BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 16 /2019/TT-BTTTT	*Hà Nội, ngày 05 tháng 12 năm 2019*

THÔNG TƯ
Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa

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 Vụ trưởng Vụ Khoa học và Công nghệ,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa.

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa (Phụ lục kèm theo).

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với 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 được cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số chuyên dùng, tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài có chứng thư số được Bộ Thông tin và Truyền thông công nhận tại Việt Nam cung cấp dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa; tổ chức, cá nhân phát triển ứng dụng sử dụng chữ ký số, cung cấp giải pháp chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa.

Điều 3. Tổ chức thực hiện

1. Bộ Thông tin và Truyền thông rà soát, sửa đổi, bổ sung Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số

theo mô hình ký số trên thiết bị di động và ký số từ xa quy định tại Điều 1 Thông tư này phù hợp với tình hình phát triển công nghệ và chính sách quản lý của Nhà nước.

2. Vụ Khoa học và Công nghệ có trách nhiệm chủ trì rà soát, cập nhật Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa quy định tại Điều 1 Thông tư này.

3. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn, kiểm tra, đánh giá việc áp dụng các tiêu chuẩn thuộc Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa quy định tại Điều 1 Thông tư này.

Điều 4. Điều khoản thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 4 năm 2020.

2. Trong trường hợp có sự khác nhau giữa quy định của Thông tư này với quy định của Thông tư số 39/2017/TT-BTTTT ngày 15 tháng 12 năm 2017 ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước về cùng một tiêu chuẩn liên quan đến sử dụng chữ ký số và dịch vụ chứng thực chữ ký số do các tổ chức cung cấp dịch vụ chứng thực chữ ký số cung cấp trong cơ quan nhà nước thì áp dụng quy định của Thông tư này.

3. Chánh Văn phòng, Vụ trưởng Vụ Khoa học và Công nghệ, Giám đốc Trung tâm Chứng thực điện tử quốc gia, Thủ trưởng các cơ quan, đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

4. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, tổ chức và cá nhân phản ánh kịp thời về Bộ Thông tin và Truyền thông 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 và Sở TTTT các tỉnh, thành phố trực thuộc TW;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Công báo, Cổng thông tin điện tử Chính phủ;
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng thông tin điện tử Bộ TTTT;
- Lưu: VT, KHCN (250).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

Phụ lục

DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNG VỀ CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ THEO MÔ HÌNH KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG VÀ KÝ SỐ TỪ XA

(Ban hành kèm theo Thông tư số 16 /2019/TT-BTTTT ngày 05 tháng 12 năm 2019 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	**Chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động (Mobile PKI)**			
1.1	**Tiêu chuẩn mật mã và chữ ký số**			
1.1.1	Mật mã phi đối xứng và chữ ký số	PKCS #1	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn RSA: + Phiên bản 2.1 + Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký. + Độ dài khóa tối thiểu là 1024 bit - Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
1.1.2	Mật mã đối xứng	TCVN 7816:2007 (FIPS PUB 197)	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES (Advanced Encryption Standard)	Áp dụng một trong hai tiêu chuẩn
		NIST 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.1.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	
1.2	**Tiêu chuẩn thông tin, dữ liệu**			
1.2.1	Định dạng chứng thư số và danh sách thu hồi chứng thư số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
1.2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
1.2.3	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
1.3	**Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số**			
1.3.1	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
1.4	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**			
1.4.1	Lược đồ Giao thức truy nhập thư mục	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng một trong hai tiêu chuẩn

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
1.4.2	Giao thức truy nhập thư mục	RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng tiêu chuẩn RFC 2251 hoặc bộ bốn tiêu chuẩn: RFC 4510, RFC 4511, RFC 4512, RFC 4513
		RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	
		RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	
1.5	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**			
1.5.1	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
1.5.2	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	
1.6	**Tiêu chuẩn bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ chứng thực chữ ký số**			
1.6.1	Yêu cầu an ninh đối với khối an ninh phần cứng	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu mức 3 (level 3)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	HSM			
1.7	**Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số của khách hàng**			
1.7.1	Yêu cầu bảo mật cho thẻ SIM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn FIPS PUB 140-2: Yêu cầu tối thiểu mức 2 (level 2) - Đối với tiêu chuẩn TCVN 8709 (ISO/IEC 15408): Yêu cầu tối thiểu EAL mức 4 (level 4)
		TCVN 8709 (ISO/IEC 15408)	Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin (Common Criteria for Information Technology Security Evaluation)	
1.7.2	Yêu cầu về chức năng, nghiệp vụ	ETSI TR 102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements	Phiên bản V1.1.1
1.7.3	Giao diện dịch vụ Web	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface	Phiên bản V1.1.4
1.7.4	Khung bảo mật	ETSI TR 102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework	Phiên bản V1.1.3
1.7.5	Thông số kỹ thuật chuyển vùng	ETSI TS 102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services	Phiên bản V1.1.3

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2	**Chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa (Remote signing)**			
2.1	Tiêu chuẩn mật mã và chữ ký số			
2.1.1	Mật mã phi đối xứng và chữ ký số	PKCS #1	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn RSA: + 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
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
2.1.2	Mật mã đối xứng	TCVN 7816:2007 (FIPS PUB 197)	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES	Áp dụng một trong hai tiêu chuẩn
		NIST 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	
2.1.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256,
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
				SHA3-384, SHA3-512, SHAKE128, SHAKE256
2.2	**Tiêu chuẩn thông tin, dữ liệu**			
2.2.1	Định dạng chứng thư số và danh sách thu hồi chứng thư số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
2.2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
2.2.3	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
2.2.4	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
2.2.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
2.2.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
2.3	**Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số**			
2.3.1	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
2.4	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**			
2.4.1	Lược đồ Giao thức truy nhập thư mục	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng một trong hai tiêu chuẩn
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			X.509 Certificates	
2.4.2	Giao thức truy nhập thư mục	RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng tiêu chuẩn RFC 2251 hoặc bộ bốn tiêu chuẩn: RFC 4510, RFC 4511, RFC 4512, RFC 4513
		RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	
		RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	
2.5	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**			
2.5.1	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
2.5.2	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	
2.6	**Tiêu chuẩn bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ chứng thực chữ ký số**			
2.6.1	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn FIPS PUB 140-2: Yêu cầu tối thiểu
		EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
				mức 3 (level 3)
2.7	**Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số của khách hàng**			
2.7.1	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	
2.7.2	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)
2.7.3	Ứng dụng ký trên máy chủ ký số	EN 419241-1:2018	Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements	
2.7.4	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	
2.7.5	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	