BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /2021/TT-BQP	*Hà Nội, ngày tháng năm 2021*

DỰ THẢO

THÔNG TƯ

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

Căn cứ Luật Tiêu chuẩn và Quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật và Nghị định số 78/2018/NĐ-CP ngày 16 tháng 5 năm 2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 127/2007/NĐ-CP;

Căn cứ Nghị định số 164/2017/NĐ-CP ngày 30 tháng 12 năm 2017 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 ngày 27 tháng 01 năm 2014 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

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

Bộ trưởng Bộ Quốc phòng ban hành Thông tư 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.

Điều 1. Ban hành kèm theo Thông tư này 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 (QCVN .../2021/BQP).

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày tháng năm 2021.

Điều 3. Trưởng ban Ban Cơ yếu Chính phủ, Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này./.

Nơi nhận:
- Chính phủ (để báo cáo);
- Thủ tướng Chính phủ (để báo cáo);
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Thủ trưởng BQP, CN TCCT;
- Ban Cơ yếu Chính phủ;
- Cục Tiêu chuẩn - Đo lường - Chất lượng/BQP;
- Cục Kiểm tra văn bản QPPL Bộ Tư pháp;
- Công báo, Cổng TTĐTCP;
- Cổng TTĐTBQP;
- Vụ Pháp chế/BQP;
- Lưu: VT, BCY. BN100.

BỘ TRƯỞNG

Thượng tướng Phan Văn Giang

DỰ THẢO

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN XXXX:2021/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ YÊU CẦU KỸ THUẬT MẬT MÃ SỬ DỤNG TRONG CÁC SẢN PHẨM MẬT MÃ DÂN SỰ THUỘC NHÓM SẢN PHẨM BẢO MẬT LUỒNG IP

National technical regulation on cryptographic technical requirements used in civil cryptography products under IP security products group

HÀ NỘI – 2021

MỤC LỤC

Lời nói đầu

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

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn kỹ thuật quốc gia này quy định mức giới hạn các đặc tính kỹ thuật mật mã của các sản phẩm bảo mật luồng IP sử dụng công nghệ SSL/TLS VPN, IPSec VPN phục vụ bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.2. Đối tượng áp dụng

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

1.3. Giải thích từ ngữ

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

1.3.1. "Thông tin không thuộc phạm vi bí mật nhà nước" là thông tin không thuộc nội dung tin "tuyệt mật", "tối mật" và "mật" được quy định tại Luật bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018.

1.3.2. "Mật mã" là quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin nhằm bảo đảm bí mật, xác thực, toàn vẹn của nội dung thông tin.

1.3.3. "Mật mã dân sự" là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

1.3.4. "Sản phẩm mật mã dân sự" là các tài liệu, trang thiết bị kỹ thuật và nghiệp vụ mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

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

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

1.3.7. Mã hóa

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

1.3.8. Giải mã

Phép toán ngược với phép mã hóa tương ứng

1.3.9. Mã khối

Hệ thống mã khối đối xứng, với tính chất là thuật toán mã hóa thao tác trên khối bản rõ, tức xâu bít có độ dài xác định, cho ra khối bản mã.

1.3.10. Khóa

Dãy các ký tự sử dụng trong một phép biến đổi mật mã (ví dụ phép mã hóa, giải mã).

1.3.11. Chữ ký số

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

1.3.12. Chữ viết tắt

1	Tiêu chuẩn mã hóa tiên tiến *(Advanced Encryption Standard)*	*AES*
2	Diffie-Hellman	*DH*
3	Thuật toán chữ ký số	*DSA*
4	Đường cong Elliptic	*EC*
5	Thuật toán chữ ký số dựa trên đường cong Elliptic	*ECDSA*
6	Tiêu chuẩn mật mã khóa công khai *(Puplic Key Cryptography Standard)* do Phòng thí nghiệm RSA (Mỹ) ban hành.	*PKCS*
7	Lược đồ ký xác suất *(Probabilistic Signature Scheme)*	*PSS*
8	Tên của hệ mã do ba nhà toán học Rivest, Shamir và Adleman sáng tạo ra	*RSA*
9	Lược đồ ký RSA kèm phụ lục *(RSA Signature Scheme with Appendix)*	*RSASSA*
10	Thuật toán băm an toàn *(Secure Hash Algorithm).*	*SHA*
11	Tầng socket bảo mật *(Secure Sockets Layer)*	*SSL*
12	Bảo mật tầng giao vận *(Transport Layer Security)*	*TLS*
13	Mạng riêng ảo *(Virtual Private Network)*	*VPN*

2. QUY ĐỊNH KỸ THUẬT

2.1. Các chỉ tiêu kỹ thuật sản phẩm sử dụng công nghệ IPsec VPN

2.1.1. Xác thực và trao đổi khóa (IKE)

Phiên bản áp dụng: IKE v1, IKE v2

Xác thực và trao đổi khóa	Sử dụng đến năm
IKE v1	2025
IKEv2	2030

Các yêu cầu kỹ thuật:

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

STT	Thuật toán mã khối	Chế độ hoạt động của mã khối	Độ dài khóa	Sử dụng đến năm
1	AES	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥128 bit	2030
2	TDES	CBC, CFB, OFB hoặc CTR	192 bit	2030
3	Camellia	CBC, CFB, OFB, GCM, CCM hoặc CTR	≥128 bit	2030
4	CAST	CBC, CFB, OFB hoặc CTR	≥128 bit	2030

- Hàm dẫn xuất khóa: Sử dụng một trong các thuật toán sau

STT	Hàm dẫn xuất khóa	Sử dụng đến năm
1	AES128_XCBC	2030
2	AES128_CMAC	2030
3	HMAC_SHA1	2023
4	HMAC_SHA2_256	2030
5	HMAC_SHA2_384	2030
6	HMAC_SHA2_512	2030
7	HMAC_SHA3_256	2030
8	HMAC_SHA3_384	2030
9	HMAC_SHA3_512	2030

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

STT	Thuật toán xác thực	Sử dụng đến năm
1	HMAC_SHA1_96	2023

2	AES_XCBC_96	2030
3	AES_GMAC_128	2030
4	HMAC_SHA2_256_128	2030
5	HMAC_SHA2_256	2030
6	HMAC_SHA2_384_192	2030
7	HMAC_SHA2_384	2030
8	HMAC_SHA2_512_256	2030
9	HMAC_SHA2_512	2030
10	HMAC_SHA3_256_128	2030
11	HMAC_SHA3_256	2030
12	HMAC_SHA3_384_192	2030
13	HMAC_SHA3_384	2030
14	HMAC_SHA3_512_256	2030
15	HMAC_SHA3_512	2030

- Tiêu chuẩn độ dài số modulo p trong các nhóm Diffie-Hellman:

STT	Tiêu chuẩn	Sử dụng đến năm
I	**Nhóm DH trên trường hữu hạn**	
1	2048-bit MODP	2025
2	3072-bit MODP	2030
3	4096-bit MODP	2030
4	6144-bit MODP	2030
5	8192-bit MODP	2030
II	**Nhóm DH trên đường cong Elliptic**	
1	256-bit random ECP	2030
2	384-bit random ECP	2030
3	521-bit random ECP	2030
4	2048-bit MODP with 256-bit Prime Order Subgroup	2025
5	brainpoolP256r1	2030
6	brainpoolP384r1	2030
7	brainpoolP512r1	2030

- Phương thức xác thực: Sử dụng một trong các thuật toán ký số sau

STT	Phương thức xác thực	Độ dài theo bit	Hàm băm	Sử dụng đến năm
1	ECDSA-256 with curve secp256r1	256	SHA-256	

2	ECDSA-384 with curve secp384r1	384	SHA-384	2030
3	ECDSA-512 with curve secp521r1	512	SHA-512	
4	ECDSA-256 with brainpoolP256r1	256	SHA-256	2030
5	ECDSA-384 with brainpoolP384r1	384	SHA-384	
6	ECDSA-512 with brainpoolP512r1	512	SHA-512	
7	RSASSA-PSS	2048	SHA-256	2025
8	RSASSA-PSS	4096	SHA-384	2030
9	ECGDSA-256 with brainpoolP256r1	256	SHA-256	2030
10	ECGDSA-384 with brainpoolP384r1	384	SHA-384	
11	ECGDSA-512 with brainpoolP512r1	512	SHA-512	

2.1.2. Đóng gói dữ liệu bảo mật

Áp dụng:

- Chế độ ESP: Tunnel Mode và Transport Mode.
- Phiên bản ESP: phiên bản 2, 3
- Mã khối: Sử dụng một trong các thuật toán sau

Tên thuật toán	Độ dài khóa	Chế độ sử dụng	Sử dụng đến năm
AES	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	2030
TDES	192 bit	CBC, CFB, OFB hoặc CTR	
CAST	≥128 bit	CBC, CFB, OFB hoặc CTR	
Camellia	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	
SEED	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	

- Đảm bảo tính xác thực và toàn vẹn của các gói tin ESP

STT	Thuật toán	Sử dụng đến năm
1	HMAC_SHA1_96	2023
2	AES_XCBC_96	2030
3	AES_CMAC_96	2030
4	HMAC_SHA2_256_128	2030
5	HMAC_SHA2_256	2030
6	HMAC_SHA2_384_192	2030
7	HMAC_SHA2_384	2030
8	HMAC_SHA2_512_256	2030

9	HMAC_SHA2_512	2030
10	HMAC_SHA3_256_128	2030
11	HMAC_SHA3_256	2030
12	HMAC_SHA3_384_192	2030
13	HMAC_SHA3_384	2030
14	HMAC_SHA3_512_256	2030
15	HMAC_SHA3_512	2030

- Đảm bảo tính xác thực và toàn vẹn của các gói tin AH

STT	Thuật toán	Sử dụng đến năm
1	HMAC_SHA1_96	2023
2	AES_XCBC_96	2030
3	AES_CMAC_96	2030
4	HMAC_SHA2_256_128	2030
5	HMAC_SHA2_256	2030
6	HMAC_SHA2_384_192	2030
7	HMAC_SHA2_384	2030
8	HMAC_SHA2_512_256	2030
9	HMAC_SHA2_512	2030
10	HMAC_SHA3_256_128	2030
11	HMAC_SHA3_256	2030
12	HMAC_SHA3_384_192	2030
13	HMAC_SHA3_384	2030
14	HMAC_SHA3_512_256	2030
15	HMAC_SHA3_512	2030

2.2. Các chỉ tiêu kỹ thuật sản phẩm sử dụng công nghệ SSL/TLS VPN

2.2.1. Phiên bản của SSL/TLS

Áp dụng: TLS 1.2 hoặc TLS 1.3

2.2.2. Yêu cầu khi sử dụng TLS 1.2

- Trao đổi khóa sử dụng một trong các thuật toán sau:

STT	Thuật toán	Độ dài theo bit (modulo p)	Sử dụng đến năm
1	RSA	2048 bit	2025
2		≥3072 bit	2030
3	Diffie–Hellman	2048 bit	2025
4		≥3072 bit	2030
5	ECDH	≥256 bit	2030

6	PSK		2030

- Đảm bảo tính xác thực sử dụng một trong các thuật toán sau:

STT	Thuật toán	Độ dài theo bit (modulo p)	Sử dụng đến năm
1	RSA	2048 bit	2025
2		≥3072 bit	2030
3	DSA	2048 bit	2025
4		≥3072 bit	2030
5	ECDSA	≥256 bit	2030

- Hàm băm mật mã sử dụng một trong các hàm sau:

STT	Thuật toán	Sử dụng đến năm
1	SHA-1	2023
2	SHA-224, SHA3-224	2025
3	SHA-256, SHA-512/256, SHA3-256	2030
4	SHA-384, SHA3-384	2030
5	SHA-512, SHA3-512	2030

- Thuật toán mã khối sử dụng một trong các thuật toán sau:

Tên thuật toán	Độ dài khóa	Chế độ sử dụng	Sử dụng đến năm
AES	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	2030
TDES	192 bit	CBC, CFB, OFB hoặc CTR	
CAST	≥128 bit	CBC, CFB, OFB hoặc CTR	
Camellia	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	
SEED	≥128 bit	CBC, CFB, OFB, GCM, CCM hoặc CTR	

2.2.3. Yêu cầu khi sử dụng TLS 1.3

- Sử dụng một trong các chế độ PSK sau:

STT	Bộ tham số	Sử dụng đến năm
1	psk_ke	2030
2	psk_dhe_ke	2030

- Sử dụng một trong các nhóm Diffie-Hellman (DH) sau:

STT	Bộ tham số	Sử dụng đến năm
1	secp256r1	2030
2	secp384r1	2030
3	brainpoolP256r1tls13	2030
4	brainpoolP384r1tls13	2030
5	brainpoolP512r1tls13	2030
6	ffdhe2048	2025
7	ffdhe3072	2030
8	ffdhe4096	2030

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

STT	Bộ tham số	Sử dụng đến năm
I	**Thuật toán chữ ký cho TLS 1.3 (máy khách/ máy chủ)**	
1	rsa_pss_rsae_sha256	2030
2	rsa_pss_rsae_sha384	2030
3	rsa_pss_rsae_sha512	2030
4	rsa_pss_pss_sha256	2030
5	rsa_pss_pss_sha384	2030
6	rsa_pss_pss_sha512	2030
7	ecdsa_secp256r1_sha256	2030
8	ecdsa_secp384r1_sha384	2030
9	ecdsa_brainpoolP256r1tls13_sha256	2030
10	ecdsa_brainpoolP384r1tls13_sha384	2030
11	ecdsa_brainpoolP512r1tls13_sha512	2030
II	**Thuật toán chữ ký cho TLS 1.3 (chữ ký trong chứng thư)**	
1	rsa_pkcs1_sha256	2030
2	rsa_pkcs1_sha384	2030
3	rsa_pkcs1_sha512	2030
4	rsa_pss_rsae_sha256	2030
5	rsa_pss_rsae_sha384	2030
6	rsa_pss_rsae_sha512	2030
7	rsa_pss_pss_sha256	2030
8	rsa_pss_pss_sha384	2030
9	rsa_pss_pss_sha512	2030
10	ecdsa_secp256r1_sha256	2030
11	ecdsa_secp384r1_sha384	2030
12	ecdsa_brainpoolP256r1tls13_sha256	2030

13	ecdsa_brainpoolP384r1tls13_sha384	2030
14	ecdsa_brainpoolP512r1tls13_sha512	2030

- Hàm băm mật mã sử dụng một trong các hàm sau:

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

- Thuật toán mã khối sử dụng một trong các thuật toán sau:

Tên thuật toán	Độ dài khóa	Chế độ sử dụng	Sử dụng đến năm
AES	≥128 bit	GCM, CCM	2030

- Độ dài khóa tối thiểu cho giao thức bắt tay TLS

STT	Thuật toán	Độ dài khóa tối thiểu theo bít	Sử dụng đến năm
I	**Khóa chữ ký cho chứng thư và thỏa thuận khóa**		
1	ECDSA	224	2025
2		256	2030
3	DSS	2048	2025
4		3072	2030
5	RSA	2048	2025
6		3072	2030
II	**Các khóa Diffie-Hellman tĩnh và tạm thời**		
1	ECDH	224	2025
2		256	2030
3	DH	2048	2025
4		3072	2030

3. QUY ĐỊNH VỀ QUẢN LÝ

3.1. Các mức giới hạn của đặc tính kỹ thuật mật mã của sản phẩm bảo mật luồng IP và yêu cầu quản lý của các thuật toán mật mã nêu tại Quy chuẩn này là các chỉ tiêu chất lượng phục vụ và được quản lý theo Quy định về quản lý chất lượng sản phẩm mật mã dân sự, được quy định tại Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015.

3.2. Công bố hợp quy, chứng nhận hợp quy theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 và Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 sửa

đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012, quản lý công bố hợp quy dựa trên kết quả chứng nhận của tổ chức chứng nhận được chỉ định theo quy định của pháp luật.

3.3. Hoạt động kiểm tra, đánh giá chất lượng sản phẩm mật mã được cơ quan quản lý nhà nước có thẩm quyền tiến hành định kỳ hàng năm hoặc đột xuất.

3.4. Các quy định trong trong Quy chuẩn được rà soát lại cứ 5 năm một lần.

4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Cơ quan, tổ chức cá nhân hoạt động kinh doanh và sử dụng sản phẩm bảo mật luồng IP phải đảm bảo chất lượng phù hợp với Quy chuẩn này, thực hiện công bố hợp quy theo Quy định về chứng nhận hợp chuẩn, chứng nhận hợp quy và công bố hợp chuẩn, công bố hợp quy ban hành kèm theo Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 và Thông tư số 02/2017/TT-BKHCN ngày 31/3/2017 sửa đổi, bổ sung một số điều của Thông tư số 28/2012/TT-BKHCN ngày 12/12/2012 và theo quy định tại Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 và chịu sự kiểm tra thường xuyên, đột xuất của cơ quan quản lý nhà nước theo các quy định hiện hành.

5. TỔ CHỨC THỰC HIỆN

Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã - Ban Cơ yếu Chính phủ có trách nhiệm hướng dẫn, tổ chức triển khai quản lý kỹ thuật mật mã theo Quy chuẩn này.

Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng rà soát, sửa đổi, bổ sung Quy chuẩn này để đảm bảo phù hợp với thực tiễn và đáp ứng yêu cầu quản lý./.

Tài liệu tham khảo

1. *NIST Special Publication 800-77, Guide to IPsec VPNs, 2020.*
2. *NIST Special Publication 800-113, Guide to SSL VPNs, 2008.*
3. *Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths*
4. *Technical Guideline TR-02102-3 Cryptographic Mechanisms: Recommendations and KeyLengths*
5. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST SP 800-90A Rev. 1, National Institute of Standards and Technology,June 2015. (*Khuyến cáo cho bộ sinh số ngẫu nhiên sử dụng bộ sinh bit ngẫu nhiên tất định*, NIST SP 800-90A Rev. 1, Viện tiêu chuẩn và công nghệ quốc gia (Mỹ), tháng 6 năm 2015).
6. RSA Laboratories. *PKCS#1 v2.1: RSA Cryptography Standard.* June 2002. (Phòng thí nghiệm RSA. *PKCS#1 v2.1: Tiêu chuẩn mật mã RSA*. Tháng 6 năm 2002).
7. TCVN 7635:2007 Kỹ thuật mật mã – Chữ ký số.
8. TCVN 7876:2007 Công nghệ thông tin – Kỹ thuật mật mã – Thuật toán mã dữ liệu AES.
9. 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.
10. TCVN 11495-1:2016 (ISO/IEC 9797-1:2011) Công nghệ thông tin – Các kỹ thuật an toàn- Mã xác nhận thông điệp.