ chế sử dụng truyền dữ liệu thủ công	
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	
44	TCVN 13177:2020	Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mật mã và kiểm thử phù hợp các cơ chế an toàn	
45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	
47	TCVN 13178-2: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký sử dụng một nhóm khóa công khai	
48	TCVN 13178-4: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu	

49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 2: Các cơ chế dựa trên logarit rời rạc	
52	TCVN 13461-1: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 1: Tổng quan	
53	TCVN 13461-2: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 2: Các cơ chế sử dụng một khóa công khai nhóm	
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	
55	TCVN 13462-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản	
56	TCVN 13720:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Kiểm thử các mô-đun mật mã trong môi trường hoạt động,	
57	TCVN 13721:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408),	
58	TCVN 13722:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viễn sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học	
59	TCVN 13723-1:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung	
60	TCVN 13723-2:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh	

		giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)	
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với đánh giá viên theo TCVN 8709 (ISO/IEC 15408)	
62	TCVN 12197:2024	An toàn thông tin – Mã hóa có xác thực (ISO/IEC 19772:2020)	
63	TCVN 14190-1:2024	An toàn thông tin – Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học – Phần 1: Khung (ISO/IEC 19989-1:2020)	
64	TCVN 14190-2:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 2: Hiệu suất nhận dạng sinh trắc học (ISO/IEC 19989-2:2020)	
65	TCVN 14190-3:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 3: Phát hiện tấn công trình diện (ISO/IEC 19989-3:2020)	
66	TCVN 14191-1:2024	An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung (ISO/IEC 23263-1:2021)	
67	TCVN 14192-1:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-1:2019)	
68	TCVN 14192-2:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu	

		chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-2:2020)	
69	TCVN 14263:2024	Công nghệ thông tin – Kỹ thuật an toàn – Thuật toán mã khối MKV.	

Sự cần thiết xây dựng thay thế Quy chuẩn

a) Về căn cứ

- Luật An toàn thông tin mạng năm 2015, tại khoản 7 Điều 38 giao "Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự"; khoản 4 Điều 52 quy định về trách nhiệm của Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng "xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự", "quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự, quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự".

- Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó một số quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp tại khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 được sửa đổi, bổ sung, tạo điều kiện cho việc thực hiện các quy định về đánh giá sự phù hợp trong lĩnh vực mật mã dân sự. Theo đó, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước và "theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp…".

- Nghị định số 211/2025/NĐ-CP ngày 25/7/2025 của Chính phủ quy định về hoạt động mật mã dân sự và sửa đổi, bổ sung một số điều của Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử được sửa đổi, bổ sung một số điều tại Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 của Chính phủ, tại Điều 10 quy định về thừa nhận kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự "Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng xem xét,

quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước về mật mã dân sự".

b) Về mục đích

Việc xây dựng, thay thế "Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng" là rất cần thiết nhằm:

- Đảm bảo chất lượng cho các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

- Thống nhất về đặc tính kỹ thuật mật mã sử dụng sử dụng trong lĩnh vực ngân hàng.

- Là cơ sở kỹ thuật để các cơ quan quản lý tham chiếu, phục vụ công tác quản lý nhà nước về chất lượng sản phẩm mật mã sử dụng trong lĩnh vực ngân hàng.

c) Về phạm vi áp dụng

Trên cơ sở phân tích lý do và mục đích xây dựng quy chuẩn, cơ quan soạn thảo quy chuẩn nhận thấy việc xây dựng bộ chỉ tiêu kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng là rất cần thiết và phù hợp trong điều kiện hiện nay.

Quy chuẩn kỹ thuật quốc gia này thay thế QCVN 4:2016/BQP quy định mức giới hạn các đặc tính kỹ thuật mật mã của các thuật toán mã hóa dữ liệu dùng trong các sản phẩm, dịch vụ mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

3 Cơ sở xây dựng các yêu cầu kỹ thuật

Cơ sở văn bản kỹ thuật trong nước

Khi xây dựng dự thảo quy chuẩn, cơ quan soạn thảo đã tham khảo các tài liệu sau:

- Quyết định số 3480/QĐ-BKHCN ngày 31/12/2024 của Bộ trưởng Bộ Khoa học và Công nghệ công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.

- Thông tư số 161/2016/TT-BQP ngày 21/10/2016 của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

Trên cơ sở các tài liệu kỹ thuật tham khảo, cơ quan soạn thảo đã bổ sung, sửa đổi Quy chuẩn đáp ứng yêu cầu sử dụng thuật toán MKV, đáp ứng điều kiện thực tế đối với các sản phẩm đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế.

Cơ sở kinh nghiệm quốc tế

3.2.1. Cơ sở cho việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự.

Thực tiễn quốc tế cho thấy mức độ an toàn của các thuật toán mật mã và các tham số kỹ thuật liên quan có xu hướng thay đổi theo thời gian, phụ thuộc vào sự phát

triển của khoa học công nghệ và năng lực tính toán. Các thuật toán và độ dài khóa hiện đang được sử dụng có thể không còn đáp ứng yêu cầu bảo đảm an toàn thông tin trong trung và dài hạn, đặc biệt đối với các thông tin có yêu cầu bảo mật cao hoặc thời gian bảo vệ kéo dài.

Trong bối cảnh đó, nhiều quốc gia và tổ chức tiêu chuẩn hóa đã ban hành các quy định và khuyến nghị nhằm quản lý việc lựa chọn, sử dụng và thay thế các thuật toán mật mã, trên cơ sở đánh giá định kỳ mức độ an toàn và phù hợp của các giải pháp kỹ thuật. Việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự được xem là một biện pháp cần thiết nhằm hạn chế rủi ro phát sinh từ việc tiếp tục sử dụng các thuật toán hoặc tham số kỹ thuật không còn đáp ứng yêu cầu bảo mật.

Các biện pháp quản lý được áp dụng phổ biến trong thực tiễn quốc tế bao gồm:

– Quy định thời hạn sử dụng hoặc chu kỳ rà soát đối với thuật toán và độ dài khóa, làm cơ sở để các tổ chức, cá nhân chủ động cập nhật, nâng cấp hoặc thay thế các giải pháp mật mã phù hợp với mức độ nhạy cảm của thông tin được bảo vệ;

– Tham chiếu và áp dụng các tiêu chuẩn, khuyến nghị mật mã do các tổ chức tiêu chuẩn hóa uy tín ban hành (như NIST, BSI), nhằm bảo đảm sự phù hợp với thông lệ quốc tế và hạn chế nguy cơ triển khai các thuật toán hoặc tham số kỹ thuật đã được đánh giá là không còn an toàn;

– Đối với dữ liệu có mức độ nhạy cảm cao hoặc có yêu cầu bảo vệ trong thời gian dài, định hướng sử dụng các thuật toán và độ dài khóa có mức an toàn cao hơn, đáp ứng yêu cầu bảo mật trong dài hạn và có khả năng thích ứng với sự phát triển của công nghệ;

– Xây dựng lộ trình chuyển đổi phù hợp từ các thuật toán mật mã khóa công khai truyền thống sang các thuật toán mới có mức độ an toàn cao hơn, bao gồm các thuật toán có khả năng chống chịu trước các tiến bộ về năng lực tính toán, trên cơ sở đánh giá rủi ro, mức độ nhạy cảm của dữ liệu và yêu cầu quản lý nhà nước trong từng giai đoạn.

3.2.2. Rà soát, cập nhật thuật toán mật mã theo các tiêu chuẩn quốc tế mới nhất.

Bảng tổng hợp dưới đây một vài thuật toán mật mã đối xứng và các tấn công đã biết đối với từng thuật toán đó.

Thuật toán	Kích thước khóa theo bit	Kích thước khối theo bit	Các tấn công đã biết	Mô tả
AES	128, 192, 256	128	Chưa có các tấn công thám mã đã biết	Được mô tả trong FIPS 197. Đây là thuật toán mã khối công bố năm 1998 được chính phủ Mỹ làm chuẩn mã hóa, sau đó được NIST chấp thuận làm tiêu chuẩn và được sử dụng rộng rãi đến nay.
DES	56	64	Kích thước khối và khóa nhỏ, dễ bị tấn công bởi các phương pháp vét cạn, ngày sinh, vi sai, tuyến tính, khóa yếu.	Được mô tả trong FIPS 46-3. Đây là thuật toán mã khối được IBM phát triển, công bố năm 1975, và được chuẩn hóa năm 1976.
TDEA	128, 192	64	Vào năm 2016 một lỗ hổng lớn đã được phát hiện đối với thuật toán này sử dụng trong giao thức TLS, IPsec, SSH, được công bố tại CVE-2016-2183. Cuộc tấn công thực thi với thuật toán này là tấn công ngày sinh (Birthday attack).	Được mô tả trong SP 800-67. Đây là thuật toán mã khối, TDEA (còn biết đến với tên gọi Triple-DES) được công bố lần đầu năm 1981. Do lỗ hổng lớn được phát hiện nên NIST hạn chế và tiến tới loại bỏ trong các ứng dụng mới.
IDEA	128	64	Hạn chế của mã pháp này là kích thước khối nhỏ, lược đồ khóa đơn giản và chứa các lớp khóa yếu. Không có các tấn công thực tế, tuy nhiên có các tấn công lên số vòng nhỏ và khóa yếu. Tấn công tốt nhất lên IDEA là tấn công Bicliques.	Thuật toán mã khối được được thiết kế bởi James Massey của ETH Zurich và Xuejia Lai và được mô tả lần đầu tiên vào năm 1991. Thuật toán này ra đời nhằm thay cho thuật toán DES.

			• Khovratovich, Dmitry; Leurent, Gaëtan; *Rechberger*, Christian (2012). *Narrow-Bicliques: Cryptanalysis of Full IDEA. Advances in Cryptology – EUROCRYPT 2012.* Lecture Notes in Computer Science. **7237**. pp. 392–410 • Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", *Advances in Cryptology, CRYPTO 93 Proceedings*: 224–231	
RC2	40	64	Kích thước khóa quá nhỏ, kích thước khối nhỏ. Dễ tổn thương trước các dạng tấn công khác nhau.	Thuật toán mã khối được thiết kế năm 1987 bởi Ron Rivest của hãng bảo mật RSA Data Security. RC2 còn được biết đến với tên gọi ARC2.
RC5	0-2040	32, 64, 128	Tồn tại một số tấn công lên phiên bản rút gọn 12-vòng với phiên bản kích thước khối 64-bit (thám mã vi sai) với độ phức tạp 2^{44} bản rõ chọn lọc.	Thuật toán mã khối được thiết kế bởi Ronald Rivest vào năm 1994.
RC6	128, 192, 256	128	Chưa có tấn công ảnh hưởng tới phiên bản đầy đủ	Thuật toán mã khối có nguồn gốc từ RC5 và được thiết kế bởi Ron Rivest, Matt Robshaw, Ray Sidney và Yiqun Lisa Yin để đáp ứng các yêu cầu của cuộc thi Tiêu chuẩn mã hóa nâng cao (AES).

ARIA	128, 192, 256	128	• *Wenling Wu; Wentao Zhang; Dengguo Feng (2006). "Impossible Differential Cryptanalysis of ARIA and Camellia". Retrieved January 19, 2007.* • *Xuehai Tang; Bing Sun; Ruilin Li; Chao Li (March 30, 2010). "A Meet-in-the-Middle Attack on ARIA". Retrieved April 24, 2010.*	Thuật toán mã khối được thiết kế vào năm 2003 bởi một nhóm lớn các nhà nghiên cứu của Hàn Quốc. Năm 2004 thuật toán này được chuẩn hóa và sử dụng tại Hàn Quốc.
Blowfish	32-448	64	Tấn công ngày sinh (vì kích thước khối nhỏ). Tồn tại các khóa yếu.	Thuật toán mã khối do Bruce Schneier thiết kế năm 1993 như một giải pháp thay thế miễn phí, nhanh chóng cho các thuật toán mã hóa hiện có tại thời điểm đó.
Camellia	128, 192, 256	128	Được đánh giá có mức độ an toàn tương đương trong các tiêu chuẩn quốc tế.	Thuật toán mã khối được phát triển bởi Mitsubishi Electric và NTT của Nhật Bản. Được công nhận trong chuẩn ISO/IEC. Thuật toán có mức độ bảo mật và khả năng xử lý tương đương với thuật toán AES.
SEED	128	128	Chưa có các tấn công đã biết với phiên bản đầy đủ.	Thuật toán mã khối được phát triển bởi KISA (Hàn Quốc) và được công bố trong chuẩn ISO/IEC 18033-3:2010 và nhiều RFC khác (như RFC 4010, RFC 4162, RFC4196).
CAST	64	64	Kích thước khóa/khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán mã khối. Không có bản quyền, được mô tả trong RFC 2144.

CAST-128 (còn gọi là CAST5)	40-128	64	Kích thước khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán được công bố vào năm 1996 bởi Carlisle Adams và Stafford Tavares. Thuật toán này cũng đã được Cơ quan An ninh Truyền thông phê duyệt cho Chính phủ Canada sử dụng.
CAST-256 (còn gọi là CAST6)	128, 192, 256	128	Tấn công tốt nhất là tấn công tương quan không (zero-correlation) với độ phức tạp thời gian là $2^{246.9}$ và dữ liệu là $2^{98.8}$. Tấn công này không ảnh hưởng tới độ an toàn của thuật toán. Bogdanov, Andrey; Leander, Gregor; Nyberg, Kaisa; Wang, Meiqin (2012). *Integral and multidimensional linear distinguishers with correlation zero. Lecture Notes in Computer Science*. **7658**. pp. 244–261.	Thuật toán mã khối, có nguồn gốc từ CAST-128. CAST-256 được xuất bản vào 6/1998. Được thiết kế theo thiết kế "CAST" do Carlisle Adams, Stafford Tavares phát minh và Howard Heys, Michael Wiener đóng góp vào thiết kế. CAST-256 được mô tả trong RFC 2612.
SM4	128	128	Chưa có tấn công đã biết nào được công bố.	Thuật toán mã khối, nó được nhiều cơ quan đầu ngành tại Trung Quốc phát triển nhưng chủ yếu được phát triển bởi Lü Shuwang. Tháng 8/2016 được chuẩn hóa tại Trung Quốc.

Dựa vào bảng trên, có thể thấy hầu hết các thuật toán có kích thước khối 128 bit giúp hạn chế các rủi ro liên quan đến tấn công ngày sinh, phù hợp với khuyến nghị của các tổ chức quốc tế, trong đó AES là thuật toán được nhắc đến nhiều nhất trong các tài liệu của tổ chức quốc tế uy tín (NIST, BSI, ANSI), được coi là chuẩn mặc định để đánh giá độ an toàn của các thuật toán khác. Hầu hết các tài liệu kỹ thuật (Whitepaper) và cấu hình mặc định đều chỉ liệt kê AES (Advanced Encryption Standard) với các độ dài khóa 128-bit hoặc 256-bit là lựa chọn duy nhất cho mã hóa đối xứng.

Qua rà soát danh mục sản phẩm mật mã dân sự và khảo sát thị trường tại Việt Nam, cơ quan soạn thảo nhận thấy đa số sản phẩm được khảo sát có tích hợp thuật toán

mã hóa AES, hiếm thấy sản phẩm tích hợp tùy chọn các thuật toán quốc tế hoặc nội địa khác (như Camellia, CAST, SEED, SM4), các thư viện mã nguồn mở mặc định sử dụng thuật toán AES hoặc không có các tùy chọn thuật toán khác, nếu có nhu cầu sử dụng, phải tùy biến, tích hợp vào mã nguồn.

Về mặt hỗ trợ phần cứng, hầu hết các CPU hiện đại (Intel, AMD, ARM) đều có tập lệnh hỗ trợ AES-NI, giúp việc mã hóa/giải mã bằng AES có tốc độ cực nhanh mà không tốn nhiều tài nguyên. Do vậy, việc sử dụng AES là đảm bảo tính tương thích cao, tiết kiệm chi phí khi sản phẩm cần giao tiếp, phổ biến rộng rãi với hệ thống quốc tế.

Để đảm bảo tính an toàn và hội nhập cùng thế giới, các sản phẩm, dịch vụ mật mã dân sự được kinh doanh, sử dụng tại thị trường Việt Nam cần có tính an toàn, ổn định, tương thích cao, đồng thời định hướng phát triển mật mã Việt Nam đảm bảo tự chủ bền vững. Do đó, cần xây dựng quy định chặt chẽ cho việc sử dụng các thuật toán mật mã phổ biến và thuật toán mật mã của Việt Nam. Cơ quan soạn thảo đã tham khảo các khuyến nghị quốc tế về an toàn mật mã để đưa ra các sửa đổi, bổ sung phù hợp với điều kiện sử dụng sản phẩm mật mã dân sự tại Việt Nam, đảm bảo cân bằng giữa bảo mật, hiệu suất, và khả năng triển khai thực tế.

Các giải pháp này đảm bảo rằng mật mã dân sự đáp ứng được yêu cầu bảo mật ngắn hạn, đồng thời phù hợp với lộ trình cập nhật công nghệ để bảo vệ dữ liệu trong dài hạn, như đã đề cập trong các quy định của Việt Nam (QCVN 4:2016/BQP) và khuyến nghị quốc tế.

a) Đối với thuật toán TDEA

Tài liệu NIST SP 800-131A Rev 2 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) cung cấp các quy định về khuyến nghị sử dụng và lộ trình chuyển đổi đối với các thuật toán mật mã và độ dài khóa như sau:

Thuật toán	Khuyến nghị sử dụng
3TDEA cho Mã hóa	Không được chấp nhận đến năm 2023 Không được phép sau năm 2023
3TDEA cho Giải mã	Sử dụng kế thừa
AES-128 cho Mã hóa và Giải mã	Được chấp nhận
AES-192 cho Mã hóa và Giải mã	Được chấp nhận
AES-256 cho Mã hóa và Giải mã	Được chấp nhận

Tại đây NIST đặt ra giới hạn và lộ trình sử dụng thuật toán TDEA:

- Việc sử dụng đối với các biện pháp bảo vệ mật mã mới (như mã hóa, đóng gói khóa, tạo MAC) được khuyến nghị chuyển đổi trước ngày 31 tháng 12 năm 2023 và sẽ bị ngừng phê duyệt từ ngày 1 tháng 1 năm 2024.

- Tuy nhiên, TDEA vẫn được phép dùng cho chức năng giải mã, mở gói khóa và xác minh MAC đối với dữ liệu đã được bảo vệ trước đó, nhằm hỗ trợ các hệ thống kế thừa trong quá trình chuyển đổi.

Thực hiện theo lộ trình này, NIST đã công bố thông báo ngày 29 tháng 6 năm 2023 về việc rút lại NIST SP 800-67 Rev.2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, có hiệu lực từ ngày 01 tháng 01 năm 2024.

b) Đối với chế độ XTS

Chế độ XTS (XEX-based Tweaked CodeBook mode with ciphertext stealing) được thiết kế chuyên biệt cho mã hóa dữ liệu lưu giữ theo khối, đặc biệt là mã hóa ổ đĩa và vùng lưu giữ dung lượng lớn.

XTS cho phép mã hóa độc lập từng đơn vị dữ liệu (sector hoặc block), hỗ trợ hiệu quả truy cập ngẫu nhiên mà không cần duy trì trạng thái giữa các khối. Việc sử dụng tham số tweak được dẫn xuất từ chỉ số vị trí lưu giữ giúp ngăn chặn các tấn công hoán đổi khối và sao chép dữ liệu giữa các vị trí khác nhau trong không gian lưu giữ. Ngoài ra, XTS không làm thay đổi kích thước dữ liệu và không phát sinh dữ liệu phụ cho mục đích xác thực, phù hợp với các hệ thống lưu giữ hiệu năng cao.

Với các đặc tính trên, XTS hiện là chế độ được khuyến nghị rộng rãi cho mã hóa dữ liệu lưu giữ và đã được triển khai trong nhiều hệ thống thực tế.

c) Đối với chế độ KW, KWP

Trong các hệ thống bảo mật dữ liệu lưu giữ, khóa mã hóa dữ liệu không được lưu giữ ở dạng rõ ràng mà phải được bảo vệ bằng các cơ chế bọc khóa chuyên dụng. Các chế độ KW (Key Wrap) và KWP (Key Wrap with Padding) được lựa chọn nhằm bảo đảm an toàn cho quá trình lưu giữ và vận chuyển khóa mã hóa dữ liệu.

KW và KWP cung cấp cơ chế bảo vệ khóa có kiểm soát, cho phép phát hiện thay đổi trái phép và bảo đảm tính toàn vẹn của khóa được bọc. Việc sử dụng các chế độ này phù hợp với các khuyến nghị quốc tế về quản lý khóa và đáp ứng yêu cầu phân tách mục đích sử dụng khóa, theo đó khóa dùng để bọc khóa không được sử dụng cho mã hóa dữ liệu và ngược lại.

Do đó, KW và KWP giữ vai trò thiết yếu trong kiến trúc bảo mật tổng thể của các sản phẩm bảo mật dữ liệu lưu giữ, mặc dù không trực tiếp tham gia vào quá trình mã hóa dữ liệu người dùng.

d) Đối với thuật toán Kuznyechik

Đối với thuật toán Kuznyechik, chế độ XTS được cho phép sử dụng do phù hợp với mục tiêu mã hóa dữ liệu lưu giữ theo khối, đáp ứng yêu cầu bảo mật dữ liệu lưu giữ và có phạm vi áp dụng rõ ràng.

Ngoài ra, chế độ MGM là chế độ mã hóa xác thực được quy định trong hệ tiêu chuẩn GOST, được thiết kế đồng bộ với thuật toán Kuznyechik, cho phép bảo đảm

đồng thời tính bí mật và toàn vẹn dữ liệu. Việc lựa chọn MGM thay cho các chế độ AEAD khác nhằm bảo đảm tính nhất quán về hệ tiêu chuẩn và thuận lợi trong triển khai, đánh giá hợp chuẩn đối với các sản phẩm sử dụng thuật toán Kuznyechik.

Các chế độ CCM và GCM không được áp dụng cho thuật toán Kuznyechik trong Bảng 7 do không thuộc hệ chế độ được chuẩn hóa đồng bộ với thuật toán này. Việc không lựa chọn CCM và GCM đối với Kuznyechik không làm giảm mức độ an toàn của quy chuẩn, đồng thời bảo đảm tính rõ ràng, nhất quán và khả thi trong áp dụng.

e) Đối với chế độ CFB, OFB

Các chế độ CFB và OFB biến thuật toán mã hóa khối thành dạng mã hóa dòng, phụ thuộc vào trạng thái trước đó. Trong môi trường lưu giữ, các chế độ này không hỗ trợ tốt truy cập ngẫu nhiên theo khối và dễ bị ảnh hưởng bởi lỗi lan truyền hoặc các tấn công thao túng dữ liệu (bit-flipping attack) ở mức bit.

Ngoài ra, CFB và OFB không cung cấp cơ chế xác thực dữ liệu và yêu cầu quản lý chặt chẽ vector khởi tạo (IV), làm gia tăng rủi ro triển khai sai trong các hệ thống lưu giữ dung lượng lớn. Vì các lý do này, các chế độ CFB và OFB không đáp ứng được yêu cầu an toàn trong triển khai đối với một số dòng sản phẩm mật mã dân sự cụ thể (ví dụ như sản phẩm bảo mật dữ liệu lưu giữ).

f) Đối với chế độ CBC

Chế độ Cipher Block Chaining (CBC) là chế độ hoạt động truyền thống của các thuật toán mã hóa khối đối xứng như AES và Kuznyechik (GOST R 34.12-2015). Tuy nhiên, trong bối cảnh bảo mật dữ liệu lưu giữ dài hạn, chế độ CBC không còn đáp ứng đầy đủ các yêu cầu về an toàn và khả năng triển khai, do đó không được khuyến nghị sử dụng cho các hệ thống mã hóa dữ liệu lưu giữ mới.

CBC chỉ cung cấp tính bí mật mà không tích hợp cơ chế bảo đảm toàn vẹn và xác thực dữ liệu. Trong môi trường lưu giữ, điều này dẫn đến nguy cơ bị thao túng dữ liệu, bao gồm thay đổi nội dung hoặc hoán đổi các khối dữ liệu đã mã hóa mà hệ thống không thể phát hiện nếu không triển khai thêm các cơ chế bảo vệ bổ sung. Việc kết hợp CBC với các cơ chế xác thực bên ngoài làm tăng độ phức tạp triển khai và không phù hợp với yêu cầu đơn giản, tin cậy của các hệ thống lưu giữ dung lượng lớn.

Bên cạnh đó, CBC không hỗ trợ hiệu quả truy cập ngẫu nhiên theo khối và không có cơ chế ràng buộc dữ liệu với vị trí lưu giữ. Do mỗi khối dữ liệu phụ thuộc vào khối liền trước, việc giải mã hoặc cập nhật dữ liệu tại một vị trí bất kỳ trở nên kém hiệu quả. Đồng thời, chế độ này không chống được các tấn công sao chép, hoán đổi hoặc phục hồi dữ liệu ban đầu, vốn là các mối đe dọa phổ biến trong môi trường lưu giữ.

Ngoài ra, việc quản lý vector khởi tạo (IV) trong CBC gặp nhiều khó khăn trong môi trường lưu giữ dữ liệu dài hạn. Yêu cầu IV không lặp lại và được quản lý chặt chẽ khó bảo đảm trong các hệ thống có hoạt động ghi đè, sao lưu và phục hồi dữ liệu, làm gia tăng nguy cơ suy giảm mức độ an toàn.

Trên cơ sở các phân tích nêu trên và theo các khuyến nghị hiện hành, chế độ

CBC không được lựa chọn cho mã hóa dữ liệu mới. Chế độ này chỉ được dùng để giải mã dữ liệu đã được mã hóa trước đó trên hệ thống nhằm bảo đảm khả năng tương thích ngược, không khuyến nghị triển khai trong các hệ thống mới.

g) Đối với thuật toán CAMELLIA

Mặc dù được coi là một thuật toán mã hóa hiện đại và bảo mật, thuật toán Camellia dễ bị tổn thương trước các tấn công kênh kề (side-channel attacks), chẳng hạn như tấn công cache timing, và các lỗi cụ thể trong triển khai (implementation-specific flaws), tấn công phân tích lỗi (fault analysis attack). Những cuộc tấn công này khai thác sự khác biệt về thời gian hoặc đưa lỗi vào trong quá trình mã hóa để suy luận ra khóa bí mật, nhưng chúng không phải là phá vỡ thiết kế toán học cơ bản của thuật toán.

Các điểm yếu theo loại tấn công :

- Tấn công lỗi vi sai (Differential Fault Attack):

- Kẻ tấn công có thể đưa lỗi vào bản mã trong quá trình mã hóa.
- Bằng cách phân tích các bản mã bị lỗi, chúng có thể khôi phục khóa bí mật, theo ScienceDirect.com.

https://www.sciencedirect.com/science/article/abs/pii/S0164121209003331#:~:text=rights%20and%20content,Abstract,of%20software%20(cryptographic%20algorithms).

- Tấn công Cache Timing:

- Các nhà nghiên cứu đã chứng minh rằng các triển khai của Camellia dễ bị tấn công hẹn giờ bộ nhớ đệm.
- Những cuộc tấn công này khai thác thời gian cần thiết để hoàn thành các thao tác mật mã, thời gian này có thể thay đổi tùy thuộc vào phần nào của bộ nhớ đệm được sử dụng.
- Sự thành công của cuộc tấn công này phụ thuộc nhiều vào việc triển khai cụ thể, chứ không phải bản thân thuật toán, theo Cryptology ePrint Archive.

M. Joye et al. (Eds.): InfoSecHiComNet 2011, LNCS 7011, pp. 144–156, 2011.

- Phân tích vi sai (Differential Analysis) và bộ phân biệt (Distinguishers):

- Phân tích vi sai là một phương pháp tấn công phổ biến đối với các thuật toán mã hóa đối xứng.
- Mặc dù Camellia được thiết kế để chống lại các cuộc tấn công này, các nhà nghiên cứu đã phát hiện ra rằng các triển khai cụ thể có thể dễ bị tổn thương trước một số loại phân tích vi sai, chẳng hạn như những loại khai thác các đặc tính của hộp S-box.

- Các cân nhắc về bảo mật

- Tính bảo mật của Camellia phụ thuộc vào một triển khai chính xác và an toàn, giống như bất kỳ thuật toán mật mã nào khác.
- Những sai sót phổ biến như xử lý không đúng cách Vector khởi tạo (IV) trong

một số chế độ hoạt động có thể làm tổn hại nghiêm trọng đến bảo mật, ngay cả với một thuật toán mạnh, theo ghi nhận của MojoAuth.

https://mojoauth.com/compare-encryption-algorithms/chacha20-256-vs-camellia-256/

- Một số nhà nghiên cứu đã chỉ ra rằng một số lượng vòng nhất định có thể bị làm yếu trước các cuộc tấn công cụ thể, nhưng điều này thường không làm tổn hại đến bảo mật tổng thể.

Mặc dù thuật toán Camellia sở hữu thiết kế mật mã mạnh mẽ và đã được chứng minh chống lại các tấn công vét cạn và phân tích vi sai, nhưng việc đánh giá tính an toàn thực tế của nó cần xem xét hai yếu tố quan trọng: tính dễ bị tổn thương trong triển khai và tính phổ biến trên thị trường.

1. Tính dễ bị tổn thương trong triển khai: Camellia đã được chứng minh là dễ bị tổn thương trước các tấn công kênh kề (side-channel attacks), đặc biệt là tấn công cache timing. Những lỗ hổng này không phải là lỗi toán học, nhưng chúng đòi hỏi các biện pháp phòng vệ và triển khai cực kỳ cẩn thận. Việc này làm tăng độ phức tạp và nguy cơ lỗi trong quá trình tích hợp vào ứng dụng.
2. Tính phổ biến thấp: So với các tiêu chuẩn đã được chấp nhận rộng rãi và được hỗ trợ mạnh mẽ như AES (Advanced Encryption Standard), Camellia có mức độ phổ biến và sự hỗ trợ công cụ (tooling support) thấp hơn nhiều.

Do sự kết hợp của rủi ro bảo mật liên quan đến triển khai (đòi hỏi kỹ thuật chuyên sâu để vá lỗi kênh kề) và tính thiếu phổ biến (dẫn đến ít sự giám sát của cộng đồng và ít công cụ tối ưu), việc ưu tiên sử dụng Camellia so với các thuật toán đã được thiết lập tốt như AES là không thực tế.

3.3 Cơ sở thực tiễn và căn cứ thừa nhận kết quả đánh giá sự phù hợp

Công tác quản lý chất lượng sản phẩm mật mã dân sự, đánh giá chứng nhận hợp chuẩn, hợp quy sản phẩm mật mã dân sự trong nước gặp nhiều khó khăn trong quá trình triển khai do thực trạng hiện nay ở Việt Nam chưa có tổ chức thử nghiệm đạt các chứng chỉ về thử nghiệm sản phẩm mật mã dân sự và được chỉ định (ISO/IEC 17025). Các quy chuẩn kỹ thuật trong lĩnh vực mật mã dân sự tại Việt Nam được xây dựng được xây dựng trên cơ sở hài hòa với tiêu chuẩn quốc tế. Cùng với đó, đa số các sản phẩm mật mã dân sự hiện nay được nhập khẩu từ nước ngoài và đã được đánh giá bởi các tổ chức uy tín, có năng lực. Về cơ bản, đối với sản phẩm có chung tiêu chuẩn kỹ thuật, kết quả đánh giá từ các tổ chức quốc tế có năng lực được công nhận không có sai lệch, khác biệt và đảm bảo rằng việc đánh giá tuân thủ quy chuẩn là nhất quán và công bằng. Do vậy, việc chấp nhận kết quả thử nghiệm từ tổ chức được chỉ định và tổ chức nước ngoài được công nhận theo ISO/IEC 17025 trong khi điều kiện trong nước chưa thực hiện được là phù hợp để triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

4 Nội dung Quy chuẩn kỹ thuật quốc gia QCVN 4:2025/BQP

Căn cứ vào quá trình rà soát các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng đã được Ban Cơ yếu Chính phủ cấp phép; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng với thuật toán mã khối MKV; Xem xét từ những yêu cầu, khuyến nghị được nêu ra trong các tài liệu tham khảo từ các tổ chức NIST, CC, BSI, Cơ quan soạn thảo đề xuất xây dựng quy chuẩn như sau:

Nguyên tắc xây dựng nội dung

- Các tham số an toàn được lựa chọn theo các khuyến nghị của ISO/IEC, NIST, CC, BSI và các tổ chức quốc tế khác để đảm bảo an toàn và phù hợp nhất;

- Phù hợp với điều kiện thực tế đối với các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế;

- Đáp ứng được sự phát triển của công nghệ trong vòng 5 năm tới.

Nội dung Quy chuẩn kỹ thuật

Chuẩn hóa từ ngữ, thuật ngữ, bổ sung các nội dung về thuật toán MKV, lược bỏ các nội dung chi tiết của các thuật toán tại mục 1 "Quy định chung", cụ thể như sau:

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 thuật toán mã hóa dữ liệu dùng trong các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

1.2 Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các tổ chức kinh doanh, sử dụng sản phẩm, dịch vụ mật mã dân sự trong lĩnh vực ngân hàng.

1.3 Tài liệu viện dẫn

Các Tài liệu viện dẫn sau là cần thiết cho việc áp dụng quy chuẩn này. Trường hợp các tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất.

TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

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*".

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

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. Kỹ thuật mật mã

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

1.4.6. Mã hóa

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

1.4.7. Giải mã

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

1.4.8. Mã khối

Hệ mật đối xứng với tính chất là thuật toán mã hóa thao tác trên một khối của bản rõ, nghĩa là trên một xâu bit có độ dài xác định, kết quả cho ra một khối của bản mã.

1.4.9. Mã dòng

Hệ mật đối xứng với tính chất là thuật toán mã hóa bao gồm tổ hợp một dãy các ký tự của bản rõ với dãy các ký tự của khóa dòng, mỗi lần một ký tự, sử dụng một hàm khả nghịch.

1.4.10. Khóa

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

1.4.11. Khóa dòng

Là dãy các ký tự giả ngẫu nhiên bí mật, được sử dụng bởi các thuật toán mã hóa và giải mã của mã dòng.

1.4.12. 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.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CBC	Cipher Block Chaining Mode	Chế độ móc xích khối mã
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC
CFB	Cipher Feedback Mode	Chế độ phản hồi bản mã
CTR	Counter Mode	Chế độ bộ đếm
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
FIPS PUB	Federal Information Processing Standards Publication	Công bố tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois
GOST	Gosudarstvennyy Standart	Tiêu chuẩn quốc gia Liên bang Nga
KW	Key Wrap	Bọc khóa

KWP	Key Wrap with Padding	Bọc khóa với đệm dữ liệu
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
QCVN		Quy chuẩn quốc gia Việt Nam
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF (Internet Engineering Task Force) công bố
SP	Special Publication	Ấn phẩm đặc biệt (Viện Tiêu chuẩn và Kỹ thuật quốc gia Hoa Kỳ)
TCVN		Tiêu chuẩn quốc gia Việt Nam
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối XTS

2 QUY ĐỊNH KỸ THUẬT

Các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng tuân thủ các quy định về thuật toán mã hóa đối xứng sau:

2.1 Quy định về thuật toán mật mã

Sử dụng thuật toán trong danh sách sau:

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

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015] [RFC 7801]

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

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

Bảng 2 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mã hóa đối xứng

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128	XTS, CTR, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
2	AES	128	XTS, CTR, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
3	Kuznyechik	256	XTS, CTR, MGM	2030
			CBC (chỉ để giải mã)	2028
CHÚ THÍCH: Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong				

quy chuẩn này áp dụng theo TCVN 14263:2024.

Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo FIPS 197 hoặc TCVN 11367-3:2016.

Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801).

Các chế độ hoạt động của mã khối trong quy chuẩn này áp dụng theo TCVN 12213, SP 800-38C, SP 800-38D, SP 800-38E, SP 800-38F, RFC 9058.

2.3 Quy định về an toàn trong sử dụng

- Trong bọc khóa bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: KW, KWP, CCM, GCM.

- Các khóa mật mã chỉ được sử dụng cho một mục đích, không được phép sử dụng chung khóa để mã hóa khóa và mã hóa dữ liệu.

- Đối với chế độ CBC, chỉ được phép sử dụng để giải mã dữ liệu cũ, không dùng để mã hóa dữ liệu mới.

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 an toàn phục vụ quản lý theo quy định về quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 1; Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012. 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.

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 sử dụng sản phẩm, dịch vụ mật mã dân sự có trách nhiệm đảm bảo tuân thủ quy chuẩn này và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định của pháp luật hiện hành.

4.3 Các tổ chức có hoạt động sản xuất, kinh doanh sản phẩm, dịch vụ 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 của pháp luật 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, dịch vụ 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./.

6 Bảng đối chiếu nội dung QCVN với các tài liệu tham khảo

Tên nội dung	Tài liệu tham khảo	Phương án xây dựng
Bổ sung quy định đối với thuật toán MKV	TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV	Chấp nhận toàn vẹn
Dừng đề xuất sử dụng thuật toán TDEA	NIST SP 800-131A Rev.2 (2019)	Chấp nhận toàn vẹn
Bổ sung quy định về an toàn đối với các thuật toán mật mã sử dụng chế độ CBC tại bảng 2 và mục 2.3	NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode. NIST Special Publication 800-57, Recommendation for Key Management. IEEE Std 1619, Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths. Common Criteria Portal, Supporting Documents and Guidance.	Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định thuật toán Kuznyechik	RFC 7801	Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định về chế độ MGM	RFC 9058	Chấp nhận toàn vẹn
Loại bỏ thuật toán GOST R 34.10-2001	GOST R 34.10-2012 (RFC 7091)	Chấp nhận toàn vẹn
Chấp nhận kết quả thử nghiệm	Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật (2025)	Dựa theo khuyến nghị của các tổ chức

7 Đánh giá tác động áp dụng Sửa đổi QCVN

Việc triển khai thay thế *Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng* tại thời điểm này là vấn đề cấp thiết, liên quan trực tiếp đến công tác bảo đảm an toàn thông tin mạng, bảo vệ quyền riêng tư và lợi ích của người sử dụng. Quy chuẩn này áp dụng đối với các tổ chức, cá nhân sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự trong lĩnh vực ngân hàng; các tổ chức tín dụng (trừ quỹ tín dụng nhân dân cơ sở có tài sản dưới 10 tỷ đồng, tổ chức tài chính vi mô) sử dụng sản phẩm, dịch vụ mật mã dân sự.

Các đối tượng chịu tác động khi QCVN được ban hành:

- Doanh nghiệp sản xuất/kinh doanh/nhập khẩu: phải đảm bảo đáp ứng QCVN và phải chứng nhận, công bố hợp quy khi kinh doanh sản phẩm trong lĩnh vực ngân hàng tại Việt Nam.

- Người sử dụng (cơ quan, tổ chức): Mức độ ảnh hưởng thấp do là đối tượng thụ hưởng cuối cùng. Các yếu tố an toàn được đảm bảo, bảo vệ lợi ích của người dùng cuối.

7.1. Tác động đến thị trường sản phẩm

* Tác động tích cực:

- Người sử dụng cuối (đối tượng áp dụng): Tăng cảm giác an tâm và tin tưởng khi sử dụng các sản phẩm mật mã dân sự đã được công bố hợp quy. Bảo vệ quyền riêng tư và dữ liệu cá nhân của họ trước các rủi ro mất an toàn thông tin. Giảm thiểu rủi ro mất dữ liệu quan trọng và thông tin nhạy cảm. Tăng khả năng đáp ứng các yêu cầu về bảo vệ dữ liệu và quyền riêng tư từ phía khách hàng và cơ quan quản lý. Tăng cảm giác an toàn và hỗ trợ cho việc xây dựng một môi trường sống và làm việc an toàn hơn.

- Nhà sản xuất: Nâng cao uy tín và niềm tin của khách hàng thông qua việc cung cấp các sản phẩm được chứng nhận hợp quy. Các sản phẩm nội địa chất lượng cao có cơ hội tiếp cận thị trường nước ngoài có yêu cầu cao.

- Nhà phân phối và bán lẻ: Có thể sử dụng chứng nhận hợp quy của sản phẩm làm lợi thế bán hàng để thu hút khách hàng và tăng doanh số bán hàng.

- Tổ chức đánh giá sự phù hợp và cấp chứng nhận: thuận lợi trong việc triển khai công tác đánh giá chất lượng sản phẩm mật mã dân sự, giảm thời gian kiểm định, đánh giá, tránh kiểm tra chồng chéo mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Tăng chi phí: Quá trình cấp chứng nhận hợp quy và công bố hợp quy có thể đòi hỏi đầu tư lớn vào việc nâng cấp và thay đổi công nghệ, làm tăng chi phí sản xuất và phân phối các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

- Phức tạp hóa quy trình sản xuất: Việc tuân thủ các yêu cầu tại Sửa đổi Quy chuẩn có thể đòi hỏi các quy trình và thủ tục phức tạp hơn trong quá trình sản xuất, làm tăng chi phí và thời gian sản xuất.

- Giảm hiệu suất sản xuất: Tích hợp các biện pháp đảm bảo yêu cầu kỹ thuật có thể làm giảm hiệu suất sản xuất do tăng thời gian kiểm tra và thử nghiệm, cũng như việc áp dụng các quy trình kiểm soát chất lượng nghiêm ngặt hơn.

- Tăng thời gian tiến hành kiểm định và cấp chứng nhận: Quá trình đạt được chứng nhận hợp quy có thể đòi hỏi thời gian dài và tốn kém để thực hiện kiểm định, đánh giá sự phù hợp, làm trì hoãn việc tung ra thị trường và làm chậm quá trình phát triển sản phẩm mới.

7.2. Tác động đến cơ quan quản lý nhà nước chuyên ngành

* Tác động tích cực:

- Góp phần vào việc nâng cao an toàn và quản lý rủi ro trong quản lý nhà nước đối với lĩnh vực mật mã dân sự.

- Thuận lợi triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Cần hoàn thiện, nâng cao năng lực đo kiểm, đánh giá để thực hiện công tác đánh giá, cấp chứng nhận hợp quy cho sản phẩm.

- Cần hoàn thiện cơ chế hợp tác quốc tế, danh sách tổ chức được chỉ định, tổ chức quốc tế có năng lực được công nhận.

7.3. Tác động đến người sử dụng đầu cuối

- Người sử dụng đầu cuối là đối tượng được thụ hưởng tích cực khi sản phẩm được quản lý, bảo mật, đáp ứng các quy định của QCVN./.

Tài liệu tham khảo

[1]. QCVN 04:2016/BQP "*Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng*".

[2]. 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*".

[3]. 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*".

[4]. 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*".

[5]. TCVN 11816 (ISO/IEC 10118) "*Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng*".
[6]. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "*Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác nhận thông điệp*".
[7]. ISO/IEC 27040:2015 "*Information technology – Security techniques – Storage security*".
[8]. Federal Office for Information Security, BSI TR-02102-1 *"Cryptographic Mechanisms: Recommendations and Key Lengths"*, January 2022.
[9]. National Information Assurance Partnership, *"PP-Module for File Encryption Enterprise Management v1.0"*, 2019.
[10]. Common Criteria, "*collaborative Protection Profile for USB Portable Storage Devices Version: 1.0*", January 2015.
[11]. Common Criteria, "*collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0*", September 2016.
[12]. National Institute of Standards and Technology, Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths"*, March 2019.
[13]. National Institute of Standards and Technology, Special Publication 800-132 *"Recommendation for Password-Based Key Derivation: Part 1: Storage Applications"*, December 2010.
[14]. National Institute of Standards and Technology, FIPS 180-4 "*Secure Hash Standard (SHS)*", August 2015.
[15]. National Institute of Standards and Technology, FIPS 202 "*SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*", August 2015.
[16]. National Institute of Standards and Technology, Special Publication 800-38E "*Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*", January 2010.
[17]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General"*, May 2020.
[18]. National Institute of Standards and Technology, Special Publication 800-56B Revision 2 *"Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography"*, March 2019.
[19]. National Institute of Standards and Technology, Special Publication 800-38F, *"Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping"*, December 2012.
[20]. 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.

[21]. National Institute of Standards and Technology, Special Publication 800-38C "*Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*", July 2007.

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

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

[24]. Bài báo "*Argon2: the memory-hard function for password hashing and other applications*", March 2017. https://www.password-hashing.net/argon2-specs.pdf

[25]. Bài báo "*Password-Hashing Status*", George Hatzivasilis, June 2017. https://www.researchgate.net/publication/317936505_Password-Hashing_Status

[26]. Bài báo "*Towards Practical Attacks on Argon2i and Balloon Hashing*", Joel Alwen và Jeremiah Blocki, 2017. https://ieeexplore.ieee.org/document/7961977

BAN CƠ YẾU CHÍNH PHỦ

THUYẾT MINH

Dự thảo thay thế Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử

Hà Nội, 2026

MỤC LỤC

1 Tên gọi

"Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử".

2 Đặt vấn đề

2.1 Tình hình thực tiễn

Thông tư số 87/2024/TT-BQP của Bộ Quốc phòng ban hành và có hiệu lực từ ngày 11/11/2024. Tuy nhiên trong quá trình triển khai, Cơ quan quản lý chuyên ngành nhận thấy một số hạn chế như sau:

- Ngày 31/12/2024, Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quyết định số 3480/QĐ-BKHCN về việc công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV. Đây là thuật toán mã khối riêng của Việt Nam, do Ban Cơ yếu Chính phủ nghiên cứu, xây dựng, đề xuất ban hành. Thuật toán này hiện đang được cộng đồng doanh nghiệp quan tâm, nghiên cứu và tích hợp vào sản phẩm. Tuy nhiên trong các quy chuẩn kỹ thuật quốc gia, danh mục tiêu chuẩn bắt buộc áp dụng ban hành kèm theo Thông tư 96/2023/TT-BQP chưa cập nhật yêu cầu sử dụng với thuật toán mã khối MKV, cần thiết phải bổ sung đáp ứng yêu cầu thực tiễn sử dụng của xã hội;

- Một số nội dung kỹ thuật (*chế độ sử dụng, thời hạn sử dụng, kích thước khối*) trong quy chuẩn hiện hành đã không còn đáp ứng được các yêu cầu an toàn theo khuyến nghị từ các tổ chức quốc tế uy tín như NIST hay BSI, đặc biệt liên quan đến chế độ sử dụng và thời hạn sử dụng của sản phẩm hoặc hệ thống. Các quy định cũ có thể dẫn đến rủi ro cao hơn trong điều kiện vận hành thực tế, không đảm bảo an toàn thông tin.

- Bên cạnh đó, tại kỳ họp thứ 9 Quốc hội Khóa XIII thông qua Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó sửa đổi khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 với quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp như sau:

"2. Thừa nhận đơn phương kết quả đánh giá sự phù hợp được quy định như sau:

a) Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước;

b) Kết quả đánh giá sự phù hợp quy định tại điểm a khoản này phải được thực hiện bởi tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài được một trong các tổ chức công nhận là thành viên ký thỏa thuận

thừa nhận lẫn nhau của Tổ chức Công nhận các phòng thử nghiệm Quốc tế (ILAC), Diễn đàn Công nhận Quốc tế (IAF), Tổ chức hợp tác Công nhận khu vực Châu Á Thái Bình Dương (APAC) đánh giá và công nhận về năng lực đáp ứng tiêu chuẩn quốc tế, tiêu chuẩn quốc gia tương ứng;

Theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp quy định tại khoản này."

Căn cứ quy định trên, để phù hợp với yêu cầu thực tiễn của quản lý chất lượng sản phẩm mật mã dân sự tại Việt Nam, dự thảo Thông tư bổ sung quy định về thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức thử nghiệm nước ngoài đối với sản phẩm mật mã dân sự.

Do đó, việc sửa đổi Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử là cần thiết để khắc phục các hạn chế, nâng cao chất lượng sản phẩm MMDS, đảm bảo an toàn và đồng bộ với các văn bản pháp luật liên quan. Thay thế danh mục đáp ứng yêu cầu thực tiễn, phù hợp với tiến bộ khoa học kỹ thuật, thúc đẩy hội nhập quốc tế, nâng cao năng lực cạnh tranh của doanh nghiệp Việt Nam và bảo vệ lợi ích người tiêu dùng, góp phần xây dựng hệ thống tiêu chuẩn hóa bền vững theo Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

2.2 Tình hình tiêu chuẩn hóa tại Việt Nam

Quy chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên quy chuẩn	Ghi chú
1	QCVN 4 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng	Ban hành kèm theo Thông tư 161/2016/TT-BQP ngày 21/10/2016
2	QCVN 5 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về chữ ký số sử dụng trong lĩnh vực ngân hàng	
3	QCVN 6 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về quản lý khóa sử dụng trong lĩnh vực ngân hàng	
4	QCVN 12 : 2022/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS	Ban hành kèm theo Thông tư 23/2022/TT-BQP ngày 04/4/2022
5	QCVN 15 : 2023/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản	Ban hành kèm theo Thông tư

		phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	96/2023/TT-BQP ngày 29/11/2023

Tiêu chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên tiêu chuẩn	Ghi chú
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	
2	TCVN 7816:2007	Công nghệ thông tin – Kỹ thuật mật mã thuật toán mã dữ liệu AES	Phiên bản mới nhất TCVN 11367-3:2016
3	TCVN 7817-1:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 11770-3:2021
4	TCVN 7817-2:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng	Phiên bản mới nhất ISO/IEC 11770-2:2018
5	TCVN 7817-3:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng	Phiên bản mới nhất ISO/IEC 11770-3:2021
6	TCVN 7817-4:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 4: Cơ chế dựa trên bí mật yếu	Phiên bản mới nhất ISO/IEC 11770-4:2017
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 18014-1:2008
8	TCVN 7818-2:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 2: Cơ chế token độc lập	Phiên bản mới nhất ISO/IEC 18014-2:2021
9	TCVN 7818-3:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 3: Cơ chế tạo thẻ liên kết	Phiên bản mới nhất ISO/IEC 18014-3:2009
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	
11	TCVN	Công nghệ thông tin – Các kỹ thuật an toàn	Phiên bản mới

	11367-1:2016	– Thuật toán mật mã – Phần 1: Tổng quan	nhất ISO/IEC 18033-1:2021
12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	
13	TCVN 11367-3:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối	
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	
16	TCVN 11816-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 2: Hàm băm sử dụng mã khối n-bit.	
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	
18	TCVN 11816-4:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 4: Hàm băm sử dụng số học đồng dư	
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	
20	TCVN 11817-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng	
21	TCVN 11817-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Cơ chế sử dụng kỹ thuật chữ ký số	
22	TCVN 12214-	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng	

	1:2018	quan	
23	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	
24	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	
25	TCVN 11367-5:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật mã dựa trên định danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	
27	TCVN 12212:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô đun mật mã	
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	
29	TCVN 12852-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan	
30	TCVN 12852-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Các kỹ thuật tạo đường cong elliptic	
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	
32	TCVN 12855-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 2: Các cơ chế dựa trên phân tích số nguyên	
33	TCVN 12855-	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 3: Các cơ chế dựa trên bài toán	

	3:2020	Logarit rời rạc	
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ -Phần 1: Tổng quan	
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	
36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	
37	TCVN 12854-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng	
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	
39	TCVN 11817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Cơ chế sử dụng kỹ thuật tri thức không	
40	TCVN 11817-6:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Cơ chế sử dụng truyền dữ liệu thủ công	
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	
44	TCVN 13177:2020	Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mật mã và kiểm thử phù hợp các cơ chế an toàn	

45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	
47	TCVN 13178-2: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký sử dụng một nhóm khóa công khai	
48	TCVN 13178-4: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu	
49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 2: Các cơ chế dựa trên logarit rời rạc	
52	TCVN 13461-1: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 1: Tổng quan	
53	TCVN 13461-2: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 2: Các cơ chế sử dụng một khóa công khai nhóm	
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	
55	TCVN 13462-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản	
56	TCVN	Công nghệ thông tin – Các kỹ thuật an toàn	

	13720:2023	– Kiểm thử các mô-đun mật mã trong môi trường hoạt động,	
57	TCVN 13721:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408),	
58	TCVN 13722:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viễn sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học	
59	TCVN 13723-1:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung	
60	TCVN 13723-2:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)	
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với đánh giá viên theo TCVN 8709 (ISO/IEC 15408)	
62	TCVN 12197:2024	An toàn thông tin – Mã hóa có xác thực (ISO/IEC 19772:2020)	
63	TCVN 14190-1:2024	An toàn thông tin – Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học – Phần 1: Khung (ISO/IEC 19989-1:2020)	
64	TCVN 14190-2:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 2: Hiệu suất nhận dạng sinh	

		trắc học (ISO/IEC 19989-2:2020)	
65	TCVN 14190-3:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 3: Phát hiện tấn công trình diện (ISO/IEC 19989-3:2020)	
66	TCVN 14191-1:2024	An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung (ISO/IEC 23263-1:2021)	
67	TCVN 14192-1:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-1:2019)	
68	TCVN 14192-2:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-2:2020)	
69	TCVN 14263:2024	Công nghệ thông tin – Kỹ thuật an toàn – Thuật toán mã khối MKV.	

2.3 Sự cần thiết về việc thay thế danh mục

a) Về căn cứ

- Luật An toàn thông tin mạng năm 2015, tại khoản 7 Điều 38 giao "Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp

đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự"; khoản 4 Điều 52 quy định về trách nhiệm của Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng "xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự", "quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự, quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự".

- Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó một số quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp tại khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 được sửa đổi, bổ sung, tạo điều kiện cho việc thực hiện các quy định về đánh giá sự phù hợp trong lĩnh vực mật mã dân sự. Theo đó, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước và "theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp…".

- Nghị định số 211/2025/NĐ-CP ngày 25/7/2025 của Chính phủ quy định về hoạt động mật mã dân sự và sửa đổi, bổ sung một số điều của Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử được sửa đổi, bổ sung một số điều tại Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 của Chính phủ, tại Điều 10 quy định về thừa nhận kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự "Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước về mật mã dân sự".

b) Về mục đích

Việc thay thế danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử là rất cần thiết nhằm:

- Đảm bảo chất lượng cho các sản phẩm mật mã dân sự thuộc nhóm mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử.

- Thống nhất về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử trên phạm vi toàn quốc.

- Là cơ sở kỹ thuật để các cơ quan quản lý tham chiếu, phục vụ công tác quản lý nhà nước về chất lượng sản phẩm mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử sử dụng trong lĩnh vực mật mã dân sự.

c) Về phạm vi áp dụng

Giới hạn phạm vi xây dựng thay thế danh mục

Trên cơ sở phân tích lý do và mục đích sửa đổi danh mục, cơ quan soạn thảo nhận thấy việc sửa đổi, thay thế danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử là rất cần thiết và phù hợp trong điều kiện hiện nay.

Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử tại sửa đổi này thay thế cho danh mục ban hành kèm theo Thông tư 87/2024/TT-BQP của Bộ Quốc phòng ban hành ngày 26/10/2024.

3 Cơ sở xây dựng các yêu cầu kỹ thuật

3.1 Cơ sở văn bản kỹ thuật trong nước

Khi xây dựng dự thảo quy chuẩn, cơ quan soạn thảo đã tham khảo các tài liệu sau:

- Quyết định số 3480/QĐ-BKHCN ngày 31/12/2024 của Bộ trưởng Bộ Khoa học và Công nghệ công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.

- Thông tư 87/2024/TT-BQP của Bộ Quốc phòng Quy định Danh mục tiêu chuẩn kỹ thuật mật mã bắt buộc cho mô-đun an toàn phần cứng cho hoạt động định danh và xác thực điện tử ban hành ngày 26/10/2024.

Trên cơ sở các tài liệu kỹ thuật tham khảo, cơ quan soạn thảo đã bổ sung, thay thế danh mục đáp ứng yêu cầu sử dụng thuật toán MKV, đáp ứng điều kiện thực tế đối với các sản phẩm đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế.

3.2 Cơ sở kinh nghiệm quốc tế

3.2.1 Cơ sở cho việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự.

Thực tiễn quốc tế cho thấy mức độ an toàn của các thuật toán mật mã và các tham số kỹ thuật liên quan có xu hướng thay đổi theo thời gian, phụ thuộc vào sự phát triển của khoa học công nghệ và năng lực tính toán. Các thuật toán và độ dài khóa hiện đang được sử dụng có thể không còn đáp ứng yêu cầu bảo đảm an toàn thông tin trong trung và dài hạn, đặc biệt đối với các thông tin có yêu cầu bảo mật cao hoặc thời gian bảo vệ kéo dài.

Trong bối cảnh đó, nhiều quốc gia và tổ chức tiêu chuẩn hóa đã ban hành các quy định và khuyến nghị nhằm quản lý việc lựa chọn, sử dụng và thay thế các thuật toán mật mã, trên cơ sở đánh giá định kỳ mức độ an toàn và phù hợp của các giải pháp kỹ thuật. Việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự được xem là một biện pháp cần thiết nhằm hạn chế rủi ro phát sinh từ việc tiếp tục sử dụng các thuật toán hoặc tham số kỹ thuật không còn đáp ứng yêu cầu bảo mật.

Các biện pháp quản lý được áp dụng phổ biến trong thực tiễn quốc tế bao gồm:

– Quy định thời hạn sử dụng hoặc chu kỳ rà soát đối với thuật toán và độ dài khóa, làm cơ sở để các tổ chức, cá nhân chủ động cập nhật, nâng cấp hoặc thay thế các giải pháp mật mã phù hợp với mức độ nhạy cảm của thông tin được bảo vệ;

– Tham chiếu và áp dụng các tiêu chuẩn, khuyến nghị mật mã do các tổ chức tiêu chuẩn hóa uy tín ban hành (như NIST, BSI), nhằm bảo đảm sự phù hợp với thông lệ quốc tế và hạn chế nguy cơ triển khai các thuật toán hoặc tham số kỹ thuật đã được đánh giá là không còn an toàn;

– Đối với dữ liệu có mức độ nhạy cảm cao hoặc có yêu cầu bảo vệ trong thời gian dài, định hướng sử dụng các thuật toán và độ dài khóa có mức an toàn cao hơn, đáp ứng yêu cầu bảo mật trong dài hạn và có khả năng thích ứng với sự phát triển của công nghệ;

– Xây dựng lộ trình chuyển đổi phù hợp từ các thuật toán mật mã khóa công khai truyền thống sang các thuật toán mới có mức độ an toàn cao hơn, bao gồm các thuật toán có khả năng chống chịu trước các tiến bộ về năng lực tính toán, trên cơ sở đánh giá rủi ro, mức độ nhạy cảm của dữ liệu và yêu cầu quản lý nhà nước trong từng giai đoạn.

3.2.2 Rà soát, cập nhật thuật toán mật mã

Bảng tổng hợp dưới đây một vài thuật toán mật mã đối xứng và các tấn công đã biết đối với từng thuật toán đó.

Thuật toán	Kích thước khóa theo bit	Kích thước khối theo bit	Các tấn công đã biết	Mô tả
AES	128, 192, 256	128	Chưa có các tấn công thám mã đã biết	Được mô tả trong FIPS 197. Đây là thuật toán mã khối công bố năm 1998 được chính phủ Mỹ làm chuẩn mã hóa, sau đó được NIST chấp thuận làm tiêu chuẩn và được sử dụng rộng rãi đến nay.

DES	56	64	Kích thước khối và khóa nhỏ, dễ bị tấn công bởi các phương pháp vét cạn, ngày sinh, vi sai, tuyến tính, khóa yếu.	Được mô tả trong FIPS 46-3. Đây là thuật toán mã khối được IBM phát triển, công bố năm 1975, và được chuẩn hóa năm 1976.
TDEA	128, 192	64	Vào năm 2016 một lỗ hổng lớn đã được phát hiện đối với thuật toán này sử dụng trong giao thức TLS, IPsec, SSH, được công bố tại CVE-2016-2183. Cuộc tấn công thực thi với thuật toán này là tấn công ngày sinh (Birthday attack).	Được mô tả trong SP 800-67. Đây là thuật toán mã khối, TDEA (còn biết đến với tên gọi Triple-DES) được công bố lần đầu năm 1981. Do lỗ hổng lớn được phát hiện nên NIST hạn chế và tiến tới loại bỏ trong các ứng dụng mới.
IDEA	128	64	Hạn chế của mã pháp này là kích thước khối nhỏ, lược đồ khóa đơn giản và chứa các lớp khóa yếu. Không có các tấn công thực tế, tuy nhiên có các tấn công lên số vòng nhỏ và khóa yếu. Tấn công tốt nhất lên IDEA là tấn công Bicliques. • Khovratovich, Dmitry; Leurent, Gaëtan; *Rechberger*, Christian (2012). *Narrow-Bicliques: Cryptanalysis of Full IDEA. Advances in Cryptology – EUROCRYPT 2012.* Lecture Notes in Computer Science. **7237**. pp. 392–410 • Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", *Advances in Cryptology, CRYPTO 93*	Thuật toán mã khối được được thiết kế bởi James Massey của ETH Zurich và Xuejia Lai và được mô tả lần đầu tiên vào năm 1991. Thuật toán này ra đời nhằm thay cho thuật toán DES.

			Proceedings: 224–231	
RC2	40	64	Kích thước khóa quá nhỏ, kích thước khối nhỏ. Dễ tổn thương trước các dạng tấn công khác nhau.	Thuật toán mã khối được thiết kế năm 1987 bởi Ron Rivest của hãng bảo mật RSA Data Security. RC2 còn được biết đến với tên gọi ARC2.
RC5	0-2040	32, 64, 128	Tồn tại một số tấn công lên phiên bản rút gọn 12-vòng với phiên bản kích thước khối 64-bit (thám mã vi sai) với độ phức tạp 2^{44} bản rõ chọn lọc.	Thuật toán mã khối được thiết kế bởi Ronald Rivest vào năm 1994.
RC6	128, 192, 256	128	Chưa có tấn công ảnh hưởng tới phiên bản đầy đủ	Thuật toán mã khối có nguồn gốc từ RC5 và được thiết kế bởi Ron Rivest, Matt Robshaw, Ray Sidney và Yiqun Lisa Yin để đáp ứng các yêu cầu của cuộc thi Tiêu chuẩn mã hóa nâng cao (AES).
ARIA	128, 192, 256	128	• *Wenling Wu; Wentao Zhang; Dengguo Feng (2006). "Impossible Differential Cryptanalysis of ARIA and Camellia". Retrieved January 19, 2007.* • *Xuehai Tang; Bing Sun; Ruilin Li; Chao Li (March 30, 2010). "A Meet-in-the-Middle Attack on ARIA". Retrieved April 24, 2010.*	Thuật toán mã khối được thiết kế vào năm 2003 bởi một nhóm lớn các nhà nghiên cứu của Hàn Quốc. Năm 2004 thuật toán này được chuẩn hóa và sử dụng tại Hàn Quốc.
Blowfish	32-448	64	Tấn công ngày sinh (vì kích thước khối nhỏ). Tồn tại các khóa yếu.	Thuật toán mã khối do Bruce Schneier thiết kế năm 1993 như một giải pháp thay thế miễn phí, nhanh chóng cho các

				thuật toán mã hóa hiện có tại thời điểm đó.
Camellia	128, 192, 256	128	Được đánh giá có mức độ an toàn tương đương trong các tiêu chuẩn quốc tế.	Thuật toán mã khối được phát triển bởi Mitsubishi Electric và NTT của Nhật Bản. Được công nhận trong chuẩn ISO/IEC. Thuật toán có mức độ bảo mật và khả năng xử lý tương đương với thuật toán AES.
SEED	128	128	Chưa có các tấn công đã biết với phiên bản đầy đủ.	Thuật toán mã khối được phát triển bởi KISA (Hàn Quốc) và được công bố trong chuẩn ISO/IEC 18033-3:2010 và nhiều RFC khác (như RFC 4010, RFC 4162, RFC 4196).
CAST	64	64	Kích thước khóa/khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán mã khối. Không có bản quyền, được mô tả trong RFC 2144.
CAST-128 (còn gọi là CAST5)	40-128	64	Kích thước khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán được công bố vào năm 1996 bởi Carlisle Adams và Stafford Tavares. Thuật toán này cũng đã được Cơ quan An ninh Truyền thông phê duyệt cho Chính phủ Canada sử dụng.
CAST-256 (còn gọi là CAST6)	128, 192, 256	128	Tấn công tốt nhất là tấn công tương quan không (zero-correlation) với độ phức tạp thời gian là $2^{246.9}$ và dữ liệu là $2^{98.8}$. Tấn công này không ảnh hưởng tới độ an toàn của thuật toán. Bogdanov, Andrey; Leander, Gregor;	Thuật toán mã khối, có nguồn gốc từ CAST-128. CAST-256 được xuất bản vào 6/1998. Được thiết kế theo thiết kế "CAST" do Carlisle Adams, Stafford Tavares phát minh và Howard Heys, Michael Wiener đóng góp vào thiết kế.

			Nyberg, Kaisa; Wang, Meiqin (2012). *Integral and multidimensional linear distinguishers with correlation zero. Lecture Notes in Computer Science*. **7658**. pp. 244–261.	CAST-256 được mô tả trong RFC 2612.
SM4	128	128	Chưa có tấn công đã biết nào được công bố.	Thuật toán mã khối, nó được nhiều cơ quan đầu ngành tại Trung Quốc phát triển nhưng chủ yếu được phát triển bởi Lũ Shuwang. Tháng 8/2016 được chuẩn hóa tại Trung Quốc.

Dựa vào bảng trên, có thể thấy hầu hết các thuật toán có kích thước khối 128 bit giúp hạn chế các rủi ro liên quan đến tấn công ngày sinh, phù hợp với khuyến nghị của các tổ chức quốc tế, trong đó AES là thuật toán được nhắc đến nhiều nhất trong các tài liệu của tổ chức quốc tế uy tín (NIST, BSI, ANSI), được coi là chuẩn mặc định để đánh giá độ an toàn của các thuật toán khác. Hầu hết các tài liệu kỹ thuật (Whitepaper) và cấu hình mặc định đều chỉ liệt kê AES (Advanced Encryption Standard) với các độ dài khóa 128-bit hoặc 256-bit là lựa chọn duy nhất cho mã hóa đối xứng.

Qua rà soát danh mục sản phẩm mật mã dân sự và khảo sát thị trường tại Việt Nam, cơ quan soạn thảo nhận thấy đa số sản phẩm được khảo sát có tích hợp thuật toán mã hóa AES, hiếm thấy sản phẩm tích hợp tùy chọn các thuật toán quốc tế hoặc nội địa khác (như Camellia, CAST, SEED, SM4), các thư viện mã nguồn mở mặc định sử dụng thuật toán AES hoặc không có các tùy chọn thuật toán khác, nếu có nhu cầu sử dụng, phải tùy biến, tích hợp vào mã nguồn.

Về mặt hỗ trợ phần cứng, hầu hết các CPU hiện đại (Intel, AMD, ARM) đều có tập lệnh hỗ trợ AES-NI, giúp việc mã hóa/giải mã bằng AES có tốc độ cực nhanh mà không tốn nhiều tài nguyên. Do vậy, việc sử dụng AES là đảm bảo tính tương thích cao, tiết kiệm chi phí khi sản phẩm cần giao tiếp, phổ biến rộng rãi với hệ thống quốc tế.

Để đảm bảo tính an toàn và hội nhập cùng thế giới, các sản phẩm, dịch vụ mật mã dân sự được kinh doanh, sử dụng tại thị trường Việt Nam cần có tính an toàn, ổn định, tương thích cao, đồng thời định hướng phát triển mật mã nội địa đảm bảo tự chủ bền vững. Do đó, cần xây dựng quy định chặt chẽ cho việc sử dụng các thuật toán mật mã phổ biến và thuật toán mật mã của Việt Nam. Cơ quan soạn thảo đã tham khảo các khuyến nghị quốc tế về an toàn mật mã để đưa ra các sửa đổi, bổ sung phù hợp với điều kiện sử dụng sản phẩm mật mã dân sự tại Việt Nam,

đảm bảo cân bằng giữa bảo mật, hiệu suất, và khả năng triển khai thực tế. Các giải pháp này đảm bảo rằng mật mã dân sự đáp ứng được yêu cầu bảo mật ngắn hạn, đồng thời phù hợp với lộ trình cập nhật công nghệ để bảo vệ dữ liệu trong dài hạn.

a) Đối với thuật toán TDEA

Tài liệu NIST SP 800-131A Rev 2 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) cung cấp các quy định về khuyến nghị sử dụng và lộ trình chuyển đổi đối với các thuật toán mật mã và độ dài khóa như sau:

Thuật toán	Khuyến nghị sử dụng
3TDEA cho Mã hóa	Không được chấp nhận đến năm 2023 Không được phép sau năm 2023
3TDEA cho Giải mã	Sử dụng kế thừa
AES-128 cho Mã hóa và Giải mã	Được chấp nhận
AES-192 cho Mã hóa và Giải mã	Được chấp nhận
AES-256 cho Mã hóa và Giải mã	Được chấp nhận

Tại đây NIST đặt ra giới hạn và lộ trình sử dụng thuật toán TDEA:

- Việc sử dụng đối với các biện pháp bảo vệ mật mã mới (như mã hóa, đóng gói khóa, tạo MAC) được khuyến nghị chuyển đổi trước ngày 31 tháng 12 năm 2023 và sẽ bị ngừng phê duyệt từ ngày 1 tháng 1 năm 2024.

- Tuy nhiên, TDEA vẫn được phép dùng cho chức năng giải mã, mở gói khóa và xác minh MAC đối với dữ liệu đã được bảo vệ trước đó, nhằm hỗ trợ các hệ thống kế thừa trong quá trình chuyển đổi.

Thực hiện theo lộ trình này, NIST đã công bố thông báo ngày 29 tháng 6 năm 2023 về việc rút lại NIST SP 800-67 Rev.2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, có hiệu lực từ ngày 1 tháng 1 năm 2024.

b) Đối với thuật toán DSA

- Hướng dẫn kỹ thuật "TR-02102-1" của BSI trình bày khuyến nghị về kích thước khóa an toàn tối thiểu (công bố vào tháng 3 năm 2025), BSI đã nhấn mạnh rằng các thuật toán cổ điển (RSA, DSA, ECDSA, ECDH) có thể không còn đủ an toàn trước các cuộc tấn công lượng tử trong tương lai. Nhóm biên soạn tổng hợp lại khuyến nghị của BSI như sau:

STT	Thuật toán	Kích thước khóa theo bit	Năm sử dụng

1	RSA	2000	2022
		≥ 3000	2023 trở đi
2	DSA	2000	2022
		≥ 3000	2023 trở đi
4	ECDSA	≥ 250	2023 trở đi
5	ECDH	≥ 250	2023 trở đi

Ngày 03/02/2023, tổ chức NIST công bố tiêu chuẩn FIPS 186-5 Digital Signature Standard (DSS). Tiêu chuẩn này không còn chấp thuận DSA cho việc tạo chữ ký số. Tuy nhiên, DSA có thể được sử dụng để xác minh chữ ký được tạo trước ngày triển khai tiêu chuẩn này.

c) Đối với thuật toán Kuznyechik

Đối với thuật toán Kuznyechik, chế độ XTS được cho phép sử dụng do phù hợp với mục tiêu mã hóa dữ liệu lưu giữ theo khối, đáp ứng yêu cầu bảo mật dữ liệu lưu giữ và có phạm vi áp dụng rõ ràng.

Ngoài ra, chế độ MGM là chế độ mã hóa xác thực được quy định trong hệ tiêu chuẩn GOST, được thiết kế đồng bộ với thuật toán Kuznyechik, cho phép bảo đảm đồng thời tính bí mật và toàn vẹn dữ liệu. Việc lựa chọn MGM thay cho các chế độ AEAD khác nhằm bảo đảm tính nhất quán về hệ tiêu chuẩn và thuận lợi trong triển khai, đánh giá hợp chuẩn đối với các sản phẩm sử dụng thuật toán Kuznyechik.

Các chế độ CCM và GCM không được áp dụng cho thuật toán Kuznyechik trong Bảng 7 do không thuộc hệ chế độ được chuẩn hóa đồng bộ với thuật toán này. Việc không lựa chọn CCM và GCM đối với Kuznyechik không làm giảm mức độ an toàn của quy chuẩn, đồng thời bảo đảm tính rõ ràng, nhất quán và khả thi trong áp dụng.

d) Đối với chế độ XTS

Chế độ XTS (XEX-based Tweaked CodeBook mode with ciphertext stealing) được thiết kế chuyên biệt cho mã hóa dữ liệu lưu giữ theo khối, đặc biệt là mã hóa ổ đĩa và vùng lưu giữ dung lượng lớn.

XTS cho phép mã hóa độc lập từng đơn vị dữ liệu (sector hoặc block), hỗ trợ hiệu quả truy cập ngẫu nhiên mà không cần duy trì trạng thái giữa các khối. Việc sử dụng tham số tweak được dẫn xuất từ chỉ số vị trí lưu giữ giúp ngăn chặn các tấn công hoán đổi khối và sao chép dữ liệu giữa các vị trí khác nhau trong không gian lưu giữ. Ngoài ra, XTS không làm thay đổi kích thước dữ liệu và không phát

sinh overhead xác thực, phù hợp với các hệ thống lưu giữ hiệu năng cao.

Với các đặc tính trên, XTS hiện là chế độ được khuyến nghị rộng rãi cho mã hóa dữ liệu lưu giữ và đã được triển khai trong nhiều hệ thống thực tế.

e) Đối với chế độ CBC

Chế độ Cipher Block Chaining (CBC) là chế độ hoạt động truyền thống của các thuật toán mã hóa khối đối xứng như AES và Kuznyechik (GOST R 34.12-2015). Tuy nhiên, trong bối cảnh bảo mật dữ liệu lưu giữ dài hạn, chế độ CBC không còn đáp ứng đầy đủ các yêu cầu về an toàn và khả năng triển khai, do đó không được khuyến nghị sử dụng cho các hệ thống mã hóa dữ liệu lưu giữ mới.

CBC chỉ cung cấp tính bí mật mà không tích hợp cơ chế bảo đảm toàn vẹn và xác thực dữ liệu. Trong môi trường lưu giữ, điều này dẫn đến nguy cơ bị thao túng dữ liệu, bao gồm thay đổi nội dung hoặc hoán đổi các khối dữ liệu đã mã hóa mà hệ thống không thể phát hiện nếu không triển khai thêm các cơ chế bảo vệ bổ sung. Việc kết hợp CBC với các cơ chế xác thực bên ngoài làm tăng độ phức tạp triển khai và không phù hợp với yêu cầu đơn giản, tin cậy của các hệ thống lưu giữ dung lượng lớn.

Bên cạnh đó, CBC không hỗ trợ hiệu quả truy cập ngẫu nhiên theo khối và không có cơ chế ràng buộc dữ liệu với vị trí lưu giữ. Do mỗi khối dữ liệu phụ thuộc vào khối liền trước, việc giải mã hoặc cập nhật dữ liệu tại một vị trí bất kỳ trở nên kém hiệu quả. Đồng thời, chế độ này không chống được các tấn công sao chép, hoán đổi hoặc phục hồi dữ liệu ban đầu, vốn là các mối đe dọa phổ biến trong môi trường lưu giữ.

Ngoài ra, việc quản lý vector khởi tạo (IV) trong CBC gặp nhiều khó khăn trong môi trường lưu giữ dữ liệu dài hạn. Yêu cầu IV không lặp lại và được quản lý chặt chẽ khó bảo đảm trong các hệ thống có hoạt động ghi đè, sao lưu và phục hồi dữ liệu, làm gia tăng nguy cơ suy giảm mức độ an toàn.

Trên cơ sở các phân tích nêu trên và theo các khuyến nghị hiện hành, chế độ CBC không được lựa chọn cho mã hóa dữ liệu mới. Chế độ này chỉ được dùng để giải mã dữ liệu đã được mã hóa trước đó trên hệ thống nhằm bảo đảm khả năng tương thích ngược, không khuyến nghị triển khai trong các hệ thống mới.

f) Đối với thuật toán băm

- Theo hướng dẫn kỹ thuật "TR-02102-1" của BSI các cơ chế băm được khuyến nghị trong tài liệu này đều có độ dài mã băm (digest length) $\geq$ 256 bit, tuy nhiên đối với các ứng dụng yêu cầu bảo mật cao, dài hạn, hoặc các hệ thống có tuổi thọ dài, nên sử dụng các hàm băm có đầu ra ít nhất 384 bit.

- Năm 2012, Liên bang Nga ban hành tiêu chuẩn GOST R 34.11-2012 (còn

gọi là Streebog) để thay thế GOST R 34.11-94, nhằm nâng cao cường độ bảo mật cho thuật toán hàm băm mật mã, khắc phục các hạn chế về độ mạnh toán học và khả năng chống tấn công của phiên bản cũ (theo RFC 6986 và các chỉ đạo từ Cơ quan Tiêu chuẩn Kỹ thuật Nga - Rosstandart).

3.3 Cơ sở thực tiễn và căn cứ thừa nhận kết quả đánh giá sự phù hợp

Công tác quản lý chất lượng sản phẩm mật mã dân sự, đánh giá chứng nhận hợp chuẩn, hợp quy sản phẩm mật mã dân sự trong nước gặp nhiều khó khăn trong quá trình triển khai do thực trạng hiện nay ở Việt Nam chưa có tổ chức thử nghiệm đạt các chứng chỉ về thử nghiệm sản phẩm mật mã dân sự và được chỉ định (ISO/IEC 17025). Các quy chuẩn kỹ thuật trong lĩnh vực mật mã dân sự tại Việt Nam được xây dựng được xây dựng trên cơ sở hài hòa với tiêu chuẩn quốc tế. Cùng với đó, đa số các sản phẩm mật mã dân sự hiện nay được nhập khẩu từ nước ngoài và đã được đánh giá bởi các tổ chức uy tín, có năng lực. Về cơ bản, đối với sản phẩm có chung tiêu chuẩn kỹ thuật, kết quả đánh giá từ các tổ chức quốc tế có năng lực được công nhận không có sai lệch, khác biệt và đảm bảo rằng việc đánh giá tuân thủ quy chuẩn là nhất quán và công bằng. Do vậy, việc chấp nhận kết quả thử nghiệm từ tổ chức được chỉ định và tổ chức nước ngoài được công nhận theo ISO/IEC 17025 trong khi điều kiện trong nước chưa thực hiện được là phù hợp để triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

4 Nội dung thay thế danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử

Căn cứ vào quá trình rà soát các sản phẩm mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử đang lưu thông trong nước; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng với thuật toán mã khối MKV; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng các thuật toán mật mã nhằm bảo đảm an toàn thông tin trong bối cảnh xuất hiện các nguy cơ từ máy tính lượng tử; Căn cứ vào tình hình triển khai thực tế của các quy chuẩn kỹ thuật hiện hành và định hướng chuyển đổi sang các thuật toán mật mã hậu lượng tử; Căn cứ vào tình hình triển khai thực tế của tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng; Xem xét từ những yêu cầu, khuyến nghị được nêu ra trong các tài liệu tham khảo từ tổ chức NIST, CC, BSI. Cơ quan soạn thảo đề xuất như sau:

4.1 Nguyên tắc xây dựng nội dung

- Các tham số an toàn được lựa chọn theo các khuyến nghị của ISO/IEC, NIST, CC, BSI và các tổ chức quốc tế khác để đảm bảo an toàn và phù hợp;

- Phù hợp với điều kiện thực tế đối với các sản phẩm mật mã dân sự thuộc nhóm sản phẩm mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại

phổ biến của quốc tế;

- Đáp ứng được sự phát triển của công nghệ trong vòng 5 năm tới.

4.2 Bổ sung quy định đối với thuật toán MKV

- Bổ sung tại Mục I.1 Mật mã đối xứng và chế độ hoạt động:

+ Ký hiệu tiêu chuẩn: TCVN 14263:2024

+ Tên đầy đủ của tiêu chuẩn: Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.

+ Quy định áp dụng:

"- Đối với thuật toán MKV:

+ Sử dụng khóa có kích thước là 128 bit, 192 bit hoặc 256 bit;

+ Sử dụng một trong các chế độ: CFB, OFB, GCM, CCM, CTR, XTS."

- Tại mục II:

+ Bổ sung chữ viết tắt như sau:

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
MKV		Mã khối Việt Nam

4.3 Sửa đổi quy định áp dụng đối với Mật mã đối xứng và chế độ hoạt động

- Bổ sung quy định đối với thuật toán MKV tại mục I.1.

- Loại bỏ thuật toán TDEA khỏi danh mục.

- Loại bỏ chế độ CBC đối với thuật toán AES tại mục Quy định áp dụng;

- Bổ sung Quy định áp dụng:

"- Đối với thuật toán Kuznyechik:

+ Sử dụng khóa có kích thước là 256 bit;

+ Sử dụng một trong các chế độ: CFB, OFB, MGM, CTR."

- Bổ sung Ký hiệu tiêu chuẩn: RFC 7801, RFC 9058;

- Bổ sung Tên đầy đủ của tiêu chuẩn: GOST R 34.12-2015: Block Cipher "Kuznyechik", Multilinear Galois Mode (MGM).

4.4 Sửa đổi quy định áp dụng đối với Mật mã phi đối xứng và chữ ký số

- Đối với thuật toán RSA:

+ Sửa đổi kích thước tham số theo bit từ $nlen \geq 2048$ thành $2048 \leq nlen \leq 3072$.

- Bổ sung thuật toán ECDH, ECIES.

- Đối với thuật toán ECDH, ECDSA và ECIES:

+ Sửa đổi kích thước tham số theo bit từ nlen ≥ 256 thành 250 ≤ nlen ≤ 384.

- Đổi tên thuật toán DH thành FFDH.

+ Sửa đổi kích thước tham số theo bit từ L ≥ 3072, N ≥ 256 thành 2048 ≤ L ≤ 3072, 256 ≤ N ≤ 384.

- Loại bỏ thuật toán DSA ra khỏi danh mục.

4.5 Bổ sung Quy định áp dụng đối với thuật toán băm

Bổ sung tại Mục I.3:

- Ký hiệu tiêu chuẩn: RFC 6986;

- Tên đầy đủ của tiêu chuẩn: GOST R 34.11-2012: Hash Function;

- Quy định áp dung: bổ sung thuật toán băm: GOST R 34.11-2012.

4.6 Bổ sung, thay thế Giải thích chữ viết tắt và ký hiệu

- Thay thế như sau:

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC
CFB	Cipher Feedback Mode	Chế độ phản hồi bản mã
CTR	Counter Mode	Chế độ bộ đếm
CTR_DRBG	Counter - Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định dựa trên bộ đếm
DRBG	Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
ECIES	Elliptic Curve Integrated Encryption Scheme	Lược đồ mã hóa tích hợp đường cong Elliptic
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois
GOST	Gosudarstvenny Standart	Tiêu chuẩn quốc gia Liên bang

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
		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
HS	Harmonized Commodity Description and Coding System	Hệ thống hài hòa mô tả và mã hóa hàng hóa
KW	Key Wrap	Bọc khóa
KWP	Key Wrap with Padding	Bọc khóa với đệm dữ liệu
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định đa biến bậc hai
MS_DRBG	Micali-Schnorr Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định Micali-Schnorr
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
NRBG	Non-deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên bất định
OFB	Output Feedback Mode	Chế độ phản hồi đầu ra
Oversampling-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc Oversampling. Được trình bày trong tài liệu SP 800-90C của NIST.
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn xuất khóa dựa trên mật khẩu 2

Chữ viết tắt	Tên tiếng Anh	Tên tiếng Việt
PKCS	Public Key Cryptography Standards	Các tiêu chuẩn mật mã khóa công khai
QCVN		Quy chuẩn kỹ thuật quốc gia
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
XOR-NRBG		Bộ tạo bit ngẫu nhiên bất định theo cấu trúc XOR. Được trình bày trong tài liệu SP 800-90C của NIST.
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối XTS

4.7 Cập nhật quy định về mã HS của mô-đun an toàn phần cứng

Tại mục II, cập nhật bố cục và nội dung theo Nghị định số 211/2025/NĐ-CP ngày 25/7/2025 của Chính phủ, như sau:

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
1	Sản phẩm mật mã dân sự thuộc nhóm sản phẩm sinh khóa mật mã, quản lý hoặc lưu giữ khóa mật mã.	- Các sản phẩm trong hệ thống PKI sử dụng mật mã bao gồm: -- Module bảo mật phần cứng HSM (Hardware Security Module):	8471.30.90 8471.41.90 8471.49.90 8471.80.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; đầu đọc từ tính hoặc đầu đọc quang học, máy truyền dữ liệu lên các phương tiện truyền dữ liệu dưới dạng mã hóa và máy xử

STT	Tên sản phẩm, hàng hóa theo quy định của Thông tư	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
		có chức năng sinh khóa mật mã, lưu giữ và quản lý khóa mật mã, chứng thư số, ký và kiểm tra chữ ký số. -- PKI Token (PKI USBToken, PKI Smartcard, SimPKI): có chức năng sinh khóa mật mã, lưu giữ và quản lý khóa mật mã, chứng thư số, ký và kiểm tra chữ ký số. - Các sản phẩm có chức năng sinh khóa mật mã, quản lý hoặc lưu giữ khóa mật mã không thuộc hệ thống PKI.		lý những dữ liệu này, chưa được chi tiết hoặc ghi ở nơi khác gồm: - Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống; - Loại khác của hàng hóa là các bộ máy khác của máy xử lý dữ liệu tự động.

5 Bảng đối chiếu nội dung QCVN với các tài liệu tham khảo

Tên nội dung	Tài liệu tham khảo	Phương án xây dựng
Bổ sung quy định đối với thuật toán MKV	TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV"	Chấp nhận toàn vẹn
Bổ sung quy định đối với thuật toán	RFC 7801: GOST R 34.12-2015: Block Cipher "Kuznyechik";	Chấp nhận toàn vẹn

Kuznyechik	RFC 9058: Multilinear Galois Mode (MGM)	
Loại bỏ thuật toán TDEA	NIST SP 800-131A Rev.2 (2019)	Chấp nhận toàn vẹn
Loại bỏ việc sử dụng chế độ CBC đối với thuật toán AES	https://supportportal.juniper.net/s/article/End-of-support-for-cipher-suites-using-the-CBC-mode. https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode. https://cryptography.io/en/3.4.3/hazmat/primitives/symmetric-encryption.html https://www.mdpi.com/2227-7390/13/9/1383 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10184306 https://learn.microsoft.com/en-us/security-updates/securityadvisories/2018/4338110 https://www.mdpi.com/2079-3197/8/2/51 https://blog.ise.io/blog/the-dangers-of-cbc-mode	Dựa theo khuyến nghị của các tổ chức
Loại bỏ thuật toán DSA	FIPS 186-5	Căn cứ theo khuyến nghị của tổ chức NIST
Bổ sung quy định thuật toán RSA	FIPS 186-5; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, NIST SP 800-56B Rev. 2	Căn cứ ngưỡng dưới của quy định đối với các sản phẩm mật mã thuộc phạm vi bí mật nhà nước; Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định thuật toán FFDH	NIST SP 800-56A Rev. 3; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, NIST SP 800-56C Rev. 2, RFC 2631, RFC 3526, RFC 7919	
Bổ sung quy định thuật toán ECDH	NIST SP 800-186, NIST SP 800-56A Rev. 3; NIST SP 800-56C Rev. 2; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Bổ sung quy định thuật toán ECDSA	FIPS 186-5; NIST SP 800-186, TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, RFC 6090	
Bổ sung quy	NIST SP 800-186, NIST SP 800-56A Rev. 3;	

định thuật toán ECIES	NIST SP 800-56C Rev. 2; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Bổ sung thuật toán băm R34.11-2012	RFC 6986 GOST R 34.11-2012: Hash Function	Chấp nhận toàn vẹn
Chấp nhận kết quả thử nghiệm	Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật (2025)	Dựa theo khuyến nghị của các tổ chức
Cập nhật mã HS tại Phụ lục	Nghị định 211/2025/NĐ-CP	Chấp nhận toàn vẹn

6 Đánh giá tác động áp dụng thay thế danh mục tiêu chuẩn kỹ thuật

Việc triển khai sửa đổi Danh mục tiêu chuẩn kỹ thuật đối với các mô-đun an toàn phần cứng phục vụ định danh và xác thực điện tử tại thời điểm này là vấn đề cấp thiết, liên quan trực tiếp đến công tác bảo đảm an toàn thông tin mạng, bảo vệ quyền riêng tư và lợi ích của người sử dụng trong bối cảnh chuyển đổi số quốc gia.

Quy định này áp dụng đối với các tổ chức, cá nhân sản xuất, kinh doanh, nhập khẩu và sử dụng thiết bị HSM để bảo vệ các hệ thống xác thực và thông tin không thuộc phạm vi bí mật nhà nước

Các đối tượng chịu tác động khi QCVN được ban hành:

- Doanh nghiệp sản xuất/kinh doanh/nhập khẩu và các đơn vị cung cấp dịch vụ tin cậy (CA, TVAN): Phải đảm bảo thiết bị đáp ứng các tiêu chuẩn kỹ thuật mới trong Danh mục và phải chứng nhận, công bố hợp quy khi kinh doanh hoặc vận hành sản phẩm tại thị trường Việt Nam.

- Người sử dụng (cơ quan, tổ chức, người tiêu dùng): Mức độ ảnh hưởng trực tiếp thấp do là đối tượng thụ hưởng cuối cùng của hạ tầng xác thực an toàn

6.1 Tác động đến thị trường sản phẩm

* Tác động tích cực:

- Người sử dụng cuối (đối tượng áp dụng): Tăng cảm giác an tâm và tin tưởng khi sử dụng các sản phẩm mật mã dân sự đã được công bố hợp quy. Bảo vệ quyền riêng tư và dữ liệu cá nhân của họ trước các rủi ro mất an toàn thông tin. Giảm thiểu rủi ro mất dữ liệu quan trọng và thông tin nhạy cảm; Giảm thiểu rủi ro lộ lọt khóa bí mật và thông tin nhạy cảm trong giao dịch điện tử.

- Nhà sản xuất: Nâng cao uy tín và niềm tin của khách hàng thông qua việc cung cấp các sản phẩm được chứng nhận hợp quy. Các sản phẩm nội địa chất

lượng cao có cơ hội tiếp cận thị trường nước ngoài có yêu cầu cao.

- Nhà phân phối và bán lẻ: Có thể sử dụng chứng nhận hợp quy của sản phẩm làm lợi thế bán hàng để thu hút khách hàng và tăng doanh số bán hàng.

- Tổ chức đánh giá sự phù hợp và cấp chứng nhận: thuận lợi trong việc triển khai công tác đánh giá chất lượng sản phẩm mật mã dân sự, giảm thời gian kiểm định, đánh giá, tránh kiểm tra chồng chéo mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Tăng chi phí: Quá trình cấp chứng nhận hợp quy và công bố hợp quy có thể đòi hỏi đầu tư lớn vào việc nâng cấp và thay đổi công nghệ, làm tăng chi phí sản xuất và phân phối các sản phẩm bảo mật dữ liệu lưu giữ.

- Phức tạp hóa quy trình sản xuất: Việc tuân thủ các yêu cầu kỹ thuật mới trong Danh mục sửa đổi có thể đòi hỏi các quy trình quản lý khóa và sản xuất phần cứng phức tạp hơn, làm tăng chi phí và thời gian sản xuất.

- Giảm hiệu suất sản xuất: Tích hợp các biện pháp đảm bảo yêu cầu kỹ thuật có thể làm giảm hiệu suất sản xuất do tăng thời gian kiểm tra và thử nghiệm, cũng như việc áp dụng các quy trình kiểm soát chất lượng nghiêm ngặt hơn.

- Tăng thời gian tiến hành kiểm định và cấp chứng nhận: Quá trình đạt được chứng nhận hợp quy có thể đòi hỏi thời gian dài và tốn kém để thực hiện kiểm định, đánh giá sự phù hợp, làm trì hoãn việc tung ra thị trường và làm chậm quá trình phát triển sản phẩm mới.

6.2 Tác động đến cơ quan quản lý nhà nước chuyên ngành

* Tác động tích cực:

- Góp phần vào việc nâng cao an toàn và quản lý rủi ro trong quản lý nhà nước đối với lĩnh vực mật mã dân sự.

- Thuận lợi triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Cần hoàn thiện, nâng cao năng lực đo kiểm, đánh giá để thực hiện công tác đánh giá, cấp chứng nhận hợp quy cho sản phẩm.

- Cần hoàn thiện cơ chế hợp tác quốc tế, danh sách tổ chức được chỉ định, tổ chức quốc tế có năng lực được công nhận.

6.3 Tác động đến người sử dụng đầu cuối

Người sử dụng đầu cuối là đối tượng được thụ hưởng tích cực khi sản phẩm được quản lý, bảo mật, đáp ứng các quy định của QCVN./.

Tài liệu tham khảo

[1]. Thông tư 87/2024/TT-BQP của Bộ Quốc phòng: Quy định Danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc cho mô-đun an toàn phần cứng trong hoạt động định danh và xác thực điện tử".

[2]. TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

[3]. 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*".

[4]. 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*".

[5]. Federal Office for Information Security, BSI TR-02102-1 *"Cryptographic Mechanisms: Recommendations and Key Lengths"* Version: 2025-1, January 2025.

[6]. National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS 186-5 "Digital Signature Standard (DSS)", February 2023.

[7]. National Institute of Standards and Technology, Special Publication 800-131A *"Transitioning the Use of Cryptographic Algorithms and Key Lengths"*, March 2019.

[8]. National Institute of Standards and Technology, Special Publication 800-56A Revision 3 "*Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*", April 2018.

[9]. National Institute of Standards and Technology, Special Publication SP 800-56C Revision 2 "*Recommendation for Key-Derivation Methods in Key-Establishment Schemes*", August 2020.

[10]. National Institute of Standards and Technology, Special Publication 800-186 "*Recommendation for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*", April 2018

[11]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General"*, May 2020.

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

[14]. [RFC 2631]: "*Diffie-Hellman Key Agreement Method*", Internet Engineering Task Force (IETF), December 2013.

[15]. [RFC 3526]: "*More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*", Internet Engineering Task Force (IETF), May 2003

[16]. [RFC 7919]: "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)", Internet Engineering Task Force (IETF), August 2016.

[17]. [RFC 6090]: "Fundamental Elliptic Curve Cryptography Algorithms", Internet Engineering Task Force (IETF), February 2011.

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

[19]. https://supportportal.juniper.net/s/article/End-of-support-for-cipher-suites-using-the-CBC-mode.

[20]. https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode.

[21]. https://cryptography.io/en/3.4.3/hazmat/primitives/symmetric-encryption.html

[22]. https://www.mdpi.com/2227-7390/13/9/1383

[23]. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10184306

[24]. https://learn.microsoft.com/en-us/security-updates/securityadvisories/2018/4338110

[25]. https://www.mdpi.com/2079-3197/8/2/51

[26]. https://blog.ise.io/blog/the-dangers-of-cbc-mode

BAN CƠ YẾU CHÍNH PHỦ

THUYẾT MINH

Dự thảo Sửa đổi 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

Hà Nội, 2026

MỤC LỤC

1 Tên gọi và ký hiệu của QCVN

Tên gọi: Sửa đổi 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: SỬA ĐỔI 1:2026 QCVN 12:2022/BQP.

2 Đặt vấn đề

2.1 Tình hình thực tiễn

Quy chuẩn kỹ thuật quốc gia QCVN 12:2022/BQP ban hành và có hiệu lực từ ngày 04/4/2022. Tuy nhiên trong quá trình triển khai, Cơ quan quản lý chuyên ngành nhận thấy một số hạn chế như sau:

- Ngày 31/12/2024, Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quyết định số 3480/QĐ-BKHCN về việc công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV. Đây là thuật toán mã khối riêng của Việt Nam, do Ban Cơ yếu Chính phủ nghiên cứu, xây dựng, đề xuất ban hành. Thuật toán này hiện đang được cộng đồng doanh nghiệp quan tâm, nghiên cứu và tích hợp vào sản phẩm. Tuy nhiên trong các quy chuẩn kỹ thuật quốc gia, danh mục tiêu chuẩn bắt buộc áp dụng ban hành kèm theo Thông tư 23/2022/TT-BQP chưa cập nhật yêu cầu sử dụng với thuật toán mã khối MKV, cần thiết phải bổ sung đáp ứng yêu cầu thực tiễn sử dụng của xã hội;

- Một số nội dung kỹ thuật (*chế độ sử dụng, thời hạn sử dụng, kích thước khối*) trong quy chuẩn hiện hành đã không còn đáp ứng được các yêu cầu an toàn theo khuyến nghị từ các tổ chức quốc tế uy tín như NIST hay BSI, đặc biệt liên quan đến chế độ sử dụng và thời hạn sử dụng của sản phẩm hoặc hệ thống. Các quy định cũ có thể dẫn đến rủi ro cao hơn trong điều kiện vận hành thực tế, không đảm bảo an toàn thông tin.

- Bên cạnh đó, tại kỳ họp thứ 9 Quốc hội Khóa XIII thông qua Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó sửa đổi khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 với quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp như sau:

"2. Thừa nhận đơn phương kết quả đánh giá sự phù hợp được quy định như sau:

a) Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước;

b) Kết quả đánh giá sự phù hợp quy định tại điểm a khoản này phải được thực hiện bởi tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài được một trong các tổ chức công nhận là thành viên ký thỏa thuận thừa nhận lẫn nhau

của Tổ chức Công nhận các phòng thử nghiệm Quốc tế (ILAC), Diễn đàn Công nhận Quốc tế (IAF), Tổ chức hợp tác Công nhận khu vực Châu Á Thái Bình Dương (APAC) đánh giá và công nhận về năng lực đáp ứng tiêu chuẩn quốc tế, tiêu chuẩn quốc gia tương ứng;

Theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp quy định tại khoản này."

Căn cứ quy định trên, để phù hợp với yêu cầu thực tiễn của quản lý chất lượng sản phẩm mật mã dân sự tại Việt Nam, dự thảo Thông tư bổ sung quy định về thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức thử nghiệm nước ngoài đối với sản phẩm mật mã dân sự.

Do đó, việc sửa đổi và ban hành Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân bảo mật luồng IP sử dụng công nghệ IPsec và TLS là cần thiết để khắc phục các hạn chế, nâng cao chất lượng sản phẩm MMDS, đảm bảo an toàn và đồng bộ với các văn bản pháp luật liên quan. Quy chuẩn sửa đổi đáp ứng yêu cầu thực tiễn, phù hợp với tiến bộ khoa học kỹ thuật, thúc đẩy hội nhập quốc tế, nâng cao năng lực cạnh tranh của doanh nghiệp Việt Nam và bảo vệ lợi ích người tiêu dùng, góp phần xây dựng hệ thống tiêu chuẩn hóa bền vững theo Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

2.2 Tình hình tiêu chuẩn hóa tại Việt Nam

Quy chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên quy chuẩn	Ghi chú
1	QCVN 4 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng	Ban hành kèm theo Thông tư 161/2016/TT-BQP ngày 21/10/2016
2	QCVN 5 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về chữ ký số sử dụng trong lĩnh vực ngân hàng	
3	QCVN 6 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về quản lý khóa sử dụng trong lĩnh vực ngân hàng	
4	QCVN 12 : 2022/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS	Ban hành kèm theo Thông tư 23/2022/TT-BQP ngày 04/4/2022
5	QCVN 15 : 2023/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản	Ban hành kèm theo Thông tư

		phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	96/2023/TT-BQP ngày 29/11/2023

Tiêu chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên tiêu chuẩn	Ghi chú
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	
2	TCVN 7816:2007	Công nghệ thông tin – Kỹ thuật mật mã thuật toán mã dữ liệu AES	Phiên bản mới nhất TCVN 11367-3:2016
3	TCVN 7817-1:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 11770-3:2021
4	TCVN 7817-2:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng	Phiên bản mới nhất ISO/IEC 11770-2:2018
5	TCVN 7817-3:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng	Phiên bản mới nhất ISO/IEC 11770-3:2021
6	TCVN 7817-4:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 4: Cơ chế dựa trên bí mật yếu	Phiên bản mới nhất ISO/IEC 11770-4:2017
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 18014-1:2008
8	TCVN 7818-2:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 2: Cơ chế token độc lập	Phiên bản mới nhất ISO/IEC 18014-2:2021
9	TCVN 7818-3:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 3: Cơ chế tạo thẻ liên kết	Phiên bản mới nhất ISO/IEC 18014-3:2009
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	

11	TCVN 11367-1:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 1: Tổng quan	Phiên bản mới nhất ISO/IEC 18033-1:2021
12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	
13	TCVN 11367-3:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối	
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	
16	TCVN 11816-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 2: Hàm băm sử dụng mã khối n-bit.	
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	
18	TCVN 11816-4:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 4: Hàm băm sử dụng số học đồng dư	
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	
20	TCVN 11817-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng	
21	TCVN 11817-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Cơ chế sử dụng kỹ thuật chữ ký số	
22	TCVN 12214-1:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan	
23	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	

24	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	
25	TCVN 11367-5:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật mã dựa trên định danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	
27	TCVN 12212:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô đun mật mã	
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	
29	TCVN 12852-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan	
30	TCVN 12852-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Các kỹ thuật tạo đường cong elliptic	
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	
32	TCVN 12855-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 2: Các cơ chế dựa trên phân tích số nguyên	
33	TCVN 12855-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 3: Các cơ chế dựa trên bài toán Logarit rời rạc	
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ -Phần 1: Tổng quan	
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	

36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	
37	TCVN 12854-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng	
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	
39	TCVN 11817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Cơ chế sử dụng kỹ thuật tri thức không	
40	TCVN 11817-6:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Cơ chế sử dụng truyền dữ liệu thủ công	
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	
44	TCVN 13177:2020	Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mật mã và kiểm thử phù hợp các cơ chế an toàn	
45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	
47	TCVN 13178-2: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký sử dụng một nhóm khóa công khai	
48	TCVN 13178-4: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu	

49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 2: Các cơ chế dựa trên logarit rời rạc	
52	TCVN 13461-1: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 1: Tổng quan	
53	TCVN 13461-2: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 2: Các cơ chế sử dụng một khóa công khai nhóm	
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	
55	TCVN 13462-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản	
56	TCVN 13720:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Kiểm thử các mô-đun mật mã trong môi trường hoạt động,	
57	TCVN 13721:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408),	
58	TCVN 13722:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viễn sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học	
59	TCVN 13723-1:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung	
60	TCVN 13723-2:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh	

		giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)	
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với đánh giá viên theo TCVN 8709 (ISO/IEC 15408)	
62	TCVN 12197:2024	An toàn thông tin – Mã hóa có xác thực (ISO/IEC 19772:2020)	
63	TCVN 14190-1:2024	An toàn thông tin – Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học – Phần 1: Khung (ISO/IEC 19989-1:2020)	
64	TCVN 14190-2:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 2: Hiệu suất nhận dạng sinh trắc học (ISO/IEC 19989-2:2020)	
65	TCVN 14190-3:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 3: Phát hiện tấn công trình diện (ISO/IEC 19989-3:2020)	
66	TCVN 14191-1:2024	An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung (ISO/IEC 23263-1:2021)	
67	TCVN 14192-1:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-1:2019)	
68	TCVN 14192-2:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu	

		chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-2:2020)	
69	TCVN 14263:2024	Công nghệ thông tin – Kỹ thuật an toàn – Thuật toán mã khối MKV.	

2.3 Sự cần thiết xây dựng Sửa đổi Quy chuẩn

a) Về căn cứ

- Luật An toàn thông tin mạng năm 2015, tại khoản 7 Điều 38 giao "Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự"; khoản 4 Điều 52 quy định về trách nhiệm của Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng "xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự", "quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự, quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự".

- Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó một số quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp tại khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 được sửa đổi, bổ sung, tạo điều kiện cho việc thực hiện các quy định về đánh giá sự phù hợp trong lĩnh vực mật mã dân sự. Theo đó, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước và "theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp…".

- Nghị định số 211/2025/NĐ-CP ngày 25/7/2025 của Chính phủ quy định về hoạt động mật mã dân sự và sửa đổi, bổ sung một số điều của Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử được sửa đổi, bổ sung một số điều tại Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 của Chính phủ, tại Điều 10 quy định về thừa nhận kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự "Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp sản phẩm mật mã dân

sự của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước về mật mã dân sự".

b) Về mục đích

Việc xây dựng chuẩn hóa " Sửa đổi 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 " là rất cần thiết nhằm:

- Đảm bảo chất lượng cho các sản phẩm mật mã dân sự bảo mật luồng IP sử dụng công nghệ IPsec và TLS.

- Thống nhất về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS trên phạm vi toàn quốc.

- Là cơ sở kỹ thuật để các cơ quan quản lý tham chiếu, phục vụ công tác quản lý nhà nước về chất lượng sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS sử dụng trong lĩnh vực mật mã dân sự.

c) Về phạm vi áp dụng

Trên cơ sở phân tích lý do và mục đích xây dựng Sửa đổi quy chuẩn, nhóm biên tập quy chuẩn nhận thấy việc sửa đổi một số chỉ tiêu kỹ thuật cho 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 là rất cần thiết và phù hợp trong điều kiện hiện nay.

Nội dung Sửa đổi Quy chuẩn chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 12:2022/BQP. Các nội dung không được nêu tại Sửa đổi Quy chuẩn này thì tiếp tục áp dụng QCVN 12:2022/BQP ban hành kèm theo Thông tư số 23/2022/TT-BQP ngày 04/4/2022 của Bộ trưởng Bộ Quốc phòng.

3 Cơ sở xây dựng các yêu cầu kỹ thuật

3.1 Cơ sở văn bản kỹ thuật trong nước

Khi xây dựng dự thảo quy chuẩn, cơ quan soạn thảo đã tham khảo các tài liệu sau:

- Quyết định số 3480/QĐ-BKHCN ngày 31/12/2024 của Bộ trưởng Bộ Khoa học và Công nghệ công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.

- Thông tư số 23/2022/TT-BQP ngày 04/4/2022 của Bộ trưởng Bộ Quốc phòng 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.

Trên cơ sở các tài liệu kỹ thuật tham khảo, cơ quan soạn thảo đã bổ sung, sửa đổi quy chuẩn đáp ứng yêu cầu sử dụng thuật toán MKV, đáp ứng điều kiện thực tế đối với các sản phẩm đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế.

3.2 Cơ sở kinh nghiệm quốc tế

3.2.1 Cơ sở cho việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự

Thực tiễn quốc tế cho thấy mức độ an toàn của các thuật toán mật mã và các tham số kỹ thuật liên quan có xu hướng thay đổi theo thời gian, phụ thuộc vào sự phát triển của khoa học công nghệ và năng lực tính toán. Các thuật toán và độ dài khóa hiện đang được sử dụng có thể không còn đáp ứng yêu cầu bảo đảm an toàn thông tin trong trung và dài hạn, đặc biệt đối với các thông tin có yêu cầu bảo mật cao hoặc thời gian bảo vệ kéo dài.

Trong bối cảnh đó, nhiều quốc gia và tổ chức tiêu chuẩn hóa đã ban hành các quy định và khuyến nghị nhằm quản lý việc lựa chọn, sử dụng và thay thế các thuật toán mật mã, trên cơ sở đánh giá định kỳ mức độ an toàn và phù hợp của các giải pháp kỹ thuật. Việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự được xem là một biện pháp cần thiết nhằm hạn chế rủi ro phát sinh từ việc tiếp tục sử dụng các thuật toán hoặc tham số kỹ thuật không còn đáp ứng yêu cầu bảo mật.

Các biện pháp quản lý được áp dụng phổ biến trong thực tiễn quốc tế bao gồm:

– Quy định thời hạn sử dụng hoặc chu kỳ rà soát đối với thuật toán và độ dài khóa, làm cơ sở để các tổ chức, cá nhân chủ động cập nhật, nâng cấp hoặc thay thế các giải pháp mật mã phù hợp với mức độ nhạy cảm của thông tin được bảo vệ;

– Tham chiếu và áp dụng các tiêu chuẩn, khuyến nghị mật mã do các tổ chức tiêu chuẩn hóa uy tín ban hành (như NIST, BSI), nhằm bảo đảm sự phù hợp với thông lệ quốc tế và hạn chế nguy cơ triển khai các thuật toán hoặc tham số kỹ thuật đã được đánh giá là không còn an toàn;

– Đối với dữ liệu có mức độ nhạy cảm cao hoặc có yêu cầu bảo vệ trong thời gian dài, định hướng sử dụng các thuật toán và độ dài khóa có mức an toàn cao hơn, đáp ứng yêu cầu bảo mật trong dài hạn và có khả năng thích ứng với sự phát triển của công nghệ;

– Xây dựng lộ trình chuyển đổi phù hợp từ các thuật toán mật mã khóa công khai truyền thống sang các thuật toán mới có mức độ an toàn cao hơn, bao gồm các thuật toán có khả năng chống chịu trước các tiến bộ về năng lực tính toán, trên cơ sở đánh giá rủi ro, mức độ nhạy cảm của dữ liệu và yêu cầu quản lý nhà nước trong từng giai đoạn.

3.2.2 Rà soát, cập nhật thuật toán mật mã theo các tiêu chuẩn quốc tế mới nhất

Cơ quan soạn thảo đã tham khảo các khuyến nghị quốc tế về an toàn mật mã để đưa ra các sửa đổi, bổ sung phù hợp với điều kiện sử dụng sản phẩm mật mã dân sự tại Việt Nam, đảm bảo cân bằng giữa bảo mật, hiệu suất, và khả năng triển khai thực tế. Các giải pháp này đảm bảo rằng mật mã dân sự đáp ứng được yêu cầu bảo mật ngắn hạn, đồng thời phù hợp với lộ trình cập nhật công nghệ để bảo vệ dữ liệu trong dài hạn, như đã đề cập trong các quy định của Việt Nam (QCVN 12:2022/BQP) và khuyến nghị

quốc tế.

a) Đối với thuật toán TDEA

Tài liệu NIST SP 800-131A Rev 2 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) cung cấp các quy định về khuyến nghị sử dụng và lộ trình chuyển đổi đối với các thuật toán mật mã và độ dài khóa như sau:

Thuật toán	Khuyến nghị sử dụng
3TDEA cho Mã hóa	Không được chấp nhận đến năm 2023 Không được phép sau năm 2023
3TDEA cho Giải mã	Sử dụng kế thừa
AES-128 cho Mã hóa và Giải mã	Được chấp nhận
AES-192 cho Mã hóa và Giải mã	Được chấp nhận
AES-256 cho Mã hóa và Giải mã	Được chấp nhận

Tại đây NIST đặt ra giới hạn và lộ trình sử dụng thuật toán TDEA:

- Việc sử dụng đối với các biện pháp bảo vệ mật mã mới (như mã hóa, đóng gói khóa, tạo MAC) được khuyến nghị chuyển đổi trước ngày 31 tháng 12 năm 2023 và sẽ bị ngừng phê duyệt từ ngày 1 tháng 1 năm 2024.

- Tuy nhiên, TDEA vẫn được phép dùng cho chức năng giải mã, mở gói khóa và xác minh MAC đối với dữ liệu đã được bảo vệ trước đó, nhằm hỗ trợ các hệ thống kế thừa trong quá trình chuyển đổi.

Thực hiện theo lộ trình này, NIST đã công bố thông báo ngày 29 tháng 6 năm 2023 về việc rút lại NIST SP 800-67 Rev.2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, có hiệu lực từ ngày 1 tháng 1 năm 2024.

b) Đối với chế độ CBC

Một số tổ chức có các nghiên cứu và khuyến nghị không sử dụng chế độ Cipher Block Chaining (CBC) cho các thuật toán mã khối đối xứng (AES, Camellia, SEED, CAST và GOST R 34.12-2015). Do CBC có một số hạn chế bảo mật chung:

+ Chế độ CBC không tích hợp tính toàn vẹn (authentication), khiến nó dễ bị tấn công thay đổi dữ liệu (malleability) nếu không sử dụng kèm mã xác thực thông điệp (MAC).

+ Trong các phiên bản TLS cũ (TLS 1.0/1.1), CBC dễ bị tấn công vào phần đệm oracle đệm - Padding Oracle Attacks (như BEAST hoặc POODLE) do cách xử lý Vector Khởi tạo (IV) và phần đệm (padding). Các hãng công nghệ lớn như Juniper, Microsoft cho rằng các dữ liệu được mã hóa bằng chế độ CBC của các thuật toán mật mã khóa đối xứng không còn an toàn, và kết thúc hỗ trợ đối với chế độ CBC của các

thuật toán mật mã sử dụng trong các sản phẩm của hãng, khuyến nghị sử dụng các chế độ hoạt động an toàn hơn, chẳng hạn như GCM, CTR/CCM. Tài liệu tham chiếu:

https://supportportal.juniper.net/s/article/End-of-support-for-cipher-suites-using-the-CBC-mode.

https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode.

https://cryptography.io/en/3.4.3/hazmat/primitives/symmetric-encryption.html

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10184306

+ TLS 1.3 đã loại bỏ hoàn toàn CBC, ưu tiên sử dụng các chế độ mã hóa có xác thực dữ liệu kèm theo (AEAD) như GCM. Trong IPsec, CBC vẫn được hỗ trợ thông qua ESP (Encapsulating Security Payload), nhưng khuyến nghị chuyển sang GCM để đảm bảo tính toàn vẹn tốt hơn. Tài liệu tham chiếu :

https://learn.microsoft.com/en-us/securityupdates/securityadvisories/2018/4338110

https://blog.ise.io/blog/the-dangers-of-cbc-mode

https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062

c) Đối với thuật toán Kuznyechik

Đối với thuật toán Kuznyechik, chế độ MGM là chế độ mã hóa xác thực được quy định trong hệ tiêu chuẩn GOST, được thiết kế đồng bộ với thuật toán Kuznyechik, cho phép bảo đảm đồng thời tính bí mật và toàn vẹn dữ liệu. Việc lựa chọn MGM thay cho các chế độ AEAD khác nhằm bảo đảm tính nhất quán về hệ tiêu chuẩn và thuận lợi trong triển khai, đánh giá hợp chuẩn đối với các sản phẩm sử dụng thuật toán Kuznyechik.

Các chế độ CCM và GCM không được áp dụng cho thuật toán Kuznyechik do không thuộc hệ chế độ được chuẩn hóa đồng bộ với thuật toán này. Việc không lựa chọn CCM và GCM đối với Kuznyechik không làm giảm mức độ an toàn của quy chuẩn, đồng thời bảo đảm tính rõ ràng, nhất quán và khả thi trong áp dụng.

d) Đối với chế độ CFB, OFB

Các chế độ CFB, OFB tuy là các chế độ hợp lệ về mặt lý thuyết (định nghĩa FIPS/NIST), tuy nhiên không được dùng phổ biến trong Ipsec VPN, TLS VPN do:

- Tại hướng dẫn kỹ thuật "TR-02102-2" và "TR-02102-3" của tổ chức BSI, các chế độ CFB, OFB không có trong danh sách khuyến nghị sử dụng.

- CFB và OFB chỉ cung cấp tính bí mật (Confidentiality), tức là mã hóa dữ liệu để người khác không đọc được. Tuy nhiên, chúng không đảm bảo tính toàn vẹn (Integrity). Kẻ tấn công có thể thay đổi các bit trong bản mã (ciphertext) và khi giải mã, bản rõ (plaintext) sẽ bị thay đổi theo một cách dự đoán được mà không bị phát hiện nếu không có thêm cơ chế kiểm tra (như HMAC).

- Hiệu suất sử dụng không tận dụng tối đa sức mạnh của CPU đa nhân hiện đại, điều này cực kỳ quan trọng đối với đường truyền VPN tốc độ cao. CFB mã hóa không thể song song hóa (parallelize) vì khối sau phụ thuộc vào kết quả của khối trước. Còn với OFB mặc dù có thể tính toán trước dòng khóa (keystream), nhưng nó cũng hoạt động tuần tự.

- Cả CFB và OFB (đặc biệt là OFB vì nó hoạt động như stream cipher) rất nhạy cảm với việc bị tấn công thay đổi bit (bit-flipping attacks) nếu không có Message Authentication Code (MAC) đi kèm.

e) Đối với thuật toán DSA

- Hướng dẫn kỹ thuật "TR-02102-1" của BSI trình bày khuyến nghị về kích thước khóa an toàn tối thiểu (công bố vào tháng 3 năm 2025), BSI đã nhấn mạnh rằng các thuật toán cổ điển (RSA, DSA, ECDSA, ECDH) có thể không còn đủ an toàn trước các cuộc tấn công lượng tử trong tương lai. Cơ quan soạn thảo tổng hợp lại khuyến nghị của BSI như sau:

STT	Thuật toán	Kích thước khóa theo bit	Năm sử dụng
1	RSA	2000	2022
		≥ 3000	2023 trở đi
2	DSA	2000	2022
		≥ 3000	2023 trở đi
4	ECDSA	≥ 250	2023 trở đi
5	ECDH	≥ 250	2023 trở đi

Ngày 03/02/2023, tổ chức NIST công bố tiêu chuẩn FIPS 186-5 Digital Signature Standard (DSS). Tiêu chuẩn này không còn chấp thuận DSA cho việc tạo chữ ký số. Tuy nhiên, DSA có thể được sử dụng để xác minh chữ ký được tạo trước ngày triển khai tiêu chuẩn này.

f) Đối với thuật toán GOST R 34.10-2001

Năm 2012, Liên bang Nga ban hành tiêu chuẩn GOST R 34.10-2012 để thay thế GOST R 34.10-2001, nhằm nâng cao cường độ bảo mật cho thuật toán chữ ký số dựa trên đường cong elliptic, khắc phục các hạn chế về độ mạnh toán học và khả năng chống tấn công của phiên bản cũ (theo RFC 7091 và các chỉ đạo từ Cơ quan Tiêu chuẩn Kỹ thuật Nga). GOST R 34.10-2001 sau đó bị coi là lỗi thời, bị loại khỏi các ứng dụng mới trong các tiêu chuẩn quốc tế như DNSSEC (IETF chuyển trạng thái histori năm 2024) và không còn được khuyến nghị sử dụng do rủi ro bảo mật tiềm ẩn so với các thuật toán hiện đại.

g) Đối với thuật toán SEED, CAST, Camellia

Ba thuật toán SEED, CAST, Camellia đều không có trong danh sách thuật toán được khuyến nghị sử dụng cho các hệ thống mới bởi NIST (NIST SP 800-52 Revision 2; NIST SP 800-131A Revision 2), BSI (BSI-TR-02102-1; BSI-TR-02102-2; BSI-TR-02102-3).

Theo hướng dẫn kỹ thuật "TR-02102-1" của BSI để đảm bảo bảo vệ dài hạn cho các ứng dụng có yêu cầu bảo mật cao, nên sử dụng khóa có độ dài ít nhất 256 bit cho các cơ chế mã hóa đối xứng và chỉ nên sử dụng các thuật toán mã khối có kích thước khối ít nhất là 128 bit (3. Symmetric Encryption Schemes – BSI TR-02102-1).

h) Đối với thuật toán băm

- Theo hướng dẫn kỹ thuật "TR-02102-1" của BSI các cơ chế băm được khuyến nghị trong tài liệu này đều có độ dài mã băm (digest length) $\geq$ 256 bit, tuy nhiên đối với các ứng dụng yêu cầu bảo mật cao, dài hạn, hoặc các hệ thống có tuổi thọ dài, nên sử dụng các hàm băm có đầu ra ít nhất 384 bit.

- Năm 2012, Liên bang Nga ban hành tiêu chuẩn GOST R 34.11-2012 (còn gọi là Streebog) để thay thế GOST R 34.11-94, nhằm nâng cao cường độ bảo mật cho thuật toán hàm băm mật mã, khắc phục các hạn chế về độ mạnh toán học và khả năng chống tấn công của phiên bản cũ (theo RFC 6986 và các chỉ đạo từ Cơ quan Tiêu chuẩn Kỹ thuật Nga - Rosstandart).

i) Đối với thuật toán xác thực thông điệp

Theo hướng dẫn kỹ thuật "TR-02102-1" của BSI kích thước khóa được khuyến nghị trong tài liệu này cho việc sử dụng trong các hệ thống mật mã mới được dựa trên mức an toàn tối thiểu đó ($\geq$120 bit).

Thuật toán	CMAC	HMAC
Kích thước khóa theo bit	$\geq$ 128	$\geq$ 128
Kích thước thẻ (tag) được khuyến nghị theo bit	$\geq$ 96	$\geq$ 128

Theo hướng dẫn kỹ thuật "TR-02102-3" của BSI bảng sau liệt kê các thuật toán được khuyến nghị để bảo vệ tính toàn vẹn của các gói ESP:

STT	Thuật toán	Tham chiếu	Sử dụng đến năm
1	AUTH_AES_XCBC_96	[RFC 3566]	2031+
2	AUTH_AES_CMAC_96	[RFC 4494]	2031+

3	AUTH_HMAC_SHA2_256_128	[RFC 4868]	2031+
4	AUTH_HMAC_SHA2_384_192		2031+
5	AUTH_HMAC_SHA2_512_256		2031+

3.3 Thực trạng sử dụng đối với một số thuật toán mật mã

Bảng tổng hợp dưới đây một vài thuật toán mật mã đối xứng và các tấn công đã biết đối với từng thuật toán đó.

Thuật toán	Kích thước khóa theo bit	Kích thước khối theo bit	Các tấn công đã biết	Mô tả
AES	128, 192, 256	128	Chưa có các tấn công thám mã đã biết	Được mô tả trong FIPS 197. Đây là thuật toán mã khối công bố năm 1998 được chính phủ Mỹ làm chuẩn mã hóa, sau đó được NIST chấp thuận làm tiêu chuẩn và được sử dụng rộng rãi đến nay.
DES	56	64	Kích thước khối và khóa nhỏ, dễ bị tấn công bởi các phương pháp vét cạn, ngày sinh, vi sai, tuyến tính, khóa yếu.	Được mô tả trong FIPS 46-3. Đây là thuật toán mã khối được IBM phát triển, công bố năm 1975, và được chuẩn hóa năm 1/1976.
TDEA	128, 192	64	Vào năm 2016 một lỗ hổng lớn đã được phát hiện đối với thuật toán này sử dụng trong giao thức TLS, IPsec, SSH, được công bố tại CVE-2016-2183. Cuộc tấn công thực thi với thuật toán này là tấn công ngày sinh (Birthday attack).	Được mô tả trong SP 800-67. Đây là thuật toán mã khối, TDEA (còn biết đến với tên gọi Triple-DES) được công bố lần đầu năm 1981. Do lỗ hổng lớn được phát hiện nên NIST khuyến nghị ngừng sử dụng cho các ứng dụng từ năm 2017.

IDEA	128	64	Hạn chế của mã pháp này là kích thước khối nhỏ, lược đồ khóa đơn giản và chứa các lớp khóa yếu. Không có các tấn công thực tế, tuy nhiên có các tấn công lên số vòng nhỏ và khóa yếu. Tấn công tốt nhất lên IDEA là tấn công Bicliques. • Khovratovich, Dmitry; Leurent, Gaëtan; *Rechberger*, Christian (2012). *Narrow-Bicliques: Cryptanalysis of Full IDEA. Advances in Cryptology – EUROCRYPT 2012.* Lecture Notes in Computer Science. **7237**. pp. 392–410 • Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", *Advances in Cryptology, CRYPTO 93 Proceedings*: 224–231	Thuật toán mã khối được được thiết kế bởi James Massey của ETH Zurich và Xuejia Lai và được mô tả lần đầu tiên vào năm 1991. Thuật toán này ra đời nhằm thay cho thuật toán DES.
RC2	40	64	Kích thước khóa quá nhỏ, kích thước khối nhỏ. Dễ tổn thương trước các dạng tấn công khác nhau.	Thuật toán mã khối được thiết kế năm 1987 bởi Ron Rivest của hãng bảo mật RSA Data Security. RC2 còn được biết đến với tên gọi ARC2.
RC5	0-2040	32, 64, 128	Tồn tại một số tấn công lên phiên bản rút gọn 12-vòng với phiên bản kích thước khối 64-bit (thám mã vi sai) với độ phức tạp 2^{44} bản rõ chọn lọc.	Thuật toán mã khối được thiết kế bởi Ronald Rivest vào năm 1994.

RC6	128, 192, 256	128	Không tồn tại các tấn công thám mã đã biết.	Thuật toán mã khối có nguồn gốc từ RC5 và được thiết kế bởi Ron Rivest, Matt Robshaw, Ray Sidney và Yiqun Lisa Yin để đáp ứng các yêu cầu của cuộc thi Tiêu chuẩn mã hóa nâng cao (AES).
ARIA	128, 192, 256	128	• *Wenling Wu; Wentao Zhang; Dengguo Feng (2006). "Impossible Differential Cryptanalysis of ARIA and Camellia". Retrieved January 19, 2007.* • *Xuehai Tang; Bing Sun; Ruilin Li; Chao Li (March 30, 2010). "A Meet-in-the-Middle Attack on ARIA". Retrieved April 24, 2010.*	Thuật toán mã khối được thiết kế vào năm 2003 bởi một nhóm lớn các nhà nghiên cứu của Hàn Quốc. Năm 2004 thuật toán này được chuẩn hóa và sử dụng tại Hàn Quốc.
Blowfish	32-448	64	Tấn công ngày sinh (vì kích thước khối nhỏ). Tồn tại các khóa yếu.	Thuật toán mã khối do Bruce Schneier thiết kế năm 1993 như một giải pháp thay thế miễn phí, nhanh chóng cho các thuật toán mã hóa hiện có tại thời điểm đó.
Camellia	128, 192, 256	128	Có độ an toàn được xem là tương đương với AES.	Thuật toán mã khối được phát triển bởi Mitsubishi Electric và NTT của Nhật Bản. Được công nhận trong chuẩn ISO/IEC. Thuật toán có mức độ bảo mật và khả năng xử lý tương đương với thuật toán AES.

SEED	128	128	Chưa có các tấn công đã biết với phiên bản đầy đủ.	Thuật toán mã khối được phát triển bởi KISA (Hàn Quốc) và được công bố trong chuẩn ISO/IEC 18033-3:2010 và nhiều RFC khác (như RFC 4010, RFC 4162, RFC4196).
CAST	64	64	Kích thước khóa/khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán mã khối. Không có bản quyền, được mô tả trong RFC 2144.
CAST-128 (còn gọi là CAST5)	40-128	64	Kích thước khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán được công bố vào năm 1996 bởi Carlisle Adams và Stafford Tavares. Thuật toán này cũng đã được Cơ quan An ninh Truyền thông phê duyệt cho Chính phủ Canada sử dụng.
CAST-256 (còn gọi là CAST6)	128, 192, 256	128	Tấn công tốt nhất là tấn công tương quan không (zero-correlation) với độ phức tạp thời gian là $2^{246.9}$ và dữ liệu là $2^{98.8}$. Tấn công này không ảnh hưởng tới độ an toàn của thuật toán. Bogdanov, Andrey; Leander, Gregor; Nyberg, Kaisa; Wang, Meiqin (2012). *Integral and multidimensional linear distinguishers with correlation zero. Lecture Notes in Computer Science.* **7658**. pp. 244–261.	Thuật toán mã khối, có nguồn gốc từ CAST-128. CAST-256 được xuất bản vào 6/1998. Được thiết kế theo thiết kế "CAST" do Carlisle Adams, Stafford Tavares phát minh và Howard Heys, Michael Wiener đóng góp vào thiết kế. CAST-256 được mô tả trong RFC 2612.

SM4	128	128	Chưa có tấn công đã biết nào được công bố.	Thuật toán mã khối, nó được nhiều cơ quan đầu ngành tại Trung Quốc phát triển nhưng chủ yếu được phát triển bởi Lũ Shuwang. Tháng 8/2016 được chuẩn hóa tại Trung Quốc.

Dựa vào bảng trên, có thể thấy hầu hết các thuật toán có kích thước khối 128 bit giúp hạn chế các rủi ro liên quan đến tấn công ngày sinh, phù hợp với khuyến nghị của các tổ chức quốc tế, trong đó AES là thuật toán được nhắc đến nhiều nhất trong các tài liệu của tổ chức quốc tế uy tín (NIST, BSI, ANSI), được coi là chuẩn mặc định để đánh giá độ an toàn của các thuật toán khác. Hầu hết các tài liệu kỹ thuật (Whitepaper) và cấu hình mặc định đều chỉ liệt kê AES (Advanced Encryption Standard) với các độ dài khóa 128-bit hoặc 256-bit là lựa chọn duy nhất cho mã hóa đối xứng.

Qua rà soát danh mục sản phẩm mật mã dân sự và khảo sát thị trường tại Việt Nam, cơ quan soạn thảo nhận thấy đa số sản phẩm được khảo sát có tích hợp thuật toán mã hóa AES, hiếm thấy sản phẩm tích hợp tùy chọn các thuật toán quốc tế hoặc nội địa khác (như Camellia, CAST, SEED, SM4), các thư viện mã nguồn mở mặc định sử dụng thuật toán AES hoặc không có các tùy chọn thuật toán khác, nếu có nhu cầu sử dụng, phải tùy biến, tích hợp vào mã nguồn.

Về mặt hỗ trợ phần cứng, hầu hết các CPU hiện đại (Intel, AMD, ARM) đều có tập lệnh hỗ trợ AES-NI, giúp việc mã hóa/giải mã bằng AES có tốc độ cực nhanh mà không tốn nhiều tài nguyên. Do vậy, việc sử dụng AES là đảm bảo tính tương thích cao, tiết kiệm chi phí khi sản phẩm cần giao tiếp, phổ biến rộng rãi với hệ thống quốc tế.

Để đảm bảo tính an toàn và hội nhập cùng thế giới, các sản phẩm, dịch vụ mật mã dân sự được kinh doanh, sử dụng tại thị trường Việt Nam cần có tính an toàn, ổn định, tương thích cao, đồng thời định hướng phát triển mật mã Việt Nam đảm bảo tự chủ bền vững. Do đó, cần xây dựng quy định chặt chẽ cho việc sử dụng các thuật toán mật mã phổ biến và thuật toán mật mã của Việt Nam. Cơ quan soạn thảo đã tham khảo các khuyến nghị quốc tế về an toàn mật mã để đưa ra các sửa đổi, bổ sung phù hợp với điều kiện sử dụng sản phẩm mật mã dân sự tại Việt Nam, đảm bảo cân bằng giữa bảo mật, hiệu suất, và khả năng triển khai thực tế. Các giải pháp này đảm bảo rằng mật mã dân sự đáp ứng được yêu cầu bảo mật ngắn hạn, đồng thời phù hợp với lộ trình cập nhật công nghệ để bảo vệ dữ liệu trong dài hạn.

3.4 Cơ sở thực tiễn và căn cứ thừa nhận kết quả đánh giá sự phù hợp

Công tác quản lý chất lượng sản phẩm mật mã dân sự, đánh giá chứng nhận hợp chuẩn, hợp quy sản phẩm mật mã dân sự trong nước gặp nhiều khó khăn trong quá trình triển khai do thực trạng hiện nay ở Việt Nam chưa có tổ chức thử nghiệm đạt các chứng chỉ về thử nghiệm sản phẩm mật mã dân sự và được chỉ định (ISO/IEC 17025). Các quy chuẩn kỹ thuật trong lĩnh vực mật mã dân sự tại Việt Nam được xây dựng được xây dựng trên cơ sở hài hòa với tiêu chuẩn quốc tế. Cùng với đó, đa số các sản

phẩm mật mã dân sự hiện nay được nhập khẩu từ nước ngoài và đã được đánh giá bởi các tổ chức uy tín, có năng lực. Về cơ bản, đối với sản phẩm có chung tiêu chuẩn kỹ thuật, kết quả đánh giá từ các tổ chức quốc tế có năng lực được công nhận không có sai lệch, khác biệt và đảm bảo rằng việc đánh giá tuân thủ quy chuẩn là nhất quán và công bằng. Do vậy, việc chấp nhận kết quả thử nghiệm từ tổ chức được chỉ định và tổ chức nước ngoài được công nhận theo ISO/IEC 17025 trong khi điều kiện trong nước chưa thực hiện được là phù hợp để triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

4 Nội dung Sửa đổi Quy chuẩn kỹ thuật quốc gia Sửa đổi 1:2025 QCVN 12:2022/BQP bao gồm các nội dung bổ sung, thay thế các quy định của QCVN 12:2022/BQP

Căn cứ vào quá trình rà soát các sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS đã được Ban Cơ yếu Chính phủ cấp phép; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng với thuật toán mã khối MKV; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng các thuật toán mật mã nhằm bảo đảm an toàn thông tin trong bối cảnh xuất hiện các nguy cơ từ máy tính lượng tử; Căn cứ vào tình hình triển khai thực tế của các Quy chuẩn kỹ thuật hiện hành và định hướng chuyển đổi sang các thuật toán mật mã hậu lượng tử; Căn cứ vào tình hình triển khai thực tế của Quy chuẩn kỹ thuật đã được ban hành; Xem xét từ những yêu cầu, khuyến nghị được nêu ra trong các tài liệu tham khảo từ các tổ chức NIST, CC, BSI, cơ quan soạn thảo đề xuất sửa đổi như sau:

4.1 Nguyên tắc xây dựng nội dung

- Các tham số an toàn được lựa chọn theo các khuyến nghị của ISO/IEC, NIST, CC, BSI và các tổ chức quốc tế khác để đảm bảo an toàn và phù hợp;

- Phù hợp với điều kiện thực tế đối với các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế;

- Đáp ứng được sự phát triển của công nghệ trong vòng 5 năm tới.

4.2 Bổ sung quy định đối với thuật toán MKV

Tại mục 1.3 Tài liệu viện dẫn,

- Bổ sung vào dòng sau tiêu đề mục 1.3 Tài liệu viện dẫn nội dung sau:

"Các Tài liệu viện dẫn sau là cần thiết cho việc áp dụng Quy chuẩn này. Trường hợp các Tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất."

- Bổ sung các tài liệu viện dẫn vào sau dòng "TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác nhận thông điệp"" như sau:

"QCVN 12:2022/BQP "Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPSec và TLS."

TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV"."

- Thay thế mục *1.5 Chữ viết tắt* như sau như sau:

Chữ viết tắt	**Tên tiếng Anh**	**Tên tiếng Việt**
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
AH	Authentication Header	Xác thực header
CCM	Counter with Cipher Block Chaining Message Authentication Code	Chế độ bộ đếm với xác thực thông báo kiểu CBC
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
EC	Elliptic Curve	Đường cong Elliptic
ECDH	Elliptic Curve Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên 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
FFDH	Finite-Field Diffie-Hellman	Trao đổi khóa Diffie-Hellman dựa trên trường hữu hạn
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
GCM	Galois/Counter Mode	Chế độ bộ đếm Galois

GOST	Gosudarstvenny 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
MGM	Multilinear Galois Mode	Chế độ Galois đa tuyến tính
MKV		Mã khối Việt Nam
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định đa biến bậc hai
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
QCVN		Quy chuẩn kỹ thuật quốc gia
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF 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)
TLS	Transport Layer Security	Bảo mật tầng giao vận
TCVN		Tiêu chuẩn quốc gia Việt Nam
VPN	Virtual Private Network	Mạng riêng ảo

- Thay thế mục 1.6 Ký hiệu như sau:

Ký hiệu	**Mô tả**
nlen	Độ dài modulo theo bit hoặc độ dài theo bit của cấp của phần tử sinh
L	Đối với thuật toán FFDH: L là độ dài của tham số miền p theo bit
N	Đối với thuật toán FFDH: N là độ dài của tham số miền q theo bit

4.3 Thuật toán mật mã đối xứng

Tại mục 2.2.1.1:

- Loại bỏ thuật toán TDEA, SEED, CAST, Camellia khỏi danh mục;
- Bổ sung thuật toán MKV;
- Đổi tên GOST 34.12-2015 thành tên "Kuznyechik".

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015] [RFC 7801]

Tại mục 2.2.2.1:

- Loại bỏ chế độ CBC đối với thuật toán mật mã đối xứng;

- Bổ sung quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán MKV: Thời hạn sử dụng đến năm 2028 đối với kích thước khóa theo bit 128; Đối với kích thước khóa theo bit là 192 và 256 thời hạn sử dụng đến năm 2030;

- Loại bỏ thuật toán TDEA, CAST, SEED, Camellia;

- Đối với thuật toán AES: Điều chỉnh thời hạn sử dụng đến năm 2028 đối với kích thước khóa theo bit 128; Đối với kích thước khóa theo bit là 192 và 256 điều chỉnh thời hạn sử dụng đến năm 2030; Loại bỏ chế độ OFB, CFB.

- Đối với thuật toán GOST R 34.12-2015 chỉnh sửa tên thành "Kuznyechik":

+ Loại bỏ chế độ CFB, bổ sung chế độ MGM;

+ Điều chỉnh thời hạn sử dụng đối với chế độ (CTR, MGM) đến năm 2030.

STT	Thuật toán	Kích thước khóa theo bit	Các chế độ cho phép sử dụng	Sử dụng đến năm
1	MKV	128	GCM, CCM, CTR	2028
		192, 256		2030
2	AES	128	GCM, CCM, CTR	2028
		192, 256		2030
3	Kuznyechik	256	MGM, CTR	2030
CHÚ THÍCH: Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo TCVN 14263:2024. Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo FIPS 197 hoặc TCVN 11367-3:2016. Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801). Các chế độ hoạt động của mã khối trong quy chuẩn này áp dụng theo TCVN 12213, SP 800-38A, SP 800-38C, SP 800-38D, GOST R 34.13-2015, RFC 9058.				

4.4 Thuật toán mật mã phi đối xứng

Tại Mục 2.2.1.2:

- Loại bỏ thuật toán DSA và GOST R34.10-2001;

- Bổ sung, cập nhật các tài liệu, tiêu chuẩn tham chiếu mới nhất đối với các thuật toán mật mã phi đối xứng.

STT	Thuật toán	Tham chiếu
1	RSA	[FIPS 186-5], [SP 800-56B Rev. 2]

2	FFDH	[SP 800-56A Rev. 3], [RFC 2631], [RFC 3526], [RFC 7919]
3	ECDSA	[FIPS 186-5], [RFC 6090], [SP 800-186]
4	ECDH	[FIPS 186-5], [SP 800-56A Rev. 3], [SP 800-56C Rev. 2]
5	GOST R34.10-2012	[RFC 7091]

Tại Mục 2.2.2.2:

- Loại bỏ thuật toán DSA và GOST R34.10-2001 khỏi danh mục;

- Đối với thuật toán RSA: Điều chỉnh thời hạn sử dụng đến năm 2028 đối với kích thước tham số theo bit $2048 \leq nlen < 3072$; Trường hợp kích thước tham số theo bit nlen = 3072 thời hạn sử dụng đến năm 2030 (để phù hợp với lộ trình cập nhật công nghệ);

- Đối với thuật toán DH đổi tên chi tiết thành FFDH:

+ Điều chỉnh thời hạn sử dụng đến năm 2030 đối với kích thước tham số mật mã L (độ dài tham số miền p theo bit) $2048 \leq L \leq 3072$, N (độ dài tham số miền q theo bit) $256 \leq N \leq 384$ (để phù hợp với lộ trình cập nhật công nghệ);

- Đối với thuật toán ECDH, ECDSA:

+ Điều chỉnh thời hạn sử dụng đến năm 2030, sửa đổi kích thước tham số theo bit thành $250 \leq nlen \leq 384$ (để phù hợp với lộ trình cập nhật công nghệ);

- Đối với thuật toán GOST R 34.10-2012: Điều chỉnh thời hạn sử dụng từ 2027 lên 2030 (theo các khuyến nghị chung về mật mã hậu lượng tử).

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
1	RSA	$2048 \leq nlen < 3072$	2028
		$nlen = 3072$	2030

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
2	FFDH	$2048 \leq L \leq 3072$, $256 \leq N \leq 384$	2030
3	ECDH, ECDSA	$250 < nlen \leq 384$	2030
4	GOST R 34.10-2012	$nlen \geq 256$	2030

CHÚ THÍCH:

Đối với RSA và ECDSA, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo FIPS 186-5.

Đối với FFDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3.

Đối với ECDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3 và NIST SP 800-56C Rev. 2.

Đối với GOST R 34.10-2012, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.10-2012 (RFC 7091).

4.5 Thuật toán băm

Tại mục 2.2.1.3 bổ sung thuật toán băm GOST R 34.11-2012 vào danh sách sử dụng thuật toán băm như sau:

STT	Thuật toán	Tham chiếu
1	SHA-256, SHA-384, SHA-512/256, SHA-512	[FIPS 180-4], [TCVN 11816-3]
2	SHA3-256, SHA3-384, SHA3-512	[FIPS 202]
3	GOST R 34.11-2012	[RFC 6986]

4.6 Thời hạn sử dụng

- Tại mục 2.2.2.3 Thuật toán băm điều chỉnh thời hạn sử dụng từ năm "2027" thành năm "2030" và bổ sung thuật toán hàm băm GOST R 34.11-2012 (RFC 6986) như sau:

STT	Thuật toán	Sử dụng đến năm
1	SHA-256, SHA-384, SHA-512/256, SHA-512	2030
2	SHA3-256, SHA3-384, SHA3-512	2030

3	GOST R 34.11-2012	2030
CHÚ THÍCH: Đối với GOST R 34.11-2012, các tiêu chuẩn cho tham số an toàn và các bộ tham số cụ thể áp dụng theo GOST R 34.11-2012 (RFC 6986).		

- Sửa đổi mục 2.2.2.4 như sau: Điều chỉnh thời hạn sử dụng từ năm "2027" thành năm "2030".

4.7 Quy định chung

Thay thế mục 2.1 Quy định chung như sau:

"- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ IPsec VPN chỉ được phép sử dụng giao thức trao đổi khóa IKE phiên bản 2 (IKEv2) trở lên, giao thức đóng gói ESP.

- Đối với các sản phẩm mật mã dân sự sử dụng công nghệ TLS VPN chỉ được phép sử dụng giao thức phiên bản TLS 1.2 trở lên."

4.8 Quy định về an toàn sử dụng trong giao thức

- Thay thế mục 2.3.1 như sau:

"2.3.1 Quy định về an toàn sử dụng trong giao thức IPSec

"- 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)."

- Thay thế mục 2.3.2 như sau:

"- Không được phép trao đổi khóa dựa trên thuật toán Diffie-Hellman trên trường hữu hạn sử dụng khóa cố định (Static Diffie-Hellman).

- 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 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."

4.9 Quy định về quản lý

Thay thế mục 3 như sau:

"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 an toàn phục vụ quản lý theo quy định về quản lý chất lượng sản phẩm mật mã dân sự được quy định của pháp luật.

3.2 Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 1; Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012. 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."

4.10 Trách nhiệm của tổ chức, cá nhân

Thay thế Điều 4 như sau:

"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."

4.11 Tổ chức thực hiện

Thay thế Điều 5 như sau:

" 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./."

4.12 Cập nhật mã HS tại Phụ lục

Thay thế bảng PHỤ LỤC A (Quy định) Quy định về mã HS của sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS như sau:

PHỤ LỤC

(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	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả sản phẩm hàng hóa
01	Sản phẩm bảo mật luồng IP	Sản phẩm sử dụng công nghệ VPN có bảo mật (IPSec VPN, TLS VPN) để đảm bảo an toàn, bảo mật cho dữ liệu truyền nhận trên môi trường mạng IP. Trong đó, sử dụng các thuật toán mã hóa đối xứng, thuật toán mã hóa phi đối xứng, thuật toán ký số, hàm băm mật mã để bảo mật, xác thực	8471.30.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; máy truyền dữ liệu lên các phương tiện truyền dẫn dữ liệu dưới dạng hàng hóa và máy xử lý những dữ liệu này, chưa được chi tiết hay ghi ở nơi khác gồm: - Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống.
02			8471.41.90	
03			8471.49.90	

04		các thông tin truyền nhận trên môi trường mạng IP.	8517.62.42	Thiết bị dùng cho hệ thống hữu tuyến sóng mang hoặc hệ thống hữu tuyến kỹ thuật số của hàng hóa là máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Bộ tập trung hoặc bộ dồn kênh; - Bộ điều khiển và bộ thích ứng (adaptor), kể cả cổng nối, cầu nối, bộ định tuyến và các thiết bị tương tự được thiết kế để kết nối với máy xử lý dữ liệu tự động thuộc nhóm 84.71; - Loại khác.
05			8517.62.43	
06			8517.62.49	
07			8517.62.51	Thiết bị truyền dẫn khác kết hợp với thiết bị thu của hàng hóa máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Thiết bị mạng nội bộ không dây; - Thiết bị phát khác dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác.
08			8517.62.53	
09			8517.62.59	
10			8517.62.61	Thiết bị truyền dẫn khác của hàng hóa máy thu, đổi và truyền hoặc tái tạo âm thanh, hình ảnh hoặc dạng dữ liệu khác, kể cả thiết bị chuyển mạch và thiết bị định tuyến gồm: - Dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác với loại dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến;
11			8517.62.69	
12			8517.62.91	
13			8517.62.92	
14			8517.62.99	

				- Loại khác là thiết bị thu xách tay để gọi, báo hiệu hoặc nhận tin và thiết bị cảnh báo bằng tin nhắn, kể cả máy nhắn tin; - Loại khác dùng cho điện báo hoặc điện thoại truyền dẫn dưới dạng sóng vô tuyến; - Loại khác với hàng hóa thuộc nhóm 8517.62.61, 8517.62.69, 8517.62.91, 8517.62.92.

5 Bảng đối chiếu nội dung QCVN với các tài liệu tham khảo

Tên nội dung	Tài liệu tham khảo	Phương án xây dựng
Bổ sung quy định đối với thuật toán MKV	TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV	Chấp nhận toàn vẹn
Loại bỏ thuật toán TDEA	NIST SP 800-131A Rev.2 (2019)	Chấp nhận toàn vẹn
Bổ sung quy định về an toàn đối với các thuật toán mật mã sử dụng chế độ CBC tại bảng 7 và mục 2.3	https://supportportal.juniper.net/s/article/End-of-support-for-cipher-suites-using-the-CBC-mode. https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode. https://cryptography.io/en/3.4.3/hazmat/primitives/symmetric-encryption.html https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10184306 https://learn.microsoft.com/en-us/security-updates/securityadvisories/2018/4338110 https://blog.ise.io/blog/the-dangers-of-cbc-mode https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062	Dựa theo khuyến nghị của các tổ chức
Loại bỏ thuật toán DSA	FIPS 186-5	Chấp nhận toàn vẹn

Loại bỏ thuật toán GOST R 34.10-2001	GOST R 34.10-2012 (RFC 7091)	Chấp nhận toàn vẹn
Bổ sung quy định thuật toán RSA	FIPS 186-5; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	Căn cứ ngưỡng dưới của quy định đối với các sản phẩm mật mã thuộc phạm vi bí mật nhà nước; Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định thuật toán DH	NIST SP 800-56A Rev. 3; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Bổ sung quy định thuật toán ECDH	NIST SP 800-56A Rev. 3; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Bổ sung quy định thuật toán ECDSA	FIPS 186-5; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Loại bỏ thuật toán CAST	NIST SP 800-52 Revision 2; NIST SP 800-131A Revision 2; TR-02102-1; TR-02102-2; TR-02102-3	Dựa theo khuyến nghị của các tổ chức
Loại bỏ thuật toán SEED		
Loại bỏ thuật toán Camellia		
Bổ sung quy định các thuật toán băm	TR-02102-1	Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định các thuật xác thực thông điệp	TR-02102-1; TR-02102-2; TR-02102-3	Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định thuật toán băm GOST R 34.11-2012	RFC 6986	Dựa theo khuyến nghị của các tổ chức
Chấp nhận kết quả thử nghiệm	Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật (2025)	Dựa theo khuyến

		nghị của các tổ chức
Cập nhật mã HS tại Phụ lục	Nghị định 211/2025/NĐ-CP	Chấp nhận toàn vẹn

6 Đánh giá tác động áp dụng Sửa đổi QCVN

Việc triển khai sửa đổi QCVN đối với *các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng ip sử dụng công nghệ IPsec và TLS* tại thời điểm này là vấn đề cấp thiết, liên quan trực tiếp đến công tác bảo đảm an toàn thông tin mạng, bảo vệ quyền riêng tư và lợi ích của người sử dụng. Quy chuẩn này áp dụng đối với các tổ chức, cá nhân sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

Các đối tượng chịu tác động khi QCVN được ban hành:

- Doanh nghiệp sản xuất/kinh doanh/nhập khẩu: phải đảm bảo đáp ứng QCVN và phải chứng nhận, công bố hợp quy khi kinh doanh sản phẩm tại thị trường Việt Nam.

- Người sử dụng (cơ quan, tổ chức, người tiêu dùng): Mức độ ảnh hưởng thấp do là đối tượng thụ hưởng cuối cùng. Các yếu tố an toàn được đảm bảo, bảo vệ lợi ích của người dùng cuối.

6.1. Tác động đến thị trường sản phẩm

* Tác động tích cực:

- Người sử dụng cuối (đối tượng áp dụng): Tăng cảm giác an tâm và tin tưởng khi sử dụng các sản phẩm mật mã dân sự đã được công bố hợp quy. Bảo vệ quyền riêng tư và dữ liệu cá nhân của họ trước các rủi ro mất an toàn thông tin. Giảm thiểu rủi ro mất dữ liệu quan trọng và thông tin nhạy cảm. Tăng khả năng đáp ứng các yêu cầu về bảo vệ dữ liệu và quyền riêng tư từ phía khách hàng và cơ quan quản lý. Tăng cảm giác an toàn và hỗ trợ cho việc xây dựng một môi trường sống và làm việc an toàn hơn.

- Nhà sản xuất: Nâng cao uy tín và niềm tin của khách hàng thông qua việc cung cấp các sản phẩm được chứng nhận hợp quy. Các sản phẩm nội địa chất lượng cao có cơ hội tiếp cận thị trường nước ngoài có yêu cầu cao.

- Nhà phân phối và bán lẻ: Có thể sử dụng chứng nhận hợp quy của sản phẩm làm lợi thế bán hàng để thu hút khách hàng và tăng doanh số bán hàng.

- Tổ chức đánh giá sự phù hợp và cấp chứng nhận: thuận lợi trong việc triển khai công tác đánh giá chất lượng sản phẩm mật mã dân sự, giảm thời gian kiểm định, đánh giá, tránh kiểm tra chồng chéo mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Tăng chi phí: Quá trình cấp chứng nhận hợp quy và công bố hợp quy có thể đòi hỏi đầu tư lớn vào việc nâng cấp và thay đổi công nghệ, làm tăng chi phí sản xuất và phân phối các sản phẩm bảo mật dữ liệu bảo mật luồng ip sử dụng công nghệ IPsec và TLS.

- Phức tạp hóa quy trình sản xuất: Việc tuân thủ các yêu cầu tại Sửa đổi Quy chuẩn có thể đòi hỏi các quy trình và thủ tục phức tạp hơn trong quá trình sản xuất, làm tăng chi phí và thời gian sản xuất.

- Giảm hiệu suất sản xuất: Tích hợp các biện pháp đảm bảo yêu cầu kỹ thuật có thể làm giảm hiệu suất sản xuất do tăng thời gian kiểm tra và thử nghiệm, cũng như việc áp dụng các quy trình kiểm soát chất lượng nghiêm ngặt hơn.

- Tăng thời gian tiến hành kiểm định và cấp chứng nhận: Quá trình đạt được chứng nhận hợp quy có thể đòi hỏi thời gian dài và tốn kém để thực hiện kiểm định, đánh giá sự phù hợp, làm trì hoãn việc tung ra thị trường và làm chậm quá trình phát triển sản phẩm mới.

6.2. Tác động đến cơ quan quản lý nhà nước chuyên ngành

* Tác động tích cực:

- Góp phần vào việc nâng cao an toàn và quản lý rủi ro trong quản lý nhà nước đối với lĩnh vực mật mã dân sự.

- Thuận lợi triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Cần hoàn thiện, nâng cao năng lực đo kiểm, đánh giá để thực hiện công tác đánh giá, cấp chứng nhận hợp quy cho sản phẩm.

- Cần hoàn thiện cơ chế hợp tác quốc tế, danh sách tổ chức được chỉ định, tổ chức quốc tế có năng lực được công nhận.

6.3. Tác động đến người sử dụng đầu cuối

- Người sử dụng đầu cuối là đối tượng được thụ hưởng tích cực khi sản phẩm được quản lý, bảo mật, đáp ứng các quy định của QCVN./.

7 Tài liệu tham khảo

[1]. QCVN 12:2022/BQP "Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng ip sử dụng công nghệ IPsec và TLS".

[2]. 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".

[3]. 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".

[4]. 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".

[5]. TCVN 11816 (ISO/IEC 10118) "Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng".

[6]. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) "Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác nhận thông điệp".

[7]. ISO/IEC 27040:2015 "Information technology – Security techniques – Storage security".

[8]. Federal Office for Information Security, BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths", January 2022.

[9]. National Information Assurance Partnership, "PP-Module for File Encryption Enterprise Management v1.0", 2019.

[10]. Common Criteria, "collaborative Protection Profile for USB Portable Storage Devices Version: 1.0", January 2015.

[11]. Common Criteria, "collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0", September 2016.

[12]. National Institute of Standards and Technology, Special Publication 800-131A "Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019.

[13]. National Institute of Standards and Technology, Special Publication 800-132 "Recommendation for Password-Based Key Derivation: Part 1: Storage Applications", December 2010.

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

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

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

[17]. National Institute of Standards and Technology, Special Publication 800-38E "Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices", January 2010.

[18]. National Institute of Standards and Technology, Special Publication 800-90A "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", June 2015.
[19]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 "Recommendation for Key Management: Part 1 – General", May 2020.
[20]. National Institute of Standards and Technology, Special Publication 800-56B Revision 2 "Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography", March 2019.
[21]. National Institute of Standards and Technology, Special Publication 800-38F, "Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping", December 2012.
[22]. 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.
[23]. National Institute of Standards and Technology, Special Publication 800-38C "Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality", July 2007.
[24]. Internet Engineering Task Force, "IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices", October 2018.
[25]. [RFC7801]: "GOST R 34.12-2015: Block Cipher "Kuznyechik"", Internet Engineering Task Force (IETF), March 2016.
[26]. [RFC 6986]: "GOST R 34.11-2012: Hash Function", Internet Engineering Task Force (IETF), December 2013.
[27]. [RFC7091]: "GOST R 34.10-2012: Digital Signature Algorithm", Internet Engineering Task Force (IETF), December 2013.
[28]. [RFC 9106]: "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications", Internet Engineering Task Force (IETF), September 2021.
[29]. [RFC 9058]: "Multilinear Galois Mode (MGM)", Internet Engineering Task Force (IETF), June 2021.
[30]. Bài báo "Argon2: the memory-hard function for password hashing and other applications", March 2017. https://www.password-hashing.net/argon2-specs.pdf
[31]. Bài báo "Password-Hashing Status", George Hatzivasilis, June 2017. https://www.researchgate.net/publication/317936505_Password-Hashing_Status
[32]. Bài báo "Towards Practical Attacks on Argon2i and Balloon Hashing", Joel Alwen và Jeremiah Blocki, 2017. https://ieeexplore.ieee.org/document/7961977

[33]. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
[34]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf?utm_source
[35]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
[36]. https://www.rfc-editor.org/rfc/rfc6986.html

BAN CƠ YẾU CHÍNH PHỦ

THUYẾT MINH

Dự thảo Sửa đổi Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ

Hà Nội, 2026

MỤC LỤC

1 Tên gọi và ký hiệu của QCVN

Tên gọi: Sửa đổi Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ.

Ký hiệu: SỬA ĐỔI 1:2026 QCVN 15:2023/BQP.

2 Đặt vấn đề

2.1 Tình hình thực tiễn

Quy chuẩn kỹ thuật quốc gia QCVN 15:2023/BQP ban hành và có hiệu lực từ ngày 15/01/2024. Tuy nhiên trong quá trình triển khai, Cơ quan quản lý chuyên ngành nhận thấy một số hạn chế như sau:

- Ngày 31/12/2024, Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quyết định số 3480/QĐ-BKHCN về việc công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV. Đây là thuật toán mã khối riêng của Việt Nam, do Ban Cơ yếu Chính phủ nghiên cứu, xây dựng, đề xuất ban hành. Thuật toán này hiện đang được cộng đồng doanh nghiệp quan tâm, nghiên cứu và tích hợp vào sản phẩm. Tuy nhiên trong các quy chuẩn kỹ thuật quốc gia, danh mục tiêu chuẩn bắt buộc áp dụng ban hành kèm theo Thông tư 96/2023/TT-BQP chưa cập nhật yêu cầu sử dụng với thuật toán mã khối MKV, cần thiết phải bổ sung đáp ứng yêu cầu thực tiễn sử dụng của xã hội;

- Một số nội dung kỹ thuật (*chế độ sử dụng, thời hạn sử dụng, kích thước khối*) trong quy chuẩn hiện hành đã không còn đáp ứng được các yêu cầu an toàn theo khuyến nghị từ các tổ chức quốc tế uy tín như NIST hay BSI, đặc biệt liên quan đến chế độ sử dụng và thời hạn sử dụng của sản phẩm hoặc hệ thống. Các quy định cũ có thể dẫn đến rủi ro cao hơn trong điều kiện vận hành thực tế, không đảm bảo an toàn thông tin.

- Bên cạnh đó, tại kỳ họp thứ 9 Quốc hội Khóa XIII thông qua Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó sửa đổi khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 với quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp như sau:

"2. Thừa nhận đơn phương kết quả đánh giá sự phù hợp được quy định như sau:

a) Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước;

b) Kết quả đánh giá sự phù hợp quy định tại điểm a khoản này phải được thực hiện bởi tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài được một trong các tổ chức công nhận là thành viên ký thỏa thuận thừa nhận lẫn nhau của Tổ chức Công nhận các phòng thử nghiệm Quốc tế (ILAC), Diễn đàn Công nhận

Quốc tế (IAF), Tổ chức hợp tác Công nhận khu vực Châu Á Thái Bình Dương (APAC) đánh giá và công nhận về năng lực đáp ứng tiêu chuẩn quốc tế, tiêu chuẩn quốc gia tương ứng;

Theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp quy định tại khoản này."

Căn cứ quy định trên, để phù hợp với yêu cầu thực tiễn của quản lý chất lượng sản phẩm mật mã dân sự tại Việt Nam, dự thảo Thông tư bổ sung quy định về thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức thử nghiệm nước ngoài đối với sản phẩm mật mã dân sự.

Do đó, việc sửa đổi và 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 bảo mật dữ liệu lưu giữ là cần thiết để khắc phục các hạn chế, nâng cao chất lượng sản phẩm MMDS, đảm bảo an toàn và đồng bộ với các văn bản pháp luật liên quan. Quy chuẩn sửa đổi đáp ứng yêu cầu thực tiễn, phù hợp với tiến bộ khoa học kỹ thuật, thúc đẩy hội nhập quốc tế, nâng cao năng lực cạnh tranh của doanh nghiệp Việt Nam và bảo vệ lợi ích người tiêu dùng, góp phần xây dựng hệ thống tiêu chuẩn hóa bền vững theo Luật Tiêu chuẩn và Quy chuẩn kỹ thuật.

2.2 Tình hình tiêu chuẩn hóa tại Việt Nam

Quy chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên quy chuẩn	Ghi chú
1	QCVN 4 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng	Ban hành kèm theo Thông tư 161/2016/TT-BQP ngày 21/10/2016
2	QCVN 5 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về chữ ký số sử dụng trong lĩnh vực ngân hàng	
3	QCVN 6 : 2016/BQP	Quy chuẩn kỹ thuật quốc gia về quản lý khóa sử dụng trong lĩnh vực ngân hàng	
4	QCVN 12 : 2022/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPsec và TLS	Ban hành kèm theo Thông tư 23/2022/TT-BQP ngày 04/4/2022
5	QCVN 15 : 2023/BQP	Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản	Ban hành kèm theo Thông tư

		phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ	96/2023/TT-BQP ngày 29/11/2023

Tiêu chuẩn kỹ thuật quốc gia trong lĩnh vực mật mã dân sự

TT	Ký hiệu	Tên tiêu chuẩn	Ghi chú
1	TCVN 7635:2007	Công nghệ thông tin – Kỹ thuật mật mã – Chữ ký số	
2	TCVN 7816:2007	Công nghệ thông tin – Kỹ thuật mật mã thuật toán mã dữ liệu AES	Phiên bản mới nhất TCVN 11367-3:2016
3	TCVN 7817-1:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 11770-3:2021
4	TCVN 7817-2:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 2: Cơ chế sử dụng kỹ thuật đối xứng	Phiên bản mới nhất ISO/IEC 11770-2:2018
5	TCVN 7817-3:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng	Phiên bản mới nhất ISO/IEC 11770-3:2021
6	TCVN 7817-4:2007	Công nghệ thông tin – Kỹ thuật mật mã quản lý khóa – Phần 4: Cơ chế dựa trên bí mật yếu	Phiên bản mới nhất ISO/IEC 11770-4:2017
7	TCVN 7818-1:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 1: Khung tổng quát	Phiên bản mới nhất ISO/IEC 18014-1:2008
8	TCVN 7818-2:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 2: Cơ chế token độc lập	Phiên bản mới nhất ISO/IEC 18014-2:2021
9	TCVN 7818-3:2007	Công nghệ thông tin – Kỹ thuật mật mã dịch vụ tem thời gian – Phần 3: Cơ chế tạo thẻ liên kết	Phiên bản mới nhất ISO/IEC 18014-3:2009
10	TCVN 11295:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an toàn cho mô-đun mật mã	

11	TCVN 11367-1:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 1: Tổng quan	Phiên bản mới nhất ISO/IEC 18033-1:2021
12	TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng	
13	TCVN 11367-3:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối	
14	TCVN 11367-4:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng	
15	TCVN 11816-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 1: Tổng quan	
16	TCVN 11816-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 2: Hàm băm sử dụng mã khối n-bit.	
17	TCVN 11816-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng	
18	TCVN 11816-4:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 4: Hàm băm sử dụng số học đồng dư	
19	TCVN 11817-1:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Tổng quan	
20	TCVN 11817-2:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 2: Cơ chế sử dụng thuật toán mã hóa đối xứng	
21	TCVN 11817-3:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Xác thực thực thể – Phần 1: Cơ chế sử dụng kỹ thuật chữ ký số	
22	TCVN 12214-1:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục - Phần 1: Tổng quan	
23	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	

24	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	
25	TCVN 11367-5:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 5: Mật mã dựa trên định danh	
26	TCVN 12211:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu kiểm thử cho mô đun mật mã	
27	TCVN 12212:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp kiểm thử giảm thiểu các lớp tấn công không xâm lấn chống lại các mô đun mật mã	
28	TCVN 12213:2018	Công nghệ thông tin - Các kỹ thuật an toàn - Chế độ hoạt động cho mã khối n-bit	
29	TCVN 12852-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 1: Tổng quan	
30	TCVN 12852-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Kỹ thuật mật mã dựa trên đường cong elliptic – Phần 5: Các kỹ thuật tạo đường cong elliptic	
31	TCVN 12853:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo bit ngẫu nhiên	
32	TCVN 12855-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 2: Các cơ chế dựa trên phân tích số nguyên	
33	TCVN 12855-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Lược đồ chữ ký số có khôi phục thông điệp – Phần 3: Các cơ chế dựa trên bài toán Logarit rời rạc	
34	TCVN 12854-1:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ -Phần 1: Tổng quan	
35	TCVN 12854-2:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 2: Mã khối	

36	TCVN 12854-3:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 3: Mã dòng	
37	TCVN 12854-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ - Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng	
38	TCVN 11817-4:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 4: Cơ chế sử dụng hàm kiểm tra mật mã	
39	TCVN 11817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 5: Cơ chế sử dụng kỹ thuật tri thức không tiết lộ thông tin	
40	TCVN 11817-6:2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể - Phần 6: Cơ chế sử dụng truyền dữ liệu thủ công	
41	TCVN 13175:2020	Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa ký	
42	TCVN 12854-5: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm	
43	TCVN 13176:2020	Công nghệ thông tin – Kỹ thuật an toàn – Bộ tạo số nguyên tố	
44	TCVN 13177:2020	Công nghệ thông tin – Kỹ thuật an toàn – Các thuật toán mật mã và kiểm thử phù hợp các cơ chế an toàn	
45	TCVN 7817-5:2020	Công nghệ thông tin – Kỹ thuật an toàn – Quản lý khóa - Phần 5: Nhóm quản lý khóa	
46	TCVN 13178-1: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 1: Tổng quan	
47	TCVN 13178-2: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 2: Các cơ chế dựa trên chữ ký sử dụng một nhóm khóa công khai	
48	TCVN 13178-4: 2020	Công nghệ thông tin – Kỹ thuật an toàn – Xác thực thực thể ẩn danh - Phần 4: Các cơ chế dựa trên bí mật yếu	

49	TCVN 11367-6:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 6: Mã hóa đồng cấu	
50	TCVN 13460-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 1: Tổng quan	
51	TCVN 13460-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số mù – Phần 2: Các cơ chế dựa trên logarit rời rạc	
52	TCVN 13461-1: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 1: Tổng quan	
53	TCVN 13461-2: 2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chữ ký số ẩn danh – Phần 2: Các cơ chế sử dụng một khóa công khai nhóm	
54	TCVN 13462-1:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 1: Tổng quan	
55	TCVN 13462-2:2022	Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản	
56	TCVN 13720:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Kiểm thử các mô-đun mật mã trong môi trường hoạt động,	
57	TCVN 13721:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Phương pháp kiểm thử và phân tích cho các bộ tạo bit ngẫu nhiên trong TCVN 11295 (ISO/IEC 19790) và TCVN 8709 (ISO/IEC 15408),	
58	TCVN 13722:2023	Công nghệ thông tin – Các kỹ thuật an toàn – Khung xác thực viễn sinh trắc sử dụng mô-đun an toàn phần cứng sinh trắc học	
59	TCVN 13723-1:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 1: Giới thiệu, khái niệm và yêu cầu chung	
60	TCVN 13723-2:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh	

		giá viên bảo mật thông tin – Phần 2: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với kiểm thử viên theo TCVN 11295 (ISO/IEC 19790)	
61	TCVN 13723-3:2023	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về năng lực đối với kiểm thử viên và đánh giá viên bảo mật thông tin – Phần 3: Yêu cầu về kiến thức, kỹ năng và tính hiệu quả đối với đánh giá viên theo TCVN 8709 (ISO/IEC 15408)	
62	TCVN 12197:2024	An toàn thông tin – Mã hóa có xác thực (ISO/IEC 19772:2020)	
63	TCVN 14190-1:2024	An toàn thông tin – Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học – Phần 1: Khung (ISO/IEC 19989-1:2020)	
64	TCVN 14190-2:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 2: Hiệu suất nhận dạng sinh trắc học (ISO/IEC 19989-2:2020)	
65	TCVN 14190-3:2024	An toàn thông tin – Tiêu chí và phương pháp đánh giá an toàn hệ thống sinh trắc học – Phần 3: Phát hiện tấn công trình diện (ISO/IEC 19989-3:2020)	
66	TCVN 14191-1:2024	An toàn thông tin – Biên tập lại dữ liệu xác thực – Phần 1: Yêu cầu chung (ISO/IEC 23263-1:2021)	
67	TCVN 14192-1:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-1:2019)	
68	TCVN 14192-2:2024	Kỹ thuật an toàn công nghệ thông tin – Yêu cầu về công cụ kiểm thử và phương pháp hiệu	

		chuẩn công cụ kiểm thử để sử dụng trong kiểm thử các kỹ thuật giảm thiểu tấn công không xâm lấn trong mô-đun mật mã – Phần 2: Phương pháp và phương tiện hiệu chuẩn kiểm thử (ISO/IEC 20085-2:2020)	
69	TCVN 14263:2024	Công nghệ thông tin – Kỹ thuật an toàn – Thuật toán mã khối MKV.	

2.3 Sự cần thiết xây dựng Sửa đổi Quy chuẩn

a) Về căn cứ

- Luật An toàn thông tin mạng năm 2015, tại khoản 7 Điều 38 giao "Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự"; khoản 4 Điều 52 quy định về trách nhiệm của Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng "xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự", "quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự, quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự".

- Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026, trong đó một số quy định về thoả thuận thừa nhận lẫn nhau, thừa nhận đơn phương kết quả đánh giá sự phù hợp tại khoản 2 Điều 57 Luật Tiêu chuẩn và quy chuẩn kỹ thuật năm 2006 được sửa đổi, bổ sung, tạo điều kiện cho việc thực hiện các quy định về đánh giá sự phù hợp trong lĩnh vực mật mã dân sự. Theo đó, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng xem xét, quyết định việc thừa nhận đơn phương kết quả đánh giá sự phù hợp của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước và "theo yêu cầu thực tiễn của quản lý chuyên ngành, Bộ, cơ quan ngang Bộ, Bộ trưởng Bộ Quốc phòng được xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp của các tổ chức đánh giá sự phù hợp ngoài các kết quả đánh giá sự phù hợp…".

- Nghị định số 211/2025/NĐ-CP ngày 25/7/2025 của Chính phủ quy định về hoạt động mật mã dân sự và sửa đổi, bổ sung một số điều của Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử được sửa đổi, bổ sung một số điều tại Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 của Chính phủ, tại Điều 10 quy định về thừa nhận kết quả đánh giá sự phù hợp sản phẩm mật mã dân sự "Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng xem xét, quyết định thừa nhận đơn phương kết quả đánh giá sự phù hợp sản phẩm mật mã dân

sự của tổ chức đánh giá sự phù hợp quốc tế, tổ chức đánh giá sự phù hợp nước ngoài để phục vụ hoạt động quản lý nhà nước về mật mã dân sự".

b) Về mục đích

Việc xây dựng chuẩn hóa "Sửa đổi Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ" là rất cần thiết nhằm:

- Đảm bảo chất lượng cho các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ.

- Thống nhất về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm bảo mật dữ liệu lưu giữ trên phạm vi toàn quốc.

- Là cơ sở kỹ thuật để các cơ quan quản lý tham chiếu, phục vụ công tác quản lý nhà nước về chất lượng sản phẩm bảo mật dữ liệu lưu giữ sử dụng trong lĩnh vực mật mã dân sự.

c) Về phạm vi áp dụng

Trên cơ sở phân tích lý do và mục đích xây dựng Sửa đổi quy chuẩn, nhóm biên tập quy chuẩn nhận thấy việc sửa đổi một số chỉ tiêu kỹ thuật cho sản phẩm bảo mật dữ liệu lưu giữ phục vụ bảo vệ thông tin không thuộc phạm vi bí mật nhà nước là rất cần thiết và phù hợp trong điều kiện hiện nay.

Nội dung Sửa đổi Quy chuẩn chỉ bao gồm nội dung sửa đổi, bổ sung một số quy định của QCVN 15:2023/BQP. Các nội dung không được nêu tại Sửa đổi Quy chuẩn này thì tiếp tục áp dụng QCVN 15:2023/BQP ban hành kèm theo Thông tư số 96/2023/TT-BQP ngày 21/11/2023 của Bộ trưởng Bộ Quốc phòng.

3 Cơ sở xây dựng các yêu cầu kỹ thuật

3.1 Cơ sở văn bản kỹ thuật trong nước

Khi xây dựng dự thảo quy chuẩn, cơ quan soạn thảo đã tham khảo các tài liệu sau:

- Quyết định số 3480/QĐ-BKHCN ngày 31/12/2024 của Bộ trưởng Bộ Khoa học và Công nghệ công bố tiêu chuẩn quốc gia TCVN 14263:2024 Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV.

- Thông tư số 96/2023/TT-BQP ngày 29/11/2023 của Bộ trưởng Bộ Quốc phòng ban hành Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ.

Trên cơ sở các tài liệu kỹ thuật tham khảo, cơ quan soạn thảo đã bổ sung, sửa đổi Quy chuẩn đáp ứng yêu cầu sử dụng thuật toán MKV, đáp ứng điều kiện thực tế đối với các sản phẩm đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế.

3.2 Cơ sở kinh nghiệm quốc tế

3.2.1 Cơ sở cho việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự.

Thực tiễn quốc tế cho thấy mức độ an toàn của các thuật toán mật mã và các tham số kỹ thuật liên quan có xu hướng thay đổi theo thời gian, phụ thuộc vào sự phát triển của khoa học công nghệ và năng lực tính toán. Các thuật toán và độ dài khóa hiện đang được sử dụng có thể không còn đáp ứng yêu cầu bảo đảm an toàn thông tin trong trung và dài hạn, đặc biệt đối với các thông tin có yêu cầu bảo mật cao hoặc thời gian bảo vệ kéo dài.

Trong bối cảnh đó, nhiều quốc gia và tổ chức tiêu chuẩn hóa đã ban hành các quy định và khuyến nghị nhằm quản lý việc lựa chọn, sử dụng và thay thế các thuật toán mật mã, trên cơ sở đánh giá định kỳ mức độ an toàn và phù hợp của các giải pháp kỹ thuật. Việc quy định ngưỡng kỹ thuật an toàn đối với sản phẩm mật mã dân sự được xem là một biện pháp cần thiết nhằm hạn chế rủi ro phát sinh từ việc tiếp tục sử dụng các thuật toán hoặc tham số kỹ thuật không còn đáp ứng yêu cầu bảo mật.

Các biện pháp quản lý được áp dụng phổ biến trong thực tiễn quốc tế bao gồm:

– Quy định thời hạn sử dụng hoặc chu kỳ rà soát đối với thuật toán và độ dài khóa, làm cơ sở để các tổ chức, cá nhân chủ động cập nhật, nâng cấp hoặc thay thế các giải pháp mật mã phù hợp với mức độ nhạy cảm của thông tin được bảo vệ;

– Tham chiếu và áp dụng các tiêu chuẩn, khuyến nghị mật mã do các tổ chức tiêu chuẩn hóa uy tín ban hành (như NIST, BSI), nhằm bảo đảm sự phù hợp với thông lệ quốc tế và hạn chế nguy cơ triển khai các thuật toán hoặc tham số kỹ thuật đã được đánh giá là không còn an toàn;

– Đối với dữ liệu có mức độ nhạy cảm cao hoặc có yêu cầu bảo vệ trong thời gian dài, định hướng sử dụng các thuật toán và độ dài khóa có mức an toàn cao hơn, đáp ứng yêu cầu bảo mật trong dài hạn và có khả năng thích ứng với sự phát triển của công nghệ;

– Xây dựng lộ trình chuyển đổi phù hợp từ các thuật toán mật mã khóa công khai truyền thống sang các thuật toán mới có mức độ an toàn cao hơn, bao gồm các thuật toán có khả năng chống chịu trước các tiến bộ về năng lực tính toán, trên cơ sở đánh giá rủi ro, mức độ nhạy cảm của dữ liệu và yêu cầu quản lý nhà nước trong từng giai đoạn.

3.2.2 Rà soát, cập nhật thuật toán mật mã

Bảng tổng hợp dưới đây các thuật toán mật mã đối xứng và các tấn công đã biết đối với từng thuật toán đó.

Thuật toán	Kích thước khóa theo bit	Kích thước khối theo bit	Các tấn công đã biết	Mô tả
AES	128, 192, 256	128	Chưa có các tấn công thám mã đã biết	Được mô tả trong FIPS 197. Đây là thuật toán mã khối công bố năm 1998 được chính phủ Mỹ làm chuẩn mã hóa, sau đó được NIST chấp thuận làm tiêu chuẩn và được sử dụng rộng rãi đến nay.
DES	56	64	Kích thước khối và khóa nhỏ, dễ bị tấn công bởi các phương pháp vét cạn, ngày sinh, vi sai, tuyến tính, khóa yếu.	Được mô tả trong FIPS 46-3. Đây là thuật toán mã khối được IBM phát triển, công bố năm 1975, và được chuẩn hóa năm 1976.
TDEA	128, 192	64	Vào năm 2016 một lỗ hổng lớn đã được phát hiện đối với thuật toán này sử dụng trong giao thức TLS, IPsec, SSH, được công bố tại CVE-2016-2183. Cuộc tấn công thực thi với thuật toán này là tấn công ngày sinh (Birthday attack).	Được mô tả trong SP 800-67. Đây là thuật toán mã khối, TDEA (còn biết đến với tên gọi Triple-DES) được công bố lần đầu năm 1981. Do lỗ hổng lớn được phát hiện nên NIST hạn chế và tiến tới loại bỏ trong các ứng dụng mới.
IDEA	128	64	Hạn chế của mã pháp này là kích thước khối nhỏ, lược đồ khóa đơn giản và chứa các lớp khóa yếu. Không có các tấn công thực tế, tuy nhiên có các tấn công lên số vòng nhỏ và khóa yếu. Tấn công tốt nhất lên IDEA là tấn công Bicliques.	Thuật toán mã khối được được thiết kế bởi James Massey của ETH Zurich và Xuejia Lai và được mô tả lần đầu tiên vào năm 1991. Thuật toán này ra đời nhằm thay cho thuật toán DES.

			• Khovratovich, Dmitry; Leurent, Gaëtan; *Rechberger*, Christian (2012). *Narrow-Bicliques: Cryptanalysis of Full IDEA. Advances in Cryptology – EUROCRYPT 2012.* Lecture Notes in Computer Science. **7237**. pp. 392–410 • Daemen, Joan; Govaerts, Rene; Vandewalle, Joos (1993), "Weak Keys for IDEA", *Advances in Cryptology, CRYPTO 93 Proceedings*: 224–231	
RC2	40	64	Kích thước khóa quá nhỏ, kích thước khối nhỏ. Dễ tổn thương trước các dạng tấn công khác nhau.	Thuật toán mã khối được thiết kế năm 1987 bởi Ron Rivest của hãng bảo mật RSA Data Security. RC2 còn được biết đến với tên gọi ARC2.
RC5	0-2040	32, 64, 128	Tồn tại một số tấn công lên phiên bản rút gọn 12-vòng với phiên bản kích thước khối 64-bit (thám mã vi sai) với độ phức tạp 2^{44} bản rõ chọn lọc.	Thuật toán mã khối được thiết kế bởi Ronald Rivest vào năm 1994.
RC6	128, 192, 256	128	Chưa có tấn công ảnh hưởng tới phiên bản đầy đủ	Thuật toán mã khối có nguồn gốc từ RC5 và được thiết kế bởi Ron Rivest, Matt Robshaw, Ray Sidney và Yiqun Lisa Yin để đáp ứng các yêu cầu của cuộc thi Tiêu chuẩn mã hóa nâng cao (AES).

ARIA	128, 192, 256	128	• *Wenling Wu; Wentao Zhang; Dengguo Feng (2006). "Impossible Differential Cryptanalysis of ARIA and Camellia". Retrieved January 19, 2007.* • *Xuehai Tang; Bing Sun; Ruilin Li; Chao Li (March 30, 2010). "A Meet-in-the-Middle Attack on ARIA". Retrieved April 24, 2010.*	Thuật toán mã khối được thiết kế vào năm 2003 bởi một nhóm lớn các nhà nghiên cứu của Hàn Quốc. Năm 2004 thuật toán này được chuẩn hóa và sử dụng tại Hàn Quốc.
Blowfish	32-448	64	Tấn công ngày sinh (vì kích thước khối nhỏ). Tồn tại các khóa yếu.	Thuật toán mã khối do Bruce Schneier thiết kế năm 1993 như một giải pháp thay thế miễn phí, nhanh chóng cho các thuật toán mã hóa hiện có tại thời điểm đó.
Camellia	128, 192, 256	128	Được đánh giá có mức độ an toàn tương đương trong các tiêu chuẩn quốc tế.	Thuật toán mã khối được phát triển bởi Mitsubishi Electric và NTT của Nhật Bản. Được công nhận trong chuẩn ISO/IEC. Thuật toán có mức độ bảo mật và khả năng xử lý tương đương với thuật toán AES.
SEED	128	128	Chưa có các tấn công đã biết với phiên bản đầy đủ.	Thuật toán mã khối được phát triển bởi KISA (Hàn Quốc) và được công bố trong chuẩn ISO/IEC 18033-3:2010 và nhiều RFC khác (như RFC 4010, RFC 4162, RFC 4196).
CAST	64	64	Kích thước khóa/khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán mã khối. Không có bản quyền, được mô tả trong RFC 2144.

CAST-128 (còn gọi là CAST5)	40-128	64	Kích thước khối quá nhỏ bị tấn công ngày sinh, các tấn công khác như vi sai tuyến tính.	Thuật toán được công bố vào năm 1996 bởi Carlisle Adams và Stafford Tavares. Thuật toán này cũng đã được Cơ quan An ninh Truyền thông phê duyệt cho Chính phủ Canada sử dụng.
CAST-256 (còn gọi là CAST6)	128, 192, 256	128	Tấn công tốt nhất là tấn công tương quan không (zero-correlation) với độ phức tạp thời gian là $2^{246.9}$ và dữ liệu là $2^{98.8}$. Tấn công này không ảnh hưởng tới độ an toàn của thuật toán. Bogdanov, Andrey; Leander, Gregor; Nyberg, Kaisa; Wang, Meiqin (2012). *Integral and multidimensional linear distinguishers with correlation zero. Lecture Notes in Computer Science*. **7658**. pp. 244–261.	Thuật toán mã khối, có nguồn gốc từ CAST-128. CAST-256 được xuất bản vào 6/1998. Được thiết kế theo thiết kế "CAST" do Carlisle Adams, Stafford Tavares phát minh và Howard Heys, Michael Wiener đóng góp vào thiết kế. CAST-256 được mô tả trong RFC 2612.
SM4	128	128	Chưa có tấn công đã biết nào được công bố.	Thuật toán mã khối, nó được nhiều cơ quan đầu ngành tại Trung Quốc phát triển nhưng chủ yếu được phát triển bởi Lü Shuwang. Tháng 8/2016 được chuẩn hóa tại Trung Quốc.

Dựa vào bảng trên, có thể thấy hầu hết các thuật toán có kích thước khối 128 bit giúp hạn chế các rủi ro liên quan đến tấn công ngày sinh, phù hợp với khuyến nghị của các tổ chức quốc tế, trong đó AES là thuật toán được nhắc đến nhiều nhất trong các tài liệu của tổ chức quốc tế uy tín (NIST, BSI, ANSI), được coi là chuẩn mặc định để đánh giá độ an toàn của các thuật toán khác. Hầu hết các tài liệu kỹ thuật (Whitepaper) và cấu hình mặc định đều chỉ liệt kê AES (Advanced Encryption Standard) với các độ dài khóa 128-bit hoặc 256-bit là lựa chọn duy nhất cho mã hóa đối xứng.

Qua rà soát danh mục sản phẩm mật mã dân sự và khảo sát thị trường tại Việt Nam, cơ quan soạn thảo nhận thấy đa số sản phẩm được khảo sát có tích hợp thuật toán

mã hóa AES, hiếm thấy sản phẩm tích hợp tùy chọn các thuật toán quốc tế hoặc nội địa khác (như Camellia, CAST, SEED, SM4), các thư viện mã nguồn mở mặc định sử dụng thuật toán AES hoặc không có các tùy chọn thuật toán khác, nếu có nhu cầu sử dụng, phải tùy biến, tích hợp vào mã nguồn.

Về mặt hỗ trợ phần cứng, hầu hết các CPU hiện đại (Intel, AMD, ARM) đều có tập lệnh hỗ trợ AES-NI, giúp việc mã hóa/giải mã bằng AES có tốc độ cực nhanh mà không tốn nhiều tài nguyên. Do vậy, việc sử dụng AES là đảm bảo tính tương thích cao, tiết kiệm chi phí khi sản phẩm cần giao tiếp, phổ biến rộng rãi với hệ thống quốc tế.

Để đảm bảo tính an toàn và hội nhập cùng thế giới, các sản phẩm, dịch vụ mật mã dân sự được kinh doanh, sử dụng tại thị trường Việt Nam cần có tính an toàn, ổn định, tương thích cao, đồng thời định hướng phát triển mật mã nội địa đảm bảo tự chủ bền vững. Do đó, cần xây dựng quy định chặt chẽ cho việc sử dụng các thuật toán mật mã phổ biến và thuật toán mật mã của Việt Nam. Cơ quan soạn thảo đã tham khảo các khuyến nghị quốc tế về an toàn mật mã để đưa ra các sửa đổi, bổ sung phù hợp với điều kiện sử dụng sản phẩm mật mã dân sự tại Việt Nam, đảm bảo cân bằng giữa bảo mật, hiệu suất, và khả năng triển khai thực tế. Các giải pháp này đảm bảo rằng mật mã dân sự đáp ứng được yêu cầu bảo mật ngắn hạn, đồng thời phù hợp với lộ trình cập nhật công nghệ để bảo vệ dữ liệu trong dài hạn.

a) Đối với thuật toán TDEA

Tài liệu NIST SP 800-131A Rev 2 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) cung cấp các quy định về khuyến nghị sử dụng và lộ trình chuyển đổi đối với các thuật toán mật mã và độ dài khóa như sau:

Thuật toán	Khuyến nghị sử dụng
3TDEA cho Mã hóa	Không được chấp nhận đến năm 2023 Không được phép sau năm 2023
3TDEA cho Giải mã	Sử dụng kế thừa
AES-128 cho Mã hóa và Giải mã	Được chấp nhận
AES-192 cho Mã hóa và Giải mã	Được chấp nhận
AES-256 cho Mã hóa và Giải mã	Được chấp nhận

Tại đây NIST đặt ra giới hạn và lộ trình sử dụng thuật toán TDEA:

- Việc sử dụng đối với các biện pháp bảo vệ mật mã mới (như mã hóa, đóng gói khóa, tạo MAC) được khuyến nghị chuyển đổi trước ngày 31 tháng 12 năm 2023 và sẽ bị ngừng phê duyệt từ ngày 1 tháng 1 năm 2024.

- Tuy nhiên, TDEA vẫn được phép dùng cho chức năng giải mã, mở gói khóa và xác minh MAC đối với dữ liệu đã được bảo vệ trước đó, nhằm hỗ trợ các hệ thống kế thừa trong quá trình chuyển đổi.

Thực hiện theo lộ trình này, NIST đã công bố thông báo ngày 29 tháng 6 năm 2023 về việc rút lại NIST SP 800-67 Rev.2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, có hiệu lực từ ngày 1 tháng 1 năm 2024.

b) Đối với chế độ XTS

Chế độ XTS (XEX-based Tweaked CodeBook mode with ciphertext stealing) được thiết kế chuyên biệt cho mã hóa dữ liệu lưu giữ theo khối, đặc biệt là mã hóa ổ đĩa và vùng lưu giữ dung lượng lớn.

XTS cho phép mã hóa độc lập từng đơn vị dữ liệu (sector hoặc block), hỗ trợ hiệu quả truy cập ngẫu nhiên mà không cần duy trì trạng thái giữa các khối. Việc sử dụng tham số tweak được dẫn xuất từ chỉ số vị trí lưu giữ giúp ngăn chặn các tấn công hoán đổi khối và sao chép dữ liệu giữa các vị trí khác nhau trong không gian lưu giữ. Ngoài ra, XTS không làm thay đổi kích thước dữ liệu và không phát sinh dữ liệu phụ cho mục đích xác thực, phù hợp với các hệ thống lưu giữ hiệu năng cao.

Với các đặc tính trên, XTS hiện là chế độ được khuyến nghị rộng rãi cho mã hóa dữ liệu lưu giữ và đã được triển khai trong nhiều hệ thống thực tế.

c)Đối với chế độ KW, KWP

Trong các hệ thống bảo mật dữ liệu lưu giữ, khóa mã hóa dữ liệu không được lưu giữ ở dạng rõ ràng mà phải được bảo vệ bằng các cơ chế bọc khóa chuyên dụng. Các chế độ KW (Key Wrap) và KWP (Key Wrap with Padding) được lựa chọn nhằm bảo đảm an toàn cho quá trình lưu giữ và vận chuyển khóa mã hóa dữ liệu.

KW và KWP cung cấp cơ chế bảo vệ khóa có kiểm soát, cho phép phát hiện thay đổi trái phép và bảo đảm tính toàn vẹn của khóa được bọc. Việc sử dụng các chế độ này phù hợp với các khuyến nghị quốc tế về quản lý khóa và đáp ứng yêu cầu phân tách mục đích sử dụng khóa, theo đó khóa dùng để bọc khóa không được sử dụng cho mã hóa dữ liệu và ngược lại.

Do đó, KW và KWP giữ vai trò thiết yếu trong kiến trúc bảo mật tổng thể của các sản phẩm bảo mật dữ liệu lưu giữ, mặc dù không trực tiếp tham gia vào quá trình mã hóa dữ liệu người dùng.

d)Đối với thuật toán Kuznyechik

Đối với thuật toán Kuznyechik, chế độ XTS được cho phép sử dụng do phù hợp với mục tiêu mã hóa dữ liệu lưu giữ theo khối, đáp ứng yêu cầu bảo mật dữ liệu lưu giữ và có phạm vi áp dụng rõ ràng.

Ngoài ra, chế độ MGM là chế độ mã hóa xác thực được quy định trong hệ tiêu chuẩn GOST, được thiết kế đồng bộ với thuật toán Kuznyechik, cho phép bảo đảm đồng thời tính bí mật và toàn vẹn dữ liệu. Việc lựa chọn MGM thay cho các chế độ AEAD khác nhằm bảo đảm tính nhất quán về hệ tiêu chuẩn và thuận lợi trong triển khai, đánh giá hợp chuẩn đối với các sản phẩm sử dụng thuật toán Kuznyechik.

Các chế độ CCM và GCM không được áp dụng cho thuật toán Kuznyechik trong Bảng 7 do không thuộc hệ chế độ được chuẩn hóa đồng bộ với thuật toán này. Việc không lựa chọn CCM và GCM đối với Kuznyechik không làm giảm mức độ an toàn của quy chuẩn, đồng thời bảo đảm tính rõ ràng, nhất quán và khả thi trong áp dụng.

e) Đối với chế độ CFB, OFB

Các chế độ CFB và OFB biến thuật toán mã hóa khối thành dạng mã hóa dòng, phụ thuộc vào trạng thái trước đó. Trong môi trường lưu giữ, các chế độ này không hỗ trợ tốt truy cập ngẫu nhiên theo khối và dễ bị ảnh hưởng bởi lỗi lan truyền hoặc các tấn công thao túng dữ liệu (bit-flipping attack) ở mức bit.

Ngoài ra, CFB và OFB không cung cấp cơ chế xác thực dữ liệu và yêu cầu quản lý chặt chẽ vector khởi tạo (IV), làm gia tăng rủi ro triển khai sai trong các hệ thống lưu giữ dung lượng lớn. Vì các lý do này, các chế độ CFB và OFB không đáp ứng được yêu cầu an toàn trong triển khai đối với một số dòng sản phẩm mật mã dân sự.

f) Đối với chế độ CBC

Chế độ Cipher Block Chaining (CBC) là chế độ hoạt động truyền thống của các thuật toán mã hóa khối đối xứng như AES và Kuznyechik (GOST R 34.12-2015). Tuy nhiên, trong bối cảnh bảo mật dữ liệu lưu giữ dài hạn, chế độ CBC không còn đáp ứng đầy đủ các yêu cầu về an toàn và khả năng triển khai, do đó không được khuyến nghị sử dụng cho các hệ thống mã hóa dữ liệu lưu giữ mới.

CBC chỉ cung cấp tính bí mật mà không tích hợp cơ chế bảo đảm toàn vẹn và xác thực dữ liệu. Trong môi trường lưu giữ, điều này dẫn đến nguy cơ bị thao túng dữ liệu, bao gồm thay đổi nội dung hoặc hoán đổi các khối dữ liệu đã mã hóa mà hệ thống không thể phát hiện nếu không triển khai thêm các cơ chế bảo vệ bổ sung. Việc kết hợp CBC với các cơ chế xác thực bên ngoài làm tăng độ phức tạp triển khai và không phù hợp với yêu cầu đơn giản, tin cậy của các hệ thống lưu giữ dung lượng lớn.

Bên cạnh đó, CBC không hỗ trợ hiệu quả truy cập ngẫu nhiên theo khối và không có cơ chế ràng buộc dữ liệu với vị trí lưu giữ. Do mỗi khối dữ liệu phụ thuộc vào khối liền trước, việc giải mã hoặc cập nhật dữ liệu tại một vị trí bất kỳ trở nên kém hiệu quả. Đồng thời, chế độ này không chống được các tấn công sao chép, hoán đổi hoặc phục hồi dữ liệu ban đầu, vốn là các mối đe dọa phổ biến trong môi trường lưu giữ.

Ngoài ra, việc quản lý vector khởi tạo (IV) trong CBC gặp nhiều khó khăn trong môi trường lưu giữ dữ liệu dài hạn. Yêu cầu IV không lặp lại và được quản lý chặt chẽ khó bảo đảm trong các hệ thống có hoạt động ghi đè, sao lưu và phục hồi dữ liệu, làm gia tăng nguy cơ suy giảm mức độ an toàn.

Trên cơ sở các phân tích nêu trên và theo các khuyến nghị hiện hành, chế độ CBC không được lựa chọn cho mã hóa dữ liệu mới. Chế độ này chỉ được dùng để giải mã dữ liệu đã được mã hóa trước đó trên hệ thống nhằm bảo đảm khả năng tương thích ngược, không khuyến nghị triển khai trong các hệ thống mới.

g) Đối với thuật toán DSA

- Hướng dẫn kỹ thuật "TR-02102-1" của BSI trình bày khuyến nghị về kích

thước khóa an toàn tối thiểu (công bố vào tháng 3 năm 2025), BSI đã nhấn mạnh rằng các thuật toán cổ điển (RSA, DSA, ECDSA, ECDH) có thể không còn đủ an toàn trước các cuộc tấn công lượng tử trong tương lai. Cơ quan soạn thảo tổng hợp lại khuyến nghị của BSI như sau:

STT	Thuật toán	Kích thước khóa theo bit	Năm sử dụng
1	RSA	2000	2022
		≥ 3000	2023 trở đi
2	DSA	2000	2022
		≥ 3000	2023 trở đi
4	ECDSA	≥ 250	2023 trở đi
5	ECDH	≥ 250	2023 trở đi

Ngày 03/02/2023, tổ chức NIST công bố tiêu chuẩn FIPS 186-5 Digital Signature Standard (DSS). Tiêu chuẩn này không còn chấp thuận DSA cho việc tạo chữ ký số. Tuy nhiên, DSA có thể được sử dụng để xác minh chữ ký được tạo trước ngày triển khai tiêu chuẩn này.

h) Đối với thuật toán GOST R 34.10-2001

Năm 2012, Liên bang Nga ban hành tiêu chuẩn GOST R 34.10-2012 để thay thế GOST R 34.10-2001, nhằm nâng cao cường độ bảo mật cho thuật toán chữ ký số dựa trên đường cong elliptic, khắc phục các hạn chế về độ mạnh toán học và khả năng chống tấn công của phiên bản cũ (theo RFC 7091 và các chỉ đạo từ Cơ quan Tiêu chuẩn Kỹ thuật Nga). GOST R 34.10-2001 sau đó bị coi là lỗi thời, bị loại khỏi các ứng dụng mới trong các tiêu chuẩn quốc tế như DNSSEC (IETF chuyển trạng thái historic năm 2024) và không còn được khuyến nghị sử dụng do rủi ro bảo mật tiềm ẩn so với các thuật toán hiện đại.

e) Đối với thuật toán GOST R 34.11-2012

Năm 2012, Liên bang Nga ban hành tiêu chuẩn GOST R 34.11-2012 (còn gọi là Streebog) để thay thế GOST R 34.11-94, nhằm nâng cao cường độ bảo mật cho thuật toán hàm băm mật mã, khắc phục các hạn chế về độ mạnh toán học và khả năng chống tấn công của phiên bản cũ (theo RFC 6986 và các chỉ đạo từ Cơ quan Tiêu chuẩn Kỹ thuật Nga - Rosstandart).

f) Đối với việc điều chỉnh thời hạn sử dụng thuật toán băm, thuật toán xác thực thông điệp, hàm dẫn xuất khóa và bộ tạo số ngẫu nhiên

Việc điều chỉnh thời hạn sử dụng các thuật toán băm, thuật toán xác thực thông điệp, hàm dẫn xuất khóa và bộ tạo số ngẫu nhiên từ mốc năm 2027 kéo dài đến hết năm

2030 được đề xuất trên cơ sở rà soát các khuyến nghị hiện hành của các tổ chức chuẩn hóa uy tín như NIST, BSI và ANSI, đồng thời đối chiếu với thực tiễn triển khai và áp dụng trong nước.

Theo các khuyến nghị nêu trên, các thuật toán băm thuộc họ SHA-2 và SHA-3; các cơ chế xác thực thông điệp dựa trên HMAC tương ứng; các hàm dẫn xuất khóa PBKDF2 và Argon2; cũng như các bộ tạo số ngẫu nhiên xác định (DRBG) và không xác định (NRBG) như Hash_DRBG, HMAC_DRBG, CTR_DRBG (AES), XOR-NRBG và Oversampling-NRBG hiện vẫn được đánh giá đáp ứng mức an toàn mật mã tương đương từ 128 bit trở lên. Các thuật toán và cơ chế này do đó vẫn phù hợp để tiếp tục sử dụng an toàn trong các hệ thống mật mã đến sau năm 2030 đối với đa số kịch bản ứng dụng.

Bên cạnh đó, một số thuật toán và cơ chế nêu trên, đặc biệt là Argon2 và các bộ tạo số DRBG/NRBG, vẫn đang được các tổ chức chuẩn hóa quốc tế tiếp tục cập nhật và hoàn thiện trong các tài liệu hướng dẫn mới, cho thấy chúng chưa bị xem là lỗi thời hoặc cần loại bỏ trong giai đoạn hiện tại.

Trên cơ sở các phân tích nêu trên, việc kéo dài thời hạn áp dụng các thuật toán này đến hết năm 2030 nhằm bảo đảm tính liên tục và ổn định của hệ thống tiêu chuẩn, đồng thời không làm suy giảm mức độ an toàn mật mã. Việc rà soát, điều chỉnh tiếp theo sẽ được thực hiện căn cứ vào các đánh giá và khuyến nghị quốc tế mới được ban hành sau mốc thời gian này.

3.3 Cơ sở thực tiễn và căn cứ thừa nhận kết quả đánh giá sự phù hợp

Công tác quản lý chất lượng sản phẩm mật mã dân sự, đánh giá chứng nhận hợp chuẩn, hợp quy sản phẩm mật mã dân sự trong nước gặp nhiều khó khăn trong quá trình triển khai do thực trạng hiện nay ở Việt Nam chưa có tổ chức thử nghiệm đạt các chứng chỉ về thử nghiệm sản phẩm mật mã dân sự và được chỉ định (ISO/IEC 17025). Các quy chuẩn kỹ thuật trong lĩnh vực mật mã dân sự tại Việt Nam được xây dựng được xây dựng trên cơ sở hài hòa với tiêu chuẩn quốc tế. Cùng với đó, đa số các sản phẩm mật mã dân sự hiện nay được nhập khẩu từ nước ngoài và đã được đánh giá bởi các tổ chức uy tín, có năng lực. Về cơ bản, đối với sản phẩm có chung tiêu chuẩn kỹ thuật, kết quả đánh giá từ các tổ chức quốc tế có năng lực được công nhận không có sai lệch, khác biệt và đảm bảo rằng việc đánh giá tuân thủ quy chuẩn là nhất quán và công bằng. Do vậy, việc chấp nhận kết quả thử nghiệm từ tổ chức được chỉ định và tổ chức nước ngoài được công nhận theo ISO/IEC 17025 trong khi điều kiện trong nước chưa thực hiện được là phù hợp để triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

4 Nội dung Sửa đổi Quy chuẩn kỹ thuật quốc gia Sửa đổi 1:2025 QCVN 15:2023/BQP bao gồm các nội dung bổ sung, thay thế các quy định của QCVN 15:2023/BQP

Căn cứ vào quá trình rà soát các sản phẩm bảo mật dữ liệu lưu giữ đã được Ban Cơ yếu Chính phủ cấp phép; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng với thuật toán mã khối MKV; Căn cứ vào tính cấp thiết phải cập nhật yêu cầu sử dụng các thuật toán mật mã nhằm bảo đảm an toàn thông tin trong bối cảnh xuất hiện các nguy cơ từ máy tính lượng tử; Căn cứ vào tình hình triển khai thực tế của Quy chuẩn kỹ thuật đã được ban hành; Xem xét từ những yêu cầu, khuyến nghị được nêu ra trong các tài liệu tham khảo từ các tổ chức NIST, CC, BSI, cơ quan soạn thảo đề xuất sửa đổi như sau:

4.1 Nguyên tắc xây dựng nội dung

- Các tham số an toàn được lựa chọn theo các khuyến nghị của ISO/IEC, NIST, CC, BSI và các tổ chức quốc tế khác để đảm bảo an toàn và phù hợp;

- Phù hợp với điều kiện thực tế đối với các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ đang được lưu thông, sử dụng tại Việt Nam và các sản phẩm thương mại phổ biến của quốc tế;

- Đáp ứng được sự phát triển của công nghệ trong vòng 5 năm tới.

4.2 Bổ sung quy định đối với thuật toán MKV

- Bổ sung vào tài liệu viện dẫn (Mục 1.3);

"TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV".

- Bổ sung chữ viết tắt tại mục 1.5 như sau:

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
MKV		Mã khối Việt Nam

- Bổ sung thuật toán MKV vào danh mục thuật toán mật mã đối xứng được phép sử dụng như sau:

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024]

4.3 Sửa đổi danh mục thuật toán mã hóa đối xứng

Tại Bảng 1 mục 2.1.1:

- Loại bỏ thuật toán TDEA (tại cả bảng chữ viết tắt mục 1.5);

- Bổ sung thuật toán MKV;

- Thay thế tên thuật toán GOST R 34.12-2015 bằng thuật toán Kuznyechik.

- Sửa đổi tài liệu tham chiếu tới các thuật toán mã hóa

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

STT	Thuật toán	Tham chiếu
1	MKV	[TCVN 14263:2024]
2	AES	[TCVN 11367-3]
3	Kuznyechik	[GOST R 34.12-2015] [RFC 7801]

Tại Bảng 7 mục 2.2.1:

- Bổ sung quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán MKV;

- Loại bỏ thuật toán TDEA;

- Đối với thuật toán AES:

+ Điều chỉnh thời hạn sử dụng đến năm 2028 đối với kích thước khóa theo bit 128; Đối với kích thước khóa theo bit là 192, 256, điều chỉnh thời hạn sử dụng đến năm 2030;

- Đối với thuật toán GOST R 34.12-2015:

+ Thay thế tên thuật toán GOST R 34.12-2015 bằng thuật toán Kuznyechik;

+ Điều chỉnh thời hạn sử dụng đến năm 2030;

- Bổ sung chế độ MGM; điều chỉnh thời hạn sử dụng đến năm 2030;

- Quy định chế độ CBC chỉ để giải mã đối với toàn bộ thuật toán, điều chỉnh thời hạn sử dụng đến năm 2028.

Bảng 7 – Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với 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	MKV	128	XTS, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028
2	AES	128	XTS, CCM, GCM, KW, KWP	2028
		192, 256		2030
		128, 192, 256	CBC (chỉ để giải mã)	2028

3	Kuznyechik	256	XTS, MGM	2030
			CBC (chỉ để giải mã)	2028

CHÚ THÍCH:

Đối với thuật toán MKV, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo TCVN 14263:2024.

Đối với thuật toán AES, độ dài tham số, cấu trúc thuật toán và các chu trình tạo khóa trong quy chuẩn này áp dụng theo FIPS 197 hoặc TCVN 11367-3:2016.

Đối với thuật toán Kuznyechik, độ dài tham số, các chu trình tạo khóa, bộ tham số cụ thể trong quy chuẩn này áp dụng theo GOST R 34.12-2015 (RFC 7801).

Các chế độ của mã khối trong quy chuẩn này áp dụng theo TCVN 12213, SP 800-38C, SP 800-38D, SP 800-38E, SP 800-38F, RFC 9058.

4.4 Thuật toán mật mã phi đối xứng

Tại Mục 1.6 Ký hiệu:

- Cập nhật mô tả của ký hiệu *nlen*;
- Loại bỏ thuật toán DSA (tại cả bảng chữ viết tắt) và GOST R34.10-2001;
- Bổ sung ký hiệu và mô tả đối với thuật toán FFDH (bổ sung tại bảng chữ viết tắt).

Ký hiệu	Mô tả
nlen	Độ dài modulo theo bit hoặc độ dài theo bit của cấp của phần tử sinh
L	Đối với thuật toán FFDH: *L* là độ dài của tham số miền *p* theo bit
N	Đối với thuật toán FFDH: *N* là độ dài của tham số miền *q* theo bit

Tại Bảng 2 Mục 2.1.2:

- Loại bỏ thuật toán DSA và GOST R34.10-2001;
- Bổ sung, cập nhật các tài liệu, tiêu chuẩn tham chiếu mới nhất đối với các thuật toán mật mã phi đối xứng.

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

STT	Thuật toán	Tham chiếu
1	RSA	[FIPS 186-5], [SP 800-56B Rev. 2]

2	FFDH	[SP 800-56A Rev. 3], [RFC 2631], [RFC 3526], [RFC 7919]
3	ECDSA	[FIPS 186-5], [RFC 6090], [SP 800-186]
4	ECDH	[SP 800-56A Rev. 3], [SP 800-56C Rev. 2]
5	GOST R34.10-2012	[RFC 7091]

Tại Bảng 8 Mục 2.2.2:

- Loại bỏ thuật toán DSA và GOST R34.10-2001;

- Đối với thuật toán RSA: Điều chỉnh thời hạn sử dụng đến năm 2028 đối với kích thước tham số theo bit $2048 \leq nlen < 3072$, đến năm 2030 với $nlen = 3072$ (để phù hợp với lộ trình cập nhật công nghệ);

- Bổ sung thuật toán FFDH, ECDH (dựa trên khuyến nghị của tổ chức BSI).

- Đối với thuật toán FFDH: Điều chỉnh thời hạn sử dụng đến năm 2030, sửa đổi kích thước tham số theo bit $2048 \leq L \leq 3072$, $256 \leq N \leq 384$ (để phù hợp với lộ trình cập nhật công nghệ);

- Đối với thuật toán ECDH, ECDSA: Điều chỉnh thời hạn sử dụng đến năm 2030, sửa đổi kích thước tham số theo bit thành $250 \leq nlen \leq 384$ (để phù hợp với lộ trình cập nhật công nghệ);

- Đối với thuật toán GOST R 34.10-2012: Điều chỉnh thời hạn sử dụng từ 2027 lên 2030 (theo các khuyến nghị chung về mật mã hậu lượng tử).

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

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
1	RSA	$2048 \leq nlen < 3072$	2028
		$nlen = 3072$	2030
2	FFDH	$2048 \leq L \leq 3072$, $256 \leq N \leq 384$	2030

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm
3	ECDH, ECDSA	$250 \leq nlen \leq 384$	2030
4	GOST R 34.10-2012	$nlen \geq 256$	2030

CHÚ THÍCH:

Đối với RSA và ECDSA, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo FIPS 186-5.

Đối với FFDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3.

Đối với ECDH, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể trong quy chuẩn áp dụng theo NIST SP 800-56A Rev.3.SP 800-56C Rev. 2.

Đối với GOST R 34.10-2012, các tiêu chuẩn cho tham số an toàn, các thuật toán sinh khóa và các bộ tham số cụ thể áp dụng theo trong quy chuẩn này áp dụng theo GOST R 34.10-2012 (RFC 7091).

4.5 Thuật toán băm

Tại Bảng 3: Bổ sung thuật toán băm như sau:

STT	Thuật toán	Tham chiếu
1	GOST R 34.11-2012	[RFC 6986]

Tại bảng 9: Bổ sung quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán băm như sau:

STT	Thuật toán	Sử dụng đến năm
1	GOST R 34.11-2012	2030

CHÚ THÍCH:

Đối với GOST R 34.11-2012, các tiêu chuẩn cho tham số an toàn và các bộ tham số cụ thể áp dụng theo trong quy chuẩn này áp dụng theo GOST R 34.11-2012 (RFC 6986).

4.6 Thời hạn sử dụng

Điều chỉnh thời gian được phép sử dụng tại cột "Sử dụng đến năm" trong các bảng 10 mục 2.2.4, bảng 11 mục 2.2.5 và bảng 12 mục 2.2.6 như sau:

Sửa năm "2027" thành năm "2030".

4.7 Quy định về an toàn trong sử dụng

Tại mục 2.3 Quy định về an toàn trong sử dụng, cập nhật mục 2.3:

- Trong mã hóa/giải mã dữ liệu bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: XTS, CCM, GCM, MGM.

- Trong bọc khóa bằng thuật toán mã hóa đối xứng phải sử dụng một trong các chế độ sau: KW, KWP, CCM, GCM.

- Đối với chế độ CBC, chỉ được phép sử dụng để giải mã dữ liệu cũ, không dùng để mã hóa dữ liệu mới.

- Các khóa mật mã chỉ được sử dụng cho một mục đích, không được phép sử dụng chung khóa để mã hóa khóa và mã hóa dữ liệu

- Đối với thuật toán RSA, chỉ được phép sử dụng lược đồ KTS-OAEP và KTS-KEM-KWS cho vận chuyển khóa.

- Trong mã hóa dữ liệu được truyền tải, áp dụng hai giao thức IPSec và TLS (phiên bản TLS 1.2 và TLS 1.3) để cung cấp khả năng bảo vệ bổ sung (nếu có).

4.8 Quy định về quản lý, chấp nhận kết quả thử nghiệm

- Thay thế mục 3.1 bằng:

"Các mức giới hạn của đặc tính kỹ thuật mật mã nêu 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 của pháp luật."

- Thay thế mục 3.2 bằng:

"Công bố hợp quy, chứng nhận hợp quy, kiểm tra chất lượng sản phẩm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 của Bộ khoa học và Công nghệ quy định về công bố hợp chuẩn, công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật, trong Quy chuẩn này được thực hiện theo phương thức 1; Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 của Bộ khoa học và Công nghệ sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012. 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."

- Thay thế mục 3.4 bằng:

"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."

4.9 Trách nhiệm của tổ chức, cá nhân

Chuyển mục 3.5 thành mục 4.1, thay thế như sau:

"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."

4.10 Tổ chức thực hiện:

Bổ sung mục 5.4 vào Điều 5 như sau:

"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."

4.11 Cập nhật mã HS tại Phụ lục

Cập nhật các thay đổi tại Nghị định 211/2025.NĐ-CP của Chính phủ, thay thế bảng Phụ lục Quy định về mã HS của sản phẩm bảo mật dữ liệu lưu giữ như sau

STT	Tên sản phẩm	Mô tả đặc tính kỹ thuật mật mã	Mã HS	Mô tả hàng hóa
01	Sản phẩm bảo mật dữ liệu lưu giữ	Sản phẩm sử dụng các thuật toán mật mã, kỹ thuật mật mã để bảo vệ dữ liệu lưu giữ trên thiết bị	8523.51.11	Các thiết bị lưu trữ bền vững, thể rắn của hàng hóa là đĩa, băng, các thiết bị lưu trữ bền vững, thể rắn, "thẻ thông minh" và các phương tiện lưu trữ thông tin khác để ghi âm thanh hoặc các nội dung, hình thức thể hiện khác, đã hoặc chưa ghi, kể cả bản khuôn mẫu và bản gốc để sản xuất ghi băng đĩa, nhưng không bao gồm các sản phẩm của vật liệu ảnh hoặc điện ảnh gồm: - Loại dùng cho máy vi tính của loại chưa ghi; - Loại dùng cho máy vi tính của loại để tái tạo các hiện tượng trừ âm thanh hoặc hình ảnh; - Loại khác với hàng hóa thuộc nhóm 8523.51.11, 8523.51.21.
02			8523.51.21	
03			8523.51.99	

04			8523.52.00	- "Thẻ thông minh".
05			8525.81.10	Thiết bị phát dùng cho phát thanh sóng vô tuyến hoặc truyền hình, có hoặc không gắn với thiết bị thu hoặc ghi hoặc tái tạo âm thanh; camera truyền hình, camera kỹ thuật số và camera ghi hình ảnh gồm: - Camera ghi hình ảnh; - Camera truyền hình; - Loại khác.
06			8525.81.20	
07			8525.81.90	
08			8542.32.00	Bộ nhớ của mạch điện tử tích hợp.
09			8471.30.90	Máy xử lý dữ liệu tự động và các khối chức năng của chúng; đầu đọc từ tính hoặc đầu đọc quang học, máy truyền dữ liệu lên các phương tiện truyền dữ liệu dưới dạng mã hóa và máy xử lý những dữ liệu này, chưa được chi tiết hoặc ghi ở nơi khác gồm: - Loại khác của hàng hóa là máy xử lý dữ liệu tự động loại xách tay, có trọng lượng không quá 10 kg, gồm ít nhất một đơn vị xử lý dữ liệu trung tâm, một bàn phím và một màn hình; - Loại khác của hàng hóa chứa trong cùng một vỏ có ít nhất một
10			8471.41.90	
11			8471.49.90	
12			8471.80.90	

				đơn vị xử lý trung tâm, một đơn vị nhập và một đơn vị xuất, kết hợp hoặc không kết hợp với nhau; - Loại khác, ở dạng hệ thống; - Loại khác của hàng hóa là các bộ máy khác của máy xử lý dữ liệu tự động.

5 Bảng đối chiếu nội dung QCVN với các tài liệu tham khảo

Tên nội dung	Tài liệu tham khảo	Phương án xây dựng
Bổ sung quy định đối với thuật toán MKV	TCVN 14263:2024 "Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV"	Chấp nhận toàn vẹn
Loại bỏ thuật toán TDEA	NIST SP 800-131A Rev.2 (2019)	Chấp nhận toàn vẹn
Bổ sung quy định về an toàn đối với các thuật toán mật mã sử dụng chế độ CBC tại bảng 7 và mục 2.3	NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode. NIST Special Publication 800-57, Recommendation for Key Management. IEEE Std 1619, Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths. Common Criteria Portal, Supporting Documents and Guidance.	Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định về chế độ MGM	RFC 9058	Chấp nhận toàn vẹn
Loại bỏ thuật toán	FIPS 186-5	Chấp nhận toàn

DSA		vẹn
Loại bỏ thuật toán GOST R 34.10-2001	GOST R 34.10-2012 (RFC 7091)	Chấp nhận toàn vẹn
Bổ sung quy định thuật toán RSA	FIPS 186-5; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, NIST SP 800-56B Rev. 2	Căn cứ ngưỡng dưới của quy định đối với các sản phẩm mật mã thuộc phạm vi bí mật nhà nước; Dựa theo khuyến nghị của các tổ chức
Bổ sung quy định thuật toán FFDH	NIST SP 800-56A Rev. 3; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, NIST SP 800-56C Rev. 2, RFC 2631, RFC 3526, RFC 7919	
Bổ sung quy định thuật toán ECDH	NIST SP 800-186, NIST SP 800-56A Rev. 3; NIST SP 800-56C Rev. 2; TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5	
Bổ sung quy định thuật toán ECDSA	FIPS 186-5; NIST SP 800-186, TR-02102-1; NIST Special Publication 800-57 Part 1 Revision 5, RFC 6090	
Bổ sung quy định thuật toán GOST R 34.10-2012	RFC 7091	
Chấp nhận kết quả thử nghiệm	Luật Sửa đổi, bổ sung một số điều của Luật Tiêu chuẩn và quy chuẩn kỹ thuật (2025)	Dựa theo khuyến nghị của các tổ chức
Cập nhật mã HS tại Phụ lục	Nghị định 211/2025/NĐ-CP	Chấp nhận toàn vẹn

6 Đánh giá tác động áp dụng Sửa đổi QCVN

Việc triển khai sửa đổi QCVN đối với *các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ* tại thời điểm này là vấn đề cấp thiết, liên quan trực tiếp đến công tác bảo đảm an toàn thông tin mạng, bảo vệ quyền riêng tư và lợi ích của người sử dụng. Quy chuẩn này áp dụng đối với các tổ chức, cá nhân sản xuất, kinh doanh và sử dụng sản phẩm mật mã dân sự để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

Các đối tượng chịu tác động khi QCVN được ban hành:

- Doanh nghiệp sản xuất/kinh doanh/nhập khẩu: phải đảm bảo đáp ứng QCVN và phải chứng nhận, công bố hợp quy khi kinh doanh sản phẩm tại thị trường Việt Nam.

- Người sử dụng (cơ quan, tổ chức, người tiêu dùng): Mức độ ảnh hưởng thấp do là đối tượng thụ hưởng cuối cùng. Các yếu tố an toàn được đảm bảo, bảo vệ lợi ích của người dùng cuối.

6.1. Tác động đến thị trường sản phẩm

* Tác động tích cực:

- Người sử dụng cuối (đối tượng áp dụng): Tăng cảm giác an tâm và tin tưởng khi sử dụng các sản phẩm mật mã dân sự đã được công bố hợp quy. Bảo vệ quyền riêng tư và dữ liệu cá nhân của họ trước các rủi ro mất an toàn thông tin. Giảm thiểu rủi ro mất dữ liệu quan trọng và thông tin nhạy cảm. Tăng khả năng đáp ứng các yêu cầu về bảo vệ dữ liệu và quyền riêng tư từ phía khách hàng và cơ quan quản lý. Tăng cảm giác an toàn và hỗ trợ cho việc xây dựng một môi trường sống và làm việc an toàn hơn.

- Nhà sản xuất: Nâng cao uy tín và niềm tin của khách hàng thông qua việc cung cấp các sản phẩm được chứng nhận hợp quy. Các sản phẩm nội địa chất lượng cao có cơ hội tiếp cận thị trường nước ngoài có yêu cầu cao.

- Nhà phân phối và bán lẻ: Có thể sử dụng chứng nhận hợp quy của sản phẩm làm lợi thế bán hàng để thu hút khách hàng và tăng doanh số bán hàng.

- Tổ chức đánh giá sự phù hợp và cấp chứng nhận: thuận lợi trong việc triển khai công tác đánh giá chất lượng sản phẩm mật mã dân sự, giảm thời gian kiểm định, đánh giá, tránh kiểm tra chồng chéo mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Tăng chi phí: Quá trình cấp chứng nhận hợp quy và công bố hợp quy có thể đòi hỏi đầu tư lớn vào việc nâng cấp và thay đổi công nghệ, làm tăng chi phí sản xuất và phân phối các sản phẩm bảo mật dữ liệu lưu giữ.

- Phức tạp hóa quy trình sản xuất: Việc tuân thủ các yêu cầu tại Sửa đổi Quy chuẩn có thể đòi hỏi các quy trình và thủ tục phức tạp hơn trong quá trình sản xuất, làm tăng chi phí và thời gian sản xuất.

- Giảm hiệu suất sản xuất: Tích hợp các biện pháp đảm bảo yêu cầu kỹ thuật có thể làm giảm hiệu suất sản xuất do tăng thời gian kiểm tra và thử nghiệm, cũng như việc áp dụng các quy trình kiểm soát chất lượng nghiêm ngặt hơn.

- Tăng thời gian tiến hành kiểm định và cấp chứng nhận: Quá trình đạt được chứng nhận hợp quy có thể đòi hỏi thời gian dài và tốn kém để thực hiện kiểm định, đánh giá sự phù hợp, làm trì hoãn việc tung ra thị trường và làm chậm quá trình phát triển sản phẩm mới.

6.2. Tác động đến cơ quan quản lý nhà nước chuyên ngành

* Tác động tích cực:

- Góp phần vào việc nâng cao an toàn và quản lý rủi ro trong quản lý nhà nước đối với lĩnh vực mật mã dân sự.

- Thuận lợi triển khai công tác quản lý nhà nước, quản lý chất lượng sản phẩm mật mã dân sự, đồng thời tạo thuận lợi cho thương mại quốc tế, tránh kiểm tra chồng chéo, giảm chi phí cho doanh nghiệp mà vẫn đảm bảo rằng các sản phẩm, hàng hóa trên thị trường đáp ứng đầy đủ yêu cầu về an toàn, chất lượng và bảo vệ người tiêu dùng.

* Tác động không tích cực:

- Cần hoàn thiện, nâng cao năng lực đo kiểm, đánh giá để thực hiện công tác đánh giá, cấp chứng nhận hợp quy cho sản phẩm.

- Cần hoàn thiện cơ chế hợp tác quốc tế, danh sách tổ chức được chỉ định, tổ chức quốc tế có năng lực được công nhận.

6.3. Tác động đến người sử dụng đầu cuối

Người sử dụng đầu cuối là đối tượng được thụ hưởng tích cực khi sản phẩm được quản lý, bảo mật, đáp ứng các quy định của QCVN./.

Tài liệu tham khảo

[1]. QCVN 15:2023/BQP "*Quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật dữ liệu lưu giữ*".

[2]. TCVN 14263:2024 "*Công nghệ thông tin - Kỹ thuật an toàn - Thuật toán mã khối MKV*".

[3]. 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*".

[4]. 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*".

[5]. Federal Office for Information Security, BSI TR-02102-1 *"Cryptographic Mechanisms: Recommendations and Key Lengths"* Version: 2025-1, January 2025.

[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 800-38E "*Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*", January 2010.

[8]. National Institute of Standards and Technology, Special Publication 800-56A Revision 3 "*Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*", April 2018.

[9]. National Institute of Standards and Technology, Special Publication SP 800-56C Revision 2 "*Recommendation for Key-Derivation Methods in Key-Establishment Schemes*", August 2020.

[10]. National Institute of Standards and Technology, Special Publication 800-186 "*Recommendation for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*", April 2018

[11]. National Institute of Standards and Technology, Special Publication 800-57 Part 1 Rev. 5 *"Recommendation for Key Management: Part 1 – General"*, May 2020.

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

[15]. [RFC 2631]: "*Diffie-Hellman Key Agreement Method*", Internet Engineering Task Force (IETF), December 2013.

[16]. [RFC 3526]: "*More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*", Internet Engineering Task Force (IETF), May 2003

[17]. [RFC 7919]: "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)", Internet Engineering Task Force (IETF), August 2016.

[18]. [RFC 6090]: "Fundamental Elliptic Curve Cryptography Algorithms", Internet Engineering Task Force (IETF), February 2011.

[19]. [RFC 709i]: "GOST R 34.10-2012: Digital Signature Algorithm", Internet Engineering Task Force (IETF), December 2013.