BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập – Tự do – Hạnh phúc
Số: 22 /2020/TT-BTTTT	
	Hà Nội, ngày 07 tháng 9 năm 2020

THÔNG TƯ
Quy định về yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số

Căn cứ Luật giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Giám đốc Trung tâm Chứng thực điện tử quốc gia,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định về yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Thông tư này quy định yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

2. Yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số cho văn bản điện tử trong cơ quan nhà nước không thuộc phạm vi điều chỉnh của Thông tư này.

Điều 2. Đối tượng áp dụng

1. Thông tư này áp dụng đối với cơ quan, tổ chức, cá nhân lựa chọn sử dụng phần mềm ký số, phần mềm kiểm tra chữ ký số trong giao dịch điện tử; các tổ chức cung cấp dịch vụ chứng thực chữ ký số; các tổ chức, cá nhân phát triển ứng dụng, sử dụng chữ ký số.

2. Thông tư này không áp dụng đối với tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

Điều 3. Giải thích từ ngữ

1. "Chứng thư số tổ chức" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức từ đó xác nhận cơ quan, tổ chức là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

2. "Chứng thư số cá nhân" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cá nhân, từ đó xác nhận cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

3. "Khóa bí mật tổ chức" là khóa bí mật tương ứng với chứng thư số tổ chức.

4. "Khóa bí mật cá nhân" là khóa bí mật tương ứng với chứng thư số cá nhân.

5. "Phần mềm ký số" là chương trình phần mềm độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng ký số vào thông điệp dữ liệu.

6. "Phần mềm kiểm tra chữ ký số" là chương trình phần mềm độc lập hoặc một thành phần (module) phần mềm hoặc giải pháp có chức năng kiểm tra tính hợp lệ của chữ ký số trên thông điệp dữ liệu ký số.

7. "Đường dẫn tin tưởng của chứng thư số" là thông tin đường dẫn địa chỉ internet trên chứng thư số cho biết tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp phát ra chứng thư số đó.

Chương II
YÊU CẦU KỸ THUẬT ĐỐI VỚI PHẦN MỀM KÝ SỐ, PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ

Mục 1- Phần mềm ký số

Điều 4. Yêu cầu chung

Tuân thủ các tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục Danh mục tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu kèm theo Thông tư này.

Điều 5. Yêu cầu chức năng

1. Chức năng ký số:

a) Trường hợp người ký số trên thông điệp dữ liệu là cá nhân, cho phép người ký số sử dụng khóa bí mật cá nhân để thực hiện việc ký số vào thông điệp dữ liệu;

b) Trường hợp người ký số trên thông điệp dữ liệu là tổ chức, cho phép người ký số sử dụng khóa bí mật tổ chức để thực hiện việc ký số vào thông điệp dữ liệu.

2. Chức năng kiểm tra hiệu lực của chứng thư số:

a) Cho phép việc kiểm tra chứng thư số của người ký số trên thông điệp dữ liệu phải kiểm tra theo đường dẫn tin tưởng trên chứng thư số và phải thực hiện đến tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

b) Nội dung kiểm tra hiệu lực của chứng thư số tại thời điểm ký số:

- Thời gian có hiệu lực của chứng thư số;

- Trạng thái chứng thư số qua danh sách chứng thư số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến trong trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số có cung cấp dịch vụ OCSP;

- Thuật toán mật mã trên chứng thư số;

- Mục đích, phạm vi sử dụng của chứng thư số.

c) Hiệu lực của chứng thư số khi đáp ứng tất cả các tiêu chí sau:

- Thời gian trên chứng thư số còn hiệu lực tại thời điểm ký số;

- Các thuật toán mật mã trên chứng thư số tuân thủ theo quy định về quy chuẩn, tiêu chuẩn kỹ thuật bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực;

- Trạng thái của chứng thư số còn hoạt động tại thời điểm ký số;

- Chứng thư số được sử dụng đúng mục đích, phạm vi sử dụng.

3. Chức năng lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số:

a) Chứng thư số tương ứng với khóa bí mật mà người ký số sử dụng để ký thông điệp dữ liệu tại thời điểm ký số;

b) Danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số để ký số tương ứng với chữ ký số trên thông điệp dữ liệu đi;

c) Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu đi;

d) Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

4. Chức năng thay đổi (thêm, bớt) chứng thư số của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

5. Chức năng thông báo (bằng chữ/bằng ký hiệu) cho người ký số biết việc ký số vào thông điệp dữ liệu thành công hay không thành công.

Mục 2-Phần mềm kiểm tra chữ ký số

Điều 6. Yêu cầu chung

Tuân thủ các tiêu chuẩn kỹ thuật về chữ ký số trên thông điệp dữ liệu tại Phụ lục Danh mục tiêu chuẩn về chữ ký số trên thông điệp dữ liệu kèm theo Thông tư này.

Điều 7. Yêu cầu chức năng

1. Chức năng kiểm tra tính hợp lệ của chữ ký số trên thông điệp dữ liệu:

a) Cho phép xác minh chữ ký số trên thông điệp dữ liệu theo nguyên tắc chữ ký số được tạo ra đúng với khóa bí mật tương ứng với khóa công khai trên chứng thư số;

b) Cho phép việc kiểm tra chứng thư số của người ký số trên thông điệp dữ liệu phải kiểm tra theo đường dẫn tin tưởng trên chứng thư số và phải thực hiện đến tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.

c) Cho phép kiểm tra, xác thực thông tin của người ký số trên thông điệp dữ liệu thực hiện tất cả các nội dung dưới đây:

- Thời gian có hiệu lực của chứng thư số;

- Trạng thái chứng thư số qua danh sách chứng thư số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến trong trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số có cung cấp dịch vụ OCSP;

- Thuật toán mật mã trên chứng thư số;

- Mục đích, phạm vi sử dụng của chứng thư số.

d) Hiệu lực của chứng thư số khi đáp ứng tất cả các tiêu chí sau:

- Thời gian trên chứng thư số còn hiệu lực tại thời điểm ký số;

- Các thuật toán mật mã trên chứng thư số tuân thủ theo quy định về quy chuẩn, tiêu chuẩn kỹ thuật bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số đang có hiệu lực;

- Trạng thái của chứng thư số còn hoạt động tại thời điểm ký số;

- Chứng thư số được sử dụng đúng mục đích, phạm vi sử dụng.

đ) Cho phép kiểm tra tính toàn vẹn của thông điệp dữ liệu ký số:

- Giải mã chữ ký số trên thông điệp dữ liệu để có thông tin về mã băm;

- Sử dụng thuật toán hàm băm an toàn đã tạo ra mã băm trên chữ ký số để thực hiện tạo mã băm cho thông điệp dữ liệu;

- So sánh sự trùng khớp của hai mã băm để kiểm tra tính toàn vẹn của thông điệp dữ liệu ký số.

e) Chữ ký số trên thông điệp dữ liệu là hợp lệ khi:

- Việc kiểm tra, xác thực được đúng thông tin người ký số;

- Chứng thư số của người ký số tại thời điểm ký còn hiệu lực;

- Xác minh chữ ký số trên thông điệp dữ liệu đúng với khóa bí mật tương ứng với khóa công khai trên chứng thư số và thông điệp dữ liệu đảm bảo tính toàn vẹn.

2. Chức năng lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số:

a) Các chứng thư số tương ứng với các chữ ký số trên thông điệp dữ liệu ký số được gửi đến;

b) Các danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp chứng thực chữ ký số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến;

c) Quy chế chứng thực của các tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp phát chứng thư số tương ứng với các chữ ký số trên thông điệp dữ liệu được gửi đến;

d) Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

3. Chức năng thay đổi (thêm, bớt) chứng thư số của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

4. Chức năng thông báo (bằng chữ/bằng ký hiệu) việc kiểm tra tính hợp lệ của chữ ký số là hợp lệ hay không hợp lệ.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 8. Tổ chức thực hiện

1. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn thực hiện các nội dung của Thông tư này.

2. Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng của cơ quan, tổ chức công bố các

đặc tả kỹ thuật (tài liệu và bộ công cụ), chứng thư số liên quan đến tổ chức cung cấp dịch vụ chứng thực chữ ký số và các tiêu chuẩn chữ ký số trên trang tin điện tử của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

3. Tổ chức, cá nhân phát triển ứng dụng, sử dụng chữ ký số có trách nhiệm tuân thủ các quy định về yêu cầu kỹ thuật, hướng dẫn sử dụng đối với phần mềm ký số, phần mềm kiểm tra chữ ký số.

Điều 9. Điều khoản chuyển tiếp

Các cơ quan, tổ chức, cá nhân đang sử dụng phần mềm ký số, phần mềm kiểm tra chữ ký số trước thời điểm Thông tư này có hiệu lực tiếp tục sử dụng cho đến khi thay đổi, nâng cấp hoặc thay thế phần mềm mới, tuân thủ quy định Thông tư này.

Điều 10. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 11 năm 2020.

2. Chánh Văn phòng, Giám đốc Trung tâm Chứng thực điện tử quốc gia, Thủ trưởng các cơ quan, đơn vị thuộc Bộ, Giám đốc Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, cơ quan, tổ chức, cá nhân phản ánh kịp thời về Bộ Thông tin và Truyền thông (Trung tâm Chứng thực điện tử quốc gia) để xem xét, giải quyết./.

Nơi nhận:
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Sở TTTT các tỉnh, thành phố trực thuộc TW;
- Sở Văn hóa, Thông tin, Thể thao và Du lịch Bạc Liêu;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Công báo, Cổng thông tin điện tử Chính phủ;
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, NEAC (250).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

PHỤ LỤC
DANH MỤC TIÊU CHUẨN KỸ THUẬT VỀ CHỮ KÝ SỐ TRÊN THÔNG ĐIỆP DỮ LIỆU

(Ban hành kèm theo Thông tư số 22 /2020/TT-BTTTT ngày 07 tháng 9 năm 2020 của Bộ trưởng Bộ Thông tin và Truyền thông)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	**Tiêu chuẩn về định dạng thông điệp dữ liệu**			
1.1	Bộ ký tự và mã hóa	ASCII	American Standard Code for Information Interchange	Khuyến nghị áp dụng
1.2	Bộ ký tự và mã hóa cho tiếng Việt	TCVN 6909:2001	TCVN 6909:2001 " Công nghệ thông tin-Bộ mã ký tự tiếng Việt 16-bit"	Bắt buộc áp dụng
1.3	Trình diễn bộ ký tự	UTF-8	8-bit Universal Character Set (UCS)/ Unicode Transformation Format	Khuyến nghị áp dụng
1.4	Ngôn ngữ định dạng thông điệp dữ liệu	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	Khuyến nghị áp dụng một trong hai tiêu chuẩn
		XML v1.1 (2nd Edition)	Extensible Markup Language version 1.1	
1.5	Định nghĩa các lược đồ trong tài liệu XML	XML Schema version 1.1	XML Schema version 1.1	Khuyến nghị áp dụng
1.6	Trao đổi dữ liệu đặc tả tài liệu XML	XML v2.4.2	XML Metadata Interchange version 2.4.2	Khuyến nghị áp dụng
2	**Tiêu chuẩn về ký số, kiểm tra chữ ký số**			
2.1	**Tiêu chuẩn về ký số trên thiết bị quản lý khóa bí mật, phần mềm ký số, tạo chữ ký số, chứng thư số, phần mềm kiểm tra chữ ký số.**			

2.1.1	Thuật toán mã hóa	TCVN 7816:2007	Công nghệ thông tin. Kỹ thuật mật mã - thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		NIST 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	Khuyến nghị áp dụng
		PKCS#1	RSA Cryptography Standard (Phiên bản 2.1 trở lên) Áp dụng, sử dụng lược đồ RSAES-OAEP để mã hoá Độ dài khóa tối thiểu là 2048 bit	Khuyến nghị áp dụng
		ECC	Elliptic Curve Crytography	Khuyến nghị áp dụng
2.1.2	Thuật toán chữ ký số	TCVN 7635:2007	Các kỹ thuật mật mã - Chữ ký số	- Áp dụng một trong ba tiêu chuẩn. - Đối với tiêu chuẩn TCVN 7635:2007 và PKCS#1: + Phiên bản 2.1 + Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký. + Độ dài khóa tối thiểu là 2048 bit - Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit
		PKCS#1	RSA Cryptography Standard	
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
2.1.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Algorithms	Áp dụng một trong các hàm băm sau: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224,
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

				SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
2.1.4	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	Bắt buộc áp dụng
		XML Signature Syntax and Processing	XML Signature Syntax and Processing	Bắt buộc áp dụng
2.1.5	Quản lý khóa công khai bản tin XML	XKMS v2.0	XML Key Management Specification version 2.0	Bắt buộc áp dụng
2.1.6	Cú pháp thông điệp mật mã cho ký, mã hóa	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing and encrypting version 1.5	Bắt buộc áp dụng
2.2	**Tiêu chuẩn về ký số trên hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số từ xa (remote signing)**			
2.2.1	Yêu cầu chính sách và an ninh cho máy chủ ký số	ETSI TS 119 431-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev	Áp dụng cả bộ tiêu chuẩn 2 phần; Phiên bản V1.1.1 (12/2018)
		ETSI TS 119 431-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation	
2.2.2	Giao thức tạo chữ ký số	ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation	Phiên bản V1.1.1 (03/2019)

2.2.3	Ứng dụng ký trên máy chủ ký số	EN 419241-1:2018	Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements	
2.2.4	Yêu cầu cho mô đun ký số	EN 419241-2:2019	Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing	
2.2.5	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	
3	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**			
3.1	Giao thức truyền, nhận chứng thư số và danh sách chứng thư số bị thu hồi	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP
3.2	Giao thức cho kiểm tra trạng thái chứng thư số trực tuyến	RFC 2560	X.509 Internet Public Key Infrastructure - On-line Certificate status protocol	