DỰ THẢO



CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN XXXX:2026/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MẬT MÃ TRONG LĨNH VỰC MẬT MÃ DÂN SỰ CHO HỆ THỐNG VOIP/WEBRTC

NATIONAL TECHNICAL REGULATION ON CRYPTOGRAPHY IN THE FIELD OF CIVIL CRYPTOGRAPHY FOR VOIP/WEBRTC SYSTEMS

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu **4**
1 QUY ĐỊNH CHUNG **5**
1.1 Phạm vi điều chỉnh **5**
1.2 Đối tượng áp dụng **5**
1.3 Tài liệu viện dẫn **5**
1.4 Giải thích từ ngữ **5**
1.5 Chữ viết tắt **6**
2 QUY ĐỊNH KĨ THUẬT **10**
2.1 Yêu cầu về mô hình bảo mật, an toàn thông tin đối với hệ thống VoIP/WebRTC **10**
2.2 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống VoIP/WebRTC **10**
2.2.1 Yêu cầu kỹ thuật chung đảm bảo an toàn quản lý khóa 10
2.2.2 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống VoIP 10
2.2.3 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống WebRTC 11
2.3 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu điều khiển **11**
2.3.1 Đối với hệ thống VoIP 11
2.3.2 Đối với hệ thống WebRTC 11
2.4 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ trao đổi khóa **12**
2.4.1 Đối với hệ thống VoIP 12
2.4.2 Đối với hệ thống WebRTC 13
2.5 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu thoại đối với hệ thống VoIP **13**
2.6 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu thoại/video đối với hệ thống WebRTC **14**
2.7 Yêu cầu an toàn nghiệp vụ mật mã **14**
2.7.1 Đối với hệ thống VoIP 14
2.7.2 Đối với hệ thống WebRTC 14
2.8 Yêu cầu an toàn dịch vụ máy chủ VoIP/WebRTC **14**
2.9 Yêu cầu về kỹ thuật mật mã **15**
2.9.1 Thuật toán mã hóa đối xứng 15
2.9.2 Thuật toán chữ ký số 16
2.9.3 Thuật toán băm 17
2.9.4 Hàm mã xác thực thông báo 18
2.9.5 Hàm dẫn suất khóa 18
2.9.6 Bộ tạo số ngẫu nhiên 18
2.10 Quy định về an toàn trong sử dụng **19**
3 QUY ĐỊNH VỀ QUẢN LÝ **19**
4 TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN **19**

5 TỔ CHỨC THỰC HIỆN.....19

Lời nói đầu

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

1 QUY ĐỊNH CHUNG

1.1 Phạm vi điều chỉnh

Quy chuẩn này quy định các mức giới hạn các đặc tính kỹ thuật mật mã của sản phẩm mật mã dân sự, hệ thống bảo mật sử dụng công nghệ VoIP/WebRTC phục vụ bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.2 Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các tổ chức, cá nhân kinh doanh và sử dụng sản phẩm mật mã dân sự để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.3 Tài liệu viện dẫn

TCVN 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 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 12214-3:2018 (ISO/IEC 14888-3:2016) *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.*

TCVN 12214-2:2018 (ISO/IEC 14888-2:2008 và đính chính kỹ thuật 1:2015) *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.*

TCVN 11816-3:2017 (ISO/IEC 10118-3:2004 with amendment 1:2006) *Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng.*

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.*

NIST Special Publication 800-90A *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*, June 2015.

FIPS PUB 186-5 *"Digital Signature Standard (DSS)"*, Federal Information Processing Standards Publication, Feb 2023.

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

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 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. Hệ thống VoIP/WebRTC có bảo mật

Là một giải pháp truyền thông thoại và video chạy trên nền Internet có sử dụng kỹ thuật mật mã để bảo vệ thông tin.

1.4.6. Kỹ thuật mật mã

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

1.4.7. Mã hóa

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

1.4.8. Giải mã

Là phép toán ngược với phép mã hóa tương ứng

1.4.9. Khóa

Dãy các ký tự điều khiển sự vận hành của các thuật toán mật mã (ví dụ, phép mã hóa, giải mã).

1.4.10. Mật mã đối xứng

Là mật mã dựa trên kỹ thuật mật mã đối xứng, sử dụng cùng một khóa bí mật cho cả thuật toán mã hóa và giải mã.

1.4.11. Mật mã phi đối xứng

Là hệ thống dựa vào các kỹ thuật mật mã phi đối xứng, ở đó phép biến đổi khóa công khai được sử dụng để mã hóa và phép biến đổi khóa bí mật dùng để giải mã và ngược lại.

1.4.12. Hàm băm mật mã

Là hàm thực hiện quá trình biến một dữ liệu đầu vào có độ dài bất kỳ thành một chuỗi đầu ra đặc trưng có độ dài cố định.

1.4.13. Hàm mã xác thực thông báo

Là một đoạn mã được tạo ra nhằm mục đích xác thực tính toàn vẹn và nguồn gốc của thông báo.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
SFU	Selective Forwarding Unit	Đơn vị chuyển tiếp chọn lọc
CBC	Cipher Block Chaining Mode	Chế độ hoạt động móc xích khối mã

MCU	Multipoint Control Unit	Bộ điều khiển đa điểm
P2P	Peer-to-Peer	Mô hình kết nối trực tiếp giữa các bên
SFU	Selective Forwarding Unit	Đơn vị chuyển tiếp chọn lọc
CCM	Counter with CBC-MAC	Bộ đếm với CBC-MAC
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
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
DTLS	Datagram Transport Layer Security	Giao thức bảo mật cho các ứng dụng truyền dữ liệu dạng “datagram”
EC	Elliptic Curve	Đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral	Thuật toán trao đổi khóa tạm thời dựa trên đường cong Elliptic
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
PFS	Perfect Forward Secrecy	
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 Galois/Bộ đếm
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
HTTPS	Hypertext Transfer Protocol Secure	Phiên bản an toàn của giao thức truyền tải siêu văn bản (HTTP), được sử dụng để mã hóa dữ liệu giữa trình duyệt web và máy chủ
ICE	Interactive Communication Establishment	Giao thức được cùng để thiết lập phiên media dựa trên UDP
KW	Key Wrap	Bọc khóa
MQ_DRBG	Multivariate Quadratic Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định bậc hai đa biến
MS_DRBG	Micali-Schnorr Deterministic Random Bit Generator	Bộ tạo bit ngẫu nhiên tất định Micali Schnorr
MIKEY	Multimedia Internet KEYing	Giao thức quản lý khóa được thiết kế riêng cho các ứng dụng đa phương tiện thời gian thực
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
PBKDF2	Password-Based Key Derivation Function 2	Hàm dẫn suất khóa dựa trên mật khẩu
PCAP	Packet Capture	Chụp gói tin
RFC	Request for Comments	Đề nghị duyệt thảo và bình luận
PSK	Pre-shared Key	Khóa chia sẻ trước
RSA	Rivest - Shamir - Adleman	Tên của hệ mã do ba nhà toán học Rivest, Shamir và Adleman sáng tạo ra

SDES	Session Description Protocol Security	Mô tả bảo mật giao thức mô tả phiên
SDP	Session Description Protocol	Giao thức mô tả phiên
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)
SRTP	Secure Real-time Transport Protocol	Giao thức truyền tải thời gian thực an toàn
SFU	Selective Forwarding Unit	Đơn vị chuyển tiếp chọn lọc
TCVN	-	Tiêu chuẩn quốc gia Việt Nam
TURN	Traversal Using NAT Relay	-
WSS	WebSocket Secure	Phiên bản bảo mật của giao thức WebSocket, sử dụng mã hóa TLS/SSL để bảo vệ dữ liệu truyền qua kết nối hai chiều giữa máy khách và máy chủ
XTS	XEX-based tweaked-codebook mode with ciphertext stealing	Chế độ mã khối hẹp
ZRTP	Zimmermann Real-Time Transport Protocol	Giao thức mã hóa để bảo mật các cuộc gọi thoại và video trên internet (VoIP) bằng cách thương lượng các khóa mã hóa cho các phiên truyền dữ liệu qua RTP

2 QUY ĐỊNH KĨ THUẬT

2.1 Yêu cầu về mô hình bảo mật, an toàn thông tin đối với hệ thống VoIP/WebRTC

a) Yêu cầu chung đối với mô hình bảo mật

- Hệ thống VoIP/WebRTC phải được thiết kế theo mô hình bảo mật nhiều lớp (defense-in-depth), đảm bảo các cơ chế bảo vệ được triển khai đồng thời ở các lớp chức năng khác nhau.
- Mô hình bảo mật phải đảm bảo các mục tiêu an toàn thông tin cơ bản gồm tính bí mật, tính toàn vẹn và tính sẵn sàng của dịch vụ.
- Các cơ chế bảo mật được lựa chọn phải phù hợp với đặc thù truyền thông thời gian thực, không gây ảnh hưởng đến chất lượng dịch vụ thoại/video.

b) Yêu cầu về tuân thủ tiêu chuẩn và pháp luật

- Mô hình bảo mật của hệ thống VoIP/WebRTC phải phù hợp với các tiêu chuẩn an toàn thông tin liên quan và quy định pháp luật hiện hành tại Việt Nam.
- Việc tuân thủ phải được xem là một phần không tách rời của yêu cầu an toàn thông tin tổng thể đối với hệ thống.

2.2 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống VoIP/WebRTC

Điều khoản này quy định các yêu cầu tối thiểu và yêu cầu buộc áp dụng nhằm bảo đảm an toàn quản lý khóa mật mã dùng cho bảo vệ kênh thoại và kênh tín hiệu trong hệ thống VoIP và WebRTC, bao gồm cơ chế thiết lập khóa, lưu trữ, sử dụng, luân chuyển, thu hồi, giám sát và kiểm soát vận hành.

2.2.1 Yêu cầu kỹ thuật chung đảm bảo an toàn quản lý khóa

- Khóa mật mã phải được sinh bằng bộ sinh số ngẫu nhiên an toàn về mặt mật mã (Cryptographically Secure Pseudo-Random Number Generator – CSPRNG) (theo quy định tại điều khoản 2.9.6).
- Độ dài khóa mật mã phải phù hợp với thuật toán mật mã được sử dụng và mức độ an toàn yêu cầu (theo quy định tại điều khoản 2.9.1 đến 2.9.4).
- Nghiêm cấm sử dụng các phương pháp sinh khóa thủ công, khóa định sẵn hoặc các hàm sinh số ngẫu nhiên không bảo mật trong quá trình sinh khóa.
- Bản sao lưu khóa mật mã phải được mã hóa bằng cơ chế mật mã an toàn theo quy định tại điều khoản 2.9.1.
- Vị trí lưu trữ bản sao lưu khóa phải tách biệt với hệ thống chính đang vận hành, bảo đảm giảm thiểu rủi ro đồng thời bị xâm phạm hoặc mất mát.
- Quyền truy cập đối với bản sao lưu khóa phải được kiểm soát chặt chẽ, tối thiểu tương đương mức kiểm soát áp dụng đối với khóa đang sử dụng, bao gồm phân quyền, xác thực và ghi nhận nhật ký truy cập.
- Phải sử dụng các bộ khóa bí mật riêng biệt đối với các môi trường phát triển (development), thử nghiệm (testing/staging) và vận hành chính thức (production). Mỗi mục đích sử dụng mật mã phải gắn với một khóa tương ứng và được quản lý độc lập trong suốt vòng đời khóa.

2.2.2 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống VoIP

Đáp ứng yêu cầu tại Điều khoản 2.2.1 và các yêu cầu dưới đây:

- Không được phép lưu trữ khóa phiên SRTP trên các phương tiện lưu trữ lâu dài. Trường hợp khóa SRTP bắt buộc phải được lưu trữ tạm thời trong bộ nhớ để phục vụ xử lý phiên, cần thực hiện xóa an toàn khóa ngay khi cuộc gọi kết thúc hoặc khi phiên truyền thông bị hủy.
- Quyền truy cập vào khóa, cấu hình bảo mật và các chức năng giải mã media phải được phân quyền nghiêm ngặt theo nguyên tắc đặc quyền tối thiểu.
- Hệ thống phải thực hiện phân tách tối thiểu các vai trò sau trong quản trị và vận hành liên quan đến khóa mật mã: Vận hành hệ thống; Quản trị an toàn thông tin; Điều tra và xử lý sự cố; Phát triển và bảo trì hệ thống.
- Mọi hành động quản trị có ảnh hưởng đến khóa mật mã, bao gồm cấp phát, thay đổi, thu hồi khóa hoặc kích hoạt các chế độ gỡ rối (debug) liên quan, phải được ghi nhận đầy đủ và bảo đảm khả năng kiểm toán theo quy định an toàn thông tin của tổ chức.

2.2.3 Yêu cầu đảm bảo an toàn quản lý khóa đối với hệ thống WebRTC

Đáp ứng yêu cầu tại Điều khoản 2.2.2.

2.3 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu điều khiển

2.3.1 Đối với hệ thống VoIP

a) Tín hiệu điều khiển trong hệ thống VoIP phải sử dụng SIPS (SIP over TLS) với TLS 1.2 hoặc TLS 1.3.

Trường hợp sử dụng TLS 1.2 cần sử dụng một trong các bộ mật mã sau:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256;
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384;
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256;
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384;
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256;
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256;
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256;
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.
```

Trường hợp sử dụng TLS 1.3, yêu cầu:

- 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.

b) Chứng thư và thuật toán khóa công khai bảo vệ kênh truyền tín hiệu áp dụng quy định tại Điều khoản 2.9.2.

2.3.2 Đối với hệ thống WebRTC

a) Kênh tín hiệu điều khiển của hệ thống WebRTC phải sử dụng HTTPS hoặc WSS (WebSocket Secure), sử dụng TLS 1.2 hoặc TLS 1.3 theo quy định tại Điểm a Điều khoản 2.3.1.

b) Kênh tín hiệu điều khiển phải đảm bảo tối thiểu các thuộc tính: xác thực máy chủ, bí mật, toàn vẹn và chống hạ mức an toàn trong quá trình kết nối.

c) Chứng thư và thuật toán khóa công khai bảo vệ kênh truyền tín hiệu áp dụng quy định tại Điều khoản 2.9.2.

2.4 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ trao đổi khóa

2.4.1 Đối với hệ thống VoIP

a) Yêu cầu kỹ thuật về cơ chế thiết lập và trao đổi khóa SRTP

- Hệ thống VoIP phải áp dụng một trong các cơ chế trao đổi khóa theo thứ tự mức an toàn giảm dần: DTLS-SRTP, ZRTP, MIKEY, SDES.
- Đối với cơ chế trao đổi khóa DTLS-SRTP:
  + Chỉ sử dụng DTLS 1.2 và DTLS 1.3.
  + Trường hợp sử dụng DTLS 1.2: Sử dụng một trong các bộ mật mã sau:

    `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`

    `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

    `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`

    `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

    `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

    `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  + Trường hợp sử dụng DTLS 1.3:
    - Bắt buộc phải sử dụng trao đổi khóa ECDHE với các đường cong mạnh có mức an toàn từ 128 bit trở lên.
    - Xác thực danh tính trong quá trình DTLS bắt tay, sử dụng ECDSA thay vì RSA.
    - Sử dụng một trong các bộ mật mã sau:

      `TLS_AES_128_GCM_SHA256`

      `TLS_AES_256_GCM_SHA384`

      `TLS_CHACHA20_POLY1305_SHA256`
- Đối với cơ chế trao đổi khóa ZRTP:
  + Bắt buộc dùng DHE hoặc ECDHE.
  + Ưu tiên ECDH, sử dụng các đường cong mạnh như X25519, P-256 hoặc P-384.
  + Bắt buộc áp dụng cơ chế xác thực.
- Đối với cơ chế trao đổi khóa MIKEY:
  + Sử dụng cơ chế sinh ngẫu nhiên trong thiết lập khóa (theo quy định tại Điều khoản 2.9.6).
  + Sử dụng cặp khóa công khai/bí mật để bọc khóa chính. Yêu cầu chứng chỉ số (X.509) và thuật toán RSA (tối thiểu 2048-bit).
- Đối với cơ chế trao đổi khóa SDES:
  + Chỉ cho phép sử dụng trong hệ thống cục bộ hoặc hệ thống phân tách tại vùng mạng an toàn.

+ Bắt buộc mã hóa kênh tín hiệu bằng TLS (SIPS).

+ Thiết lập tường lửa hoặc ACL để chỉ cho phép các thiết bị đầu cuối (IP Phone) giao tiếp với máy chủ PBX, ngăn chặn các thiết bị ngoài danh sách trong mạng nội bộ quét hoặc can thiệp vào luồng thoại.

b) Yêu cầu nghiệp vụ về cơ chế thiết lập và trao đổi khóa SRTP

- Không được tái sử dụng khóa phiên giữa các cuộc gọi khác nhau.

- Hệ thống phải có tính năng tái kết nối kênh mật khi: Phiên trao đổi khoá bị gián đoạn hoặc mất kết nối; Cần khôi phục trạng thái bảo mật sau sự cố an toàn thông tin; Phát hiện bất thường ảnh hưởng đến tính toàn vẹn hoặc xác thực của phiên trao đổi khoá.

- Hệ thống phải có khả năng phát hiện, ghi nhận và từ chối các phiên thỏa thuận khóa SRTP không đáp ứng đầy đủ các yêu cầu an toàn quy định tại điều khoản này.

2.4.2 Đối với hệ thống WebRTC

Yêu cầu bắt buộc về giao thức trao đổi khóa cho media:

- Hệ thống WebRTC phải áp dụng cơ chế trao đổi khóa DTLS-SRTP, phiên bản DTLS 1.2 trở lên.

  + Trường hợp sử dụng DTLS 1.2:

    • Sử dụng một trong các bộ mật mã sau:

    `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`

    `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

    `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`

    `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

    `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

    `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`

  + Trường hợp sử dụng DTLS 1.3:

    • Bắt buộc phải sử dụng trao đổi khóa ECDHE với các đường cong mạnh có mức an toàn từ 128 bit trở lên.

    • Xác thực danh tính trong quá trình DTLS bắt tay, sử dụng ECDSA thay vì RSA.

    • Sử dụng một trong các bộ mật mã sau:

    `TLS_AES_128_GCM_SHA256`

    `TLS_AES_256_GCM_SHA384`

    `TLS_CHACHA20_POLY1305_SHA256`

- Hệ thống phải có tính năng tái kết nối kênh mật khi: phiên DTLS bị gián đoạn hoặc mất kết nối; cần khôi phục trạng thái bảo mật sau sự cố an toàn thông tin; phát hiện bất thường ảnh hưởng đến tính toàn vẹn hoặc xác thực của phiên DTLS.

2.5 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu thoại đối với hệ thống VoIP

- Phải bảo vệ tín hiệu thoại bằng SRTP cho luồng RTP và SRTCP cho luồng RTCP.

- Bắt buộc sử dụng thuật toán mật mã tuân thủ quy định tại Điều khoản 2.9.1.

2.6 Yêu cầu đảm bảo an toàn kỹ thuật mật mã phục vụ bảo mật tín hiệu thoại/video đối với hệ thống WebRTC

- Phải sử dụng SRTP cho toàn bộ luồng thoại/video.
- Bắt buộc sử dụng thuật toán mật mã tuân thủ quy định tại Điểm b Điều khoản 2.9.1.

2.7 Yêu cầu an toàn nghiệp vụ mật mã

2.7.1 Đối với hệ thống VoIP

a) Yêu cầu phân tách các nhóm vai trò

- Phải áp dụng phân tách giữa các nhóm vai trò: Quản trị hạ tầng VoIP (vận hành dịch vụ); Quản trị an toàn thông tin/mật mã (chính sách, phê duyệt thay đổi, kiểm toán); Điều tra sự cố; Phát triển/tích hợp ứng dụng.
- Không cho phép một cá nhân/nhóm nào được đồng thời có toàn quyền: truy cập kho bí mật/khóa, trích xuất bản ghi cuộc gọi, thay đổi cấu hình bảo mật.

b) Yêu cầu nghiệp vụ về vòng đời khóa và thông tin bí mật

- Các bí mật dài hạn (khóa bí mật TLS, thông tin đăng nhập, thông tin máy chủ) phải có: Cơ chế thay đổi định kỳ; Cơ chế thu hồi khẩn cấp; Kiểm soát phân phối và cấp quyền sử dụng.
- Khóa SRTP theo phiên phải sinh mới theo từng cuộc gọi, không lưu dài hạn, tự hủy khi kết thúc cuộc gọi.
- Khi nghi ngờ lộ bí mật, hệ thống phải có thủ tục huỷ bỏ và thay thế rõ ràng và có thể thực thi trong vận hành.

c) Yêu cầu về giám sát, cảnh báo:

- Hệ thống phải giám sát, ghi nhật ký tối thiểu các thông tin sau: Lỗi xác thực thông tin tín hiệu điều khiển; Lỗi thiết lập kênh bảo mật SRTP/DTLS; Thay đổi cấu hình liên quan mật mã.
- Phải thực hiện kiểm tra định kỳ và khắc phục ngay khi phát hiện: Cấu hình phiên bản TLS và bộ mật mã; Chính sách và hồ sơ SRTP; Tình trạng chứng thư (sắp hết hạn, bị thu hồi).

2.7.2 Đối với hệ thống WebRTC

a) Yêu cầu phân tách các nhóm vai trò

- Phải phân tách tối thiểu các vai trò: vận hành WebRTC, quản trị an toàn thông tin/mật mã, điều tra sự cố, phát triển/tích hợp.
- Giới hạn quyền cho từng thực thể, không cho phép một thực thể có toàn quyền truy cập vào kho lưu thông tin bí mật, cấu hình DTLS/SRTP nếu không có phê duyệt và đánh giá.

b) Yêu cầu nghiệp vụ về khung cấu hình mật mã áp dụng:

- Lập danh sách “cho phép” và “cấm” cấu hình chống hạ cấp; không cho phép bật cấu hình yếu cho mục đích tương thích nếu chưa phê duyệt.
- Phải có kế hoạch loại bỏ các cấu hình yêu tương lại đối với các thiết bị cũ.

2.8 Yêu cầu an toàn dịch vụ máy chủ VoIP/WebRTC

- Máy chủ VoIP/WebRTC phải áp dụng nguyên tắc quyền tối thiểu cho mọi tài khoản dịch vụ và tài khoản quản trị.

- Truy cập quản trị phải thực hiện qua kênh quản trị riêng, giới hạn theo IP/segment; không quản trị trực tiếp qua mạng công cộng nếu không có các giải pháp kiểm soát tương đương.
- Không dùng tài khoản dùng chung, mọi truy cập quản trị phải gắn với danh tính cá nhân và có khả năng truy vết.
- Các tài khoản dịch vụ không được có quyền rộng hơn nhu cầu, các thông tin bí mật của tài khoản dịch vụ phải được quản lý như các dữ liệu, tham số an toàn mật mã.
- Máy chủ phải được tăng cường bảo mật tối thiểu: tắt dịch vụ không cần thiết, cấu hình tường lửa, giám sát hoạt động máy chủ (host-based), giới hạn cổng mở, tắt đăng nhập không an toàn.
- Có quy trình quản lý bản vá bảo mật cho hệ điều hành (OS) và các thành phần VoIP/WebRTC (SIP stack, media server, TURN server, reverse proxy).
- Cấu hình biên dịch và thực thi chương trình phải hạn chế bật chế độ gỡ rối (debug), không bật theo dõi mức sâu mặc định trên thiết bị.
- Bản ghi/nội dung của các cuộc hội thoại/dữ liệu phân tích (nếu có) phải được mã hóa khi lưu trữ, phân quyền truy cập theo vai trò, và có thời hạn lưu giữ, xóa an toàn.
- Phải kiểm soát việc xuất dữ liệu ghi âm, nhật ký, báo cáo. Chỉ được xuất khi có sự phê duyệt.
- Nhật ký an ninh mạng phải được lưu trữ tối thiểu 12 tháng kể từ thời điểm phát sinh sự kiện, trừ trường hợp pháp luật chuyên ngành quy định thời hạn dài hơn.
- Nhật ký quản trị khóa mật mã phải được lưu trữ tối thiểu 12 tháng kể từ thời điểm phát sinh sự kiện, bao gồm các hoạt động tạo lập, nhập, xuất, phân phối, kích hoạt, sử dụng, thay đổi trạng thái, sao lưu, khôi phục, thu hồi và hủy khóa, theo phạm vi chức năng của hệ thống, thiết bị.

2.9 Yêu cầu về kỹ thuật mật mã[1]

2.9.1 Thuật toán mã hóa đối xứng

- Đối với hệ thống VoIP/WebRTC sử dụng một trong các thuật toán sau:

STT	Thuật toán	Các chế độ cho phép sử dụng	Kích thước khóa theo bit	Sử dụng đến năm	Tham chiếu
1	MKV-128	GCM, CTR, CCM, XTS	128 bit	2030	TCVN 14263:2024
2			192 bit	2030	
3			256 bit	2035	
4	MKV-256	GCM, CTR, CCM, XTS	256 bit	2035	
5			384 bit	2040	

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

6			512 bit	2045	
7	AES	CFB, OFB, GCM, CTR, F8, CCM, XTS	128 bit	2030	[TCVN 11367-3], [TCVN 12213], [SP 800-38E], [IEEE 1619], [SP 800-38D]
8			192 bit	2030	
9			256 bit	2035	
10	ChaCha20-Poly1305	-	256 bit	2035	[RFC 8439]

- Đối với mã hóa giải mã dữ liệu thoại sử dụng thuật toán trong danh sách sau:

STT	Thuật toán	Các chế độ cho phép sử dụng	Kích thước khóa theo bit	Sử dụng đến năm	Tham chiếu
1	MKV-128	GCM, CTR, CCM	128 bit	2030	TCVN 14263:2024
2			192 bit	2030	
3			256 bit	2035	
4	MKV-256	GCM, CTR, CCM	256 bit	2035	
5			384 bit	2040	
6			512 bit	2045	
7	AES	OFB, GCM, CTR, F8	128 bit	2030	[TCVN 11367-3], [TCVN 12213], [SP 800-38E], [IEEE 1619], [SP 800-38D]
8			192 bit	2030	
9			256 bit	2035	
10	ChaCha20-Poly1305	-	256 bit	2035	[RFC 8439]

2.9.2 Thuật toán chữ ký số

- Sử dụng thuật toán trong danh sách sau:

STT	Thuật toán	Tham số	Sử dụng đến năm	Tài liệu viện dẫn
1		3072 bit $\leq nlen <$ 7680 bit	2030	[FIPS 186-5],

	RSASSA-PSS	$nlen \geq 7068$ bit	2035	[RFC 8017]
2	ECDSA	$256\ bit \leq \|p\|$ < 384 bit	2030	[FIPS 186-5] [NIST SP 800-186]
		$384\ bit \leq \|p\|$ < 512 bit	2030	
		$\|p\| \geq$ 512 bit	2035	
3	EdDSA	Ed25519	2030	[RFC 8032], [FIPS 186-5]
		Ed448	2035	
4	ML-DSA	ML-DSA-44;	2030	[FIPS 204]
		ML-DSA-65;	2035	
		ML-DSA-87	2040	
5	SLH-DSA	SLH-DSA-SHA2-128[s/f]; SLH-DSA-SHAKE-128[s/f]	2035	[FIPS 205] [NIST IR 8547]
		SLH-DSA-SHA2-192[s/f]; SLH-DSA-SHAKE-192[s/f]	2035	
		SLH-DSA-SHA2-256[s/f]; SLH-DSA-SHAKE-256[s/f]	2040	

2.9.3 Thuật toán băm

- Sử dụng thuật toán trong danh sách sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	SHA-256	2030	[TCVN 11816-3], [FIPS PUB 180-4] [FIPS PUB 202]
2	SHA-384	2030	
3	SHA-512	2035	
4	SHA-512/256	2030	
5	SHA3-256	2030	[FIPS 202]
6	SHA3-384	2030	
7	SHA3-512	2035	

2.9.4 Hàm mã xác thực thông báo

- Sử dụng hàm mã xác thực thông báo trong danh sách sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	HMAC_SHA_256	2030	[FIPS 198-1]
2	HMAC_SHA_384	2030	
3	HMAC_SHA_512	2035	
4	HMAC_SHA3_256	2030	[FIPS 198-1], [FIPS PUB 202] [SP 800-107 Rev.1]
5	HMAC_SHA3_384	2030	
6	HMAC_SHA3_512	2035	
7	Poly1305	2035	[RFC 8439]

2.9.5 Hàm dẫn suất khóa

- Sử dụng hàm dẫn suất khóa trong danh sách sau:

STT	Thuật toán	Sử dụng đến năm	Tham chiếu
1	PBKDF2	2035	[SP 800-132], [RFC 8018] [RFC 7914]
2	BCrypt	2035	
3	SCrypt	2035	
4	Argon2id	2035	
5	HKDF	2035	[RFC 5869] [RFC 5764]

2.9.6 Bộ tạo số ngẫu nhiên

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

STT	Thuật toán	Cơ chế nền	Nguồn entropy	Sử dụng đến năm
1	CTR-DRBG	AES-CTR-128	≥ 256 bit	Năm sử dụng được tính bằng năm sử dụng
2	Hash-DRBG	SHA-512	≥ 256 bit	

3	HMAC-DRBG	HMAC-SHA-384 HMAC-SHA3-256	≥ 256 bit	của các nguyên thủy mật mã tương ứng
4	TRNG[2]	SHA-256/ PHOTON	≥ 0,5 bits/bit	2035

2.10 Quy định về an toàn trong sử dụng

Nếu hệ thống có kết nối giữa 2 hay nhiều địa điểm qua VPN sử dụng công nghệ IPsec, TLS thì áp dụng các yêu cầu tại Thông tư 23/2022/TT-BQP ngày 04/4/2022 ban hành quy chuẩn kỹ thuật quốc gia về đặc tính kỹ thuật mật mã sử dụng trong các sản phẩm mật mã dân sự thuộc nhóm sản phẩm bảo mật luồng IP sử dụng công nghệ IPSec và TLS và Thông tư số 07/2026/TT-BQP ngày 20/01/2026 ban hành, sửa đổi quy chuẩn kỹ thuật quốc gia và danh mục tiêu chuẩn kỹ thuật mật mã áp dụng bắt buộc trong lĩnh vực mật mã dân sự.

3 QUY ĐỊNH VỀ QUẢN LÝ

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

3.2. Công bố hợp quy và phương thức đánh giá sự phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật theo Thông tư số 14/2026/TT-BKHCN ngày 09/4/2026 với tiêu chuẩn, quy chuẩn kỹ thuật, trong quy chuẩn này được thực hiện theo phương thức 5 hoặc phương thức 7; Quản lý công bố hợp quy dựa trên kết quả chứng nhận của tổ chức chứng nhận được chỉ định theo quy định của pháp luật.

3.3 Dấu hợp quy được sử dụng trực tiếp trên sản phẩm hoặc trên bao gói hoặc trên nhãn gắn trên sản phẩm hoặc trong chứng chỉ chất lượng, tài liệu kỹ thuật của sản phẩm.

3.4 Ban Cơ yếu Chính phủ xem xét thừa nhận kết quả đánh giá sự phủ hợp do tổ chức đánh giá sự phù hợp nước ngoài thực hiện đối với các sản phẩm mật mã dân sự thuộc trách nhiệm quản lý theo quy định.

4 TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

4.1 Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã - Ban Cơ yếu Chính phủ là cơ quan tiếp nhận công bố hợp quy, kiểm tra nhà nước về chất lượng sản phẩm mật mã dân sự.

4.2 Các tổ chức, cá nhân có hoạt động sản xuất, kinh doanh sản phẩm mật mã dân sự thuộc phạm vi điều chỉnh của quy chuẩn này có trách nhiệm thực hiện các quy định về chứng nhận, công bố hợp quy và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định hiện hành.

5 TỔ CHỨC THỰC HIỆN

5.1 Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng rà soát, sửa đổi, bổ sung hoặc ban hành thay thế quy chuẩn này để đảm bảo phù hợp với thực tiễn và đáp ứng yêu cầu quản lý.

[2] Bộ sinh số ngẫu nhiên thực (TRNG) phải sử dụng nguồn entropy vật lý, có giá trị min-entropy của dữ liệu đầu ra nguồn nhiễu thô không nhỏ hơn 0,5 bit/bit, được đánh giá theo phương pháp quy định tại NIST SP 800-90B hoặc tiêu chuẩn tương đương.

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./.