

Số: /2025/TT-.....

Hà Nội, ngày.....tháng.....năm 2025

Dự thảo Thông tư
Phiên bản 1.0

THÔNG TƯ

**Quy định tiêu chuẩn bắt buộc áp dụng cho chữ
ký số, chứng thư chữ ký số và dịch vụ tin cậy**

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 06 năm 2023;

Căn cứ Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký điện tử và dịch vụ tin cậy;

Căn cứ Nghị định số 55/2025/NĐ-CP ngày 02 tháng 3 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Khoa học và Công nghệ;

Theo đề nghị của Vụ trưởng Vụ Pháp chế và Giám đốc Trung tâm Chứng thực điện tử quốc gia;

Bộ trưởng Bộ Khoa học và Công nghệ ban hành Thông tư quy định tiêu chuẩn bắt buộc áp dụng cho chữ ký số, chứng thư chữ ký số và dịch vụ tin cậy.

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định tiêu chuẩn bắt buộc áp dụng cho chữ ký số, chứng thư chữ ký số và dịch vụ tin cậy như sau:

1. Danh mục Tiêu chuẩn bắt buộc áp dụng cho chữ ký số và dịch vụ chứng thực chữ ký số công cộng tại Phụ lục I ban hành kèm theo Thông tư này.
2. Danh mục Tiêu chuẩn bắt buộc áp dụng cho dịch vụ cấp dấu thời gian tại Phụ lục II ban hành kèm theo Thông tư này.
3. Danh mục Tiêu chuẩn bắt buộc áp dụng cho dịch vụ chứng thực thông điệp dữ liệu tại Phụ lục III ban hành kèm theo Thông tư này.
4. Danh sách các chứng thư chữ ký số gốc tin cậy tại Phụ lục IV ban hành kèm theo Thông tư này.
5. Định dạng thông tin trên chứng thư chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng tại Phụ lục V ban hành kèm theo Thông tư này.
6. Định dạng thông tin trên chứng thư chữ ký số của tổ chức cung cấp dịch vụ cấp dấu thời gian tại Phụ lục VI ban hành kèm theo Thông tư này.

7. Định dạng thông tin trên chứng thư chữ ký số của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu tại Phụ lục VII ban hành kèm theo Thông tư này.

8. Định dạng thông tin trên chứng thư chữ ký số của thuê bao tại Phụ lục VIII ban hành kèm theo Thông tư này.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với:

1. Tổ chức cung cấp dịch vụ Chứng thực điện tử quốc gia.
2. Tổ chức cung cấp dịch vụ tin cậy.
3. Tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử nước ngoài tại Việt Nam.
4. Tổ chức, cá nhân phát triển ứng dụng sử dụng chữ ký số, giải pháp cho dịch vụ tin cậy.

5. Cơ quan, tổ chức, cá nhân tham gia trực tiếp hoặc có liên quan đến chữ ký số và dịch vụ tin cậy.

Điều 3. Tổ chức thực hiện

1. Theo từng thời kỳ, Bộ Khoa học và Công nghệ xem xét, sửa đổi, bổ sung tiêu chuẩn bắt buộc áp dụng cho chữ ký số, chứng thư chữ ký số và dịch vụ tin cậy quy định tại Điều 1 của Thông tư này phù hợp với tình hình phát triển công nghệ và chính sách quản lý của Nhà nước.

2. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn việc áp dụng các tiêu chuẩn quy định tại Điều 1 của Thông tư này.

Điều 4. Điều khoản thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày.....tháng năm 2025.

2. Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số và Thông tư số 16/2019/TT-BTTTT ngày 05 tháng 12 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông 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 hết hiệu lực kể từ ngày Thông tư này có hiệu lực thi hành.

3. Đối với hồ sơ đề nghị cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng, Giấy chứng nhận đăng ký hoạt động của tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng, Giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số chuyên dùng đã nộp cho cơ quan nhà nước có thẩm quyền nhưng đến ngày Thông tư này có hiệu lực thi hành chưa được cấp giấy phép, giấy chứng nhận thì được tiếp tục áp dụng quy định của Thông tư số 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông

và Thông tư số 16/2019/TT-BTTTT ngày 05 tháng 12 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông.

4. Trong vòng 02 năm kể từ ngày Thông tư này có hiệu lực thi hành, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng đang hoạt động hợp pháp có trách nhiệm rà soát, nâng cấp hệ thống thông tin và kỹ thuật đáp ứng quy định tại Thông tư này.

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

6. 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 Khoa học và Công nghệ 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 KHCN 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 KHCN: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, NEAC.

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

Phụ lục I

DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNG VỀ CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

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 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)	
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)	
1.1.3	Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	- Áp dụng một trong các hàm băm sau: - 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	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.2	Tiêu chuẩn thông tin, dữ liệu			
1.2.1	Định dạng chứng thư chữ ký số và danh sách thu hồi chứng thư chữ ký 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 thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
1.2.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
1.2.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
1.2.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
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 chữ ký số			
1.4.1	Lược đồ Giao thức truy nhập thư mục	RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1.4.2	Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bốn tiêu chuẩn
		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 chữ ký số			
1.5.1	Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký 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 chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	
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 đối với phần cứng HSM	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
1.7	Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư chữ ký số và tạo chữ ký số của khách hàng			
1.7.1	Yêu cầu đối với 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
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		PKCS #1	RSA Cryptography Standard	- 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
	Mật mã phi đối xứng và chữ ký số	ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	- 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
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 (Advanced Encryption Standard)	
2.1.3	Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: 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	
2.2	Tiêu chuẩn thông tin, dữ liệu			
2.2.1	Định dạng chứng thư chữ ký số và danh sách thu hồi chứng thư chữ ký 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

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
2.2.3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
2.2.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
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 chữ ký số			
2.4.1	Lược đồ Giao thức truy nhập thư mục	RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
2.4.2	Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bộ bốn tiêu chuẩn
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
		RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	
2.5	Tiêu chuẩn kiểm tra trạng thái chứng thư chữ ký số			
2.5.1	Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký 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 chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	
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 đối với phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn.
		EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	- Đối với tiêu chuẩn FIPS PUB 140-2: Yêu cầu tối thiểu mức 3 (level 3)
2.7	Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư chữ ký số và tạo chữ ký số của khách hàng			
2.7.1	Yêu cầu chính sách 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	Phiên bản V1.2.1

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			service components operating a remote QSCD/SCDev	
		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	Phiên bản V1.2.1
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 V1.2.1
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 đối với phần cứng HSM	EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	
3	Chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số USB Token hoặc HSM			
3.1	Tiêu chuẩn bảo mật cho HSM và thẻ mật mã			
3.1.1	Yêu cầu đối với phần cứng HSM	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
3.1.2	Yêu cầu đối với thẻ Token và Smart card	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Yêu cầu tối thiểu mức 2 (level 2)
3.2	Tiêu chuẩn mật mã và chữ ký số			
3.2.1	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)	
3.2.2	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)	
3.2.3	Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: 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:	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Permutation-Based Hash and Extendable-Output Functions	
3.3	Tiêu chuẩn thông tin, dữ liệu			
3.3.1	Định dạng chứng thư chữ ký số và danh sách thu hồi chứng thư chữ ký số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
3.3.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
3.3.3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
3.3.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
3.3.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
3.3.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
3.4	Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số			
	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
3.5	Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư chữ ký số			
3.5.1	Lược đồ Giao thức	RFC 4523	Lightweight Directory Access Protocol	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	truy nhập thư mục		(LDAP) Schema Definitions for X.509 Certificates	
3.5.2	Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bộ bốn tiêu chuẩn
		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	
3.6	Tiêu chuẩn kiểm tra trạng thái chứng thư chữ ký số			
3.6.1	Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký 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
3.6.2	Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	

Phụ lục II
DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNG
VỀ DỊCH VỤ CẤP DẤU THỜI GIAN

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	Tiêu chuẩn mật mã và chữ ký số			
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)	
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)	
1.3	Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: 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	
2	Tiêu chuẩn thông tin, dữ liệu			

2.1	Định dạng chứng thư chữ ký số và danh sách thu hồi chứng thư chữ ký số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
2.3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
2.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
2.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
2.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
3	Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số			
	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
4	Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư chữ ký số			
4.1	Lược đồ Giao thức truy nhập thư mục	RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
4.2	Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bộ bốn tiêu chuẩn
		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	
5	Tiêu chuẩn kiểm tra trạng thái chứng thư chữ ký số			
5.1	Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký 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
5.2	Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	
6	Tiêu chuẩn bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ cấp dấu thời gian			
	Yêu cầu đối với phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu mức 3 (level 3)
7	Tiêu chuẩn dịch vụ cấp dấu thời gian			
7.1	Giao thức cấp dấu thời gian	RFC 3161	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)	Áp dụng bộ tiêu chuẩn: RFC 3161, RFC 5816.
		RFC 5816	ESSCertIDv2 Update for RFC 3161	
		ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles	Hoặc Tiêu chuẩn ETSI EN 319 422 phiên bản V1.1.1.

7.2	Dịch vụ cấp dấu thời gian	TCVN 7818-1:2024 (ISO/IEC 18014- 1:2008)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 1: Khung tổng quát	Áp dụng bộ tiêu chuẩn: TCVN 7818-1:2024, ISO/IEC 18014-2:2021, TCVN 7818-3:2010, TCVN 7818-4:2024. Hoặc Tiêu chuẩn ETSI EN 319 421 phiên bản V1.2.1
		ISO/IEC 18014- 2:2021	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 2: Cơ chế tạo thẻ độc lập	
		TCVN 7818-3:2010 (ISO/IEC 18014- 3: 2009)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 3: Cơ chế tạo thẻ liên kết	
		TCVN 7818-4:2024 (ISO/IEC 18014- 4:2015)	Công nghệ thông tin – Các kỹ thuật an toàn – Dịch vụ cấp dấu thời gian – Phần 4: Liên kết chuẩn nguồn thời gian	
		ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	

Phụ lục III

DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNG
VỀ DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆN DỮ LIỆU

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	Tiêu chuẩn mật mã và chữ ký số			
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)	
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)	
1.3	Yêu cầu hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: 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	
2	Tiêu chuẩn thông tin, dữ liệu			
2.1	Định dạng chứng thư chữ ký số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and	

	và danh sách thu hồi chứng thư chữ ký số		Certificate Revocation List (CRL) Profile	
2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
2.3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
2.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
2.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
2.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
3	Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số			
	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
4	Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư chữ ký số			
4.1	Lược đồ Giao thức truy nhập thư mục	RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
4.2	Giao thức truy nhập thư mục	RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	Áp dụng bộ bốn tiêu chuẩn
		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	
5	Tiêu chuẩn kiểm tra trạng thái chứng thư chữ ký số			
5.1	Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký 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
5.2	Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	
6	Tiêu chuẩn bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu			
	Yêu cầu đối với phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu mức 3 (level 3)
7	Tiêu chuẩn dịch vụ chứng thực thông điệp dữ liệu			
7.1	Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm: Khung và kiến trúc	ETSI EN 319 522: Part 1	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture	Phiên bản V1.2.1
7.2	Dịch vụ gửi, nhận thông điệp	ETSI EN 319 522: Part 2	Electronic Signatures and Infrastructures (ESI); Electronic Registered	Phiên bản V1.2.1

	dữ liệu bảo đảm: Nội dung ngữ nghĩa		Delivery Services; Part 2: Semantic contents	
7.3	Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm: Định dạng	ETSI EN 319 522: Part 3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats	Phiên bản V1.2.1
7.4	Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm: Ràng buộc	ETSI EN 319 522: Part 4-1	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings	Phiên bản V1.2.1
		ETSI EN 319 522: Part 4-2	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings	Phiên bản V1.1.1
7.5	Yêu cầu chính sách đối với các tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm	ETSI EN 319 521	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers	Phiên bản V1.1.1
7.6	Yêu cầu chính sách đối với các tổ chức cung cấp dịch vụ thư điện tử bảo đảm	ETSI EN 319 531	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers	Phiên bản V1.1.1
7.7	Dịch vụ thư điện tử bảo đảm	ETSI EN 319 532	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services	Phiên bản V1.2.1
7.8	Yêu cầu chính sách	ETSI TS 119 511	Electronic Signatures and Infrastructures (ESI);	Phiên bản V1.1.1

	để bảo quản chữ ký số hoặc thông điệp dữ liệu thông qua kỹ thuật chữ ký số		Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques	
7.9	Giao thức dịch vụ tin cậy bảo quản dữ liệu dài hạn	ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services	Phiên bản V1.1.1
7.10	Tạo và xác thực chữ ký số AdES	ETSI EN 319 102	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures	Phiên bản V1.3.1
7.11	Chính sách về chữ ký số và chữ ký điện tử	ETSI TS 119 172	Electronic Signatures and Infrastructures (ESI); Signature Policies	Phiên bản V1.1.1
7.12	Yêu cầu chính sách đối với các nhà cung cấp dịch vụ tin cậy	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers	Phiên bản V2.3.1
7.13	Bảo mật hệ thống bảo quản dữ liệu	ETSI TS 101 533-1	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management	Áp dụng ba tiêu chuẩn: ETSI TS 101 533-1 phiên bản V1.3.1; RFC 4998 và RFC 6283
		RFC 4998	Evidence Record Syntax (ERS)	
		RFC 6283	Extensible Markup Language Evidence Record Syntax (XMLERS)	
8	Tiêu chuẩn về ký số trên thông điệp dữ liệu để lưu trữ dài hạn			
8.1	Chữ ký số cho CMS	ETSI EN 319 122-1	Electronic Signatures and Infrastructures (ESI); CAdES digital	Phiên bản V1.3.1

			signatures; Part 1: Building blocks and CAdES baseline signatures	
		ETSI EN 319 122-2	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures	Phiên bản V1.1.1
8.2	Chữ ký số cho PDF	ETSI EN 319 142-1	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures	Áp dụng một trong hai bộ tiêu chuẩn: ETSI EN 319 142-1 Phiên bản V1.1.1 ETSI EN 319 142-2 Phiên bản V1.1.1 Hoặc ISO 14533-3:2017 ISO 32000-1:2008 ISO 32000-2:2020
		ETSI EN 319 142-2	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles	
		ISO 32000-1:2008	Document management - Portable document format - Part 1: PDF 1.7	
		ISO 14533-3:2017	Processes, data elements and documents in commerce, industry and administration — Long-term signature formats — Part 3: Long-term signature profiles for PDF Advanced Electronic Signatures (PAdES)	
		ISO 32000-2:2020	Document management - Portable document format - Part 2: PDF 2.0	
8.3	Chữ ký số cho XML	ETSI EN 319 132-1	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures	Phiên bản V1.2.1

		ETSI EN 319 132-2	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures	Phiên bản V1.1.1
--	--	----------------------	---	------------------

Phụ lục IV

DANH SÁCH CÁC CHỨNG THƯ CHỮ KÝ SỐ GỐC TIN CẬY

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

1. Danh sách các chứng thư chữ ký số gốc tin cậy dưới dạng PEM (Privacy Enhanced Mail)

STT	Chứng thư chữ ký số gốc tin cậy	Dạng PEM
1	Chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (chứng thư chữ ký số SHA256)	
2	Chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ (chứng thư chữ ký số SHA256)	

2. Thông tin về khóa công khai trên các chứng thư chữ ký số gốc tin cậy

STT	Chứng thư chữ ký số gốc tin cậy	Thuật toán sinh khóa	Khóa công khai	
			Mô-đun n (Hexadeximal)	Số mũ công khai e (Hexadeximal)
1	Chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (Chứng thư chữ ký số SHA-256)	RSA 2048 bit		
2	Chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia (Chứng thư chữ ký số SHA-256)	RSA 4096 bit		
3	Chứng thư chữ ký số gốc của Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (chứng thư chữ ký số SHA256)	RSA 4096 bit		

Phụ lục V

ĐỊNH DẠNG THÔNG TIN TRÊN CHỨNG THƯ CHỮ KÝ SỐ CỦA TỔ CHỨC CUNG CẤP DỊCH CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

ST T	Trường		Ý nghĩa	Quy định
				Chứng thư chữ ký số dịch vụ tin cậy
1	Version		Phiên bản của chứng thư chữ ký số	Version 3 (value = 2)
2	Serial Number		Số hiệu chứng thư chữ ký số	Số nguyên dương ngẫu nhiên xác định duy nhất một chứng thư chữ ký số do CA cấp cho thuê bao, độ dài không quá 20 octet (byte)
3	Signature		Thuật toán ký chứng thư chữ ký số của CA	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
4	Issuer	common Name	Tên của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cấp chứng thư chữ ký số	Tên giao dịch của tổ chức cung cấp dịch vụ tin cậy trong hồ sơ đề nghị cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của doanh nghiệp được cấp phép cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
5	Validity	notBefore	Thời điểm có hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCtime. - Từ năm 2050 trở đi: GeneralizedTime.
		notAfter	Thời điểm hết hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCtime. - Từ năm 2050 trở đi: GeneralizedTime.
6	Subject	userID	Định danh của tổ chức/doanh nghiệp	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] của tổ chức/doanh

			cung cấp dịch vụ tin cậy	ngành cung cấp dịch vụ tin cậy
		commonName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy được cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy (nếu có)
		stateOrProvinceName	Tên tỉnh/TP trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tỉnh/TP nơi đặt trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
7	Subject Public Key Info	algorithm	Thuật toán sinh khóa	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
		subjectPublicKey	Khóa công khai của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Theo quy định của Bộ Khoa học và Công nghệ tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
8	Enhanced Key Usage		Tên dịch vụ cung cấp	OID của dịch vụ cung cấp
9	signatureAlgorithm	Thuật toán ký chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia	Cùng thuật toán tại trường số 3	
10	signatureValue	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	

Phụ lục VI

ĐỊNH DẠNG THÔNG TIN TRÊN CHỨNG THƯ CHỮ KÝ SỐ CỦA TỔ CHỨC CUNG CẤP DỊCH VỤ CẤP DẤU THỜI GIAN

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

STT	Trường		Ý nghĩa	Quy định
				Chứng thư chữ ký số dịch vụ tin cậy
1	Version		Phiên bản của chứng thư chữ ký số	Version 3 (value = 2)
2	Serial Number		Số hiệu chứng thư chữ ký số	Số nguyên dương ngẫu nhiên xác định duy nhất một chứng thư chữ ký số do CA cấp cho thuê bao, độ dài không quá 20 octet (byte)
3	Signature		Thuật toán ký chứng thư chữ ký số của CA	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
4	Issuer	common Name	Tên của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cấp chứng thư chữ ký số	Tên giao dịch của tổ chức cung cấp dịch vụ tin cậy trong hồ sơ đề nghị cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của doanh nghiệp được cấp phép cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
5	Validity	notBefore	Thời điểm có hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
		notAfter	Thời điểm hết hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
6	Subject	userID	Định danh của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy
		commonName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy được cấp chứng thư chữ ký số

		organizationName	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy (nếu có)
		stateOrProvinceName	Tên tỉnh/TP trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tỉnh/TP nơi đặt trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
7	Subject Public Key Info	algorithm	Thuật toán sinh khóa	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy
		subjectPublicKey	Khóa công khai của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Theo quy định của Bộ Khoa học và Công nghệ tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy
8	Enhanced Key Usage		Tên dịch vụ cung cấp	OID của dịch vụ cung cấp
9	signatureAlgorithm	Thuật toán ký chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia	Cùng thuật toán tại trường số 3	
10	signatureValue	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	

Phụ lục VII

ĐỊNH DẠNG THÔNG TIN TRÊN CHỨNG THƯ CHỮ KÝ SỐ
CỦA TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆN
DỮ LIỆU

(Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

STT	Trường		Ý nghĩa	Quy định
				Chứng thư chữ ký số dịch vụ tin cậy
1	Version		Phiên bản của chứng thư chữ ký số	Version 3 (value = 2)
2	Serial Number		Số hiệu chứng thư chữ ký số	Số nguyên dương ngẫu nhiên xác định duy nhất một chứng thư chữ ký số do CA cấp cho thuê bao, độ dài không quá 20 octet (byte)
3	Signature		Thuật toán ký chứng thư chữ ký số của CA	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
4	Issuer	common Name	Tên của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia cấp chứng thư chữ ký số	Tên giao dịch của tổ chức cung cấp dịch vụ tin cậy trong hồ sơ đề nghị cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của doanh nghiệp được cấp phép cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
5	Validity	notBefore	Thời điểm có hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
		notAfter	Thời điểm hết hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
6	Subject	userID	Định danh của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy

		commonName	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy được cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tổ chức/đơn vị quản lý tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy (nếu có)
		stateOrProvinceName	Tên tỉnh/TP trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Tên của tỉnh/TP nơi đặt trụ sở chính của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy
		countryName	Tên nước	VN
7	Subject Public Key Info	algorithm	Thuật toán sinh khóa	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy
		subjectPublicKey	Khóa công khai của tổ chức/doanh nghiệp cung cấp dịch vụ tin cậy	Theo quy định của Bộ Khoa học và Công nghệ tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy
8	Enhanced Key Usage		Tên dịch vụ cung cấp	OID của dịch vụ cung cấp
9	signatureAlgorithm	Thuật toán ký chứng thư chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia	Cùng thuật toán tại trường số 3	
10	signatureValue	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	Chữ ký số của Tổ chức cung cấp dịch vụ chứng thực điện tử quốc gia trên chứng thư chữ ký số	

Phụ lục VIII

ĐỊNH DẠNG THÔNG TIN TRÊN CHỨNG THƯ CHỮ KÝ SỐ CỦA THUÊ BAO (Ban hành kèm theo Thông tư số.....ngày..... tháng..... năm.....của Bộ trưởng Bộ Khoa học và Công nghệ)

ST T	Trường		Ý nghĩa	Quy định
				Chứng thư chữ ký số công cộng
1	Version		Phiên bản của chứng thư chữ ký số	Version 3 (value = 2)
2	Serial Number		Số hiệu chứng thư chữ ký số	Số nguyên dương ngẫu nhiên xác định duy nhất một chứng thư chữ ký số do CA cấp cho thuê bao, độ dài không quá 20 octet (byte)
3	Signature		Thuật toán ký chứng thư chữ ký số của CA	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
4	Issuer	common Name	Tên của CA cấp chứng thư chữ ký số	Tên giao dịch của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng trong hồ sơ đề nghị cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/doanh nghiệp vận hành CA	Tên của doanh nghiệp được cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng
		countryName	Tên nước	VN
5	Validity	notBefore	Thời điểm có hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
		notAfter	Thời điểm hết hiệu lực của chứng thư chữ ký số	- Trước năm 2050: UTCTime. - Từ năm 2050 trở đi: GeneralizedTime.
6	Subject	userID	Định danh của thuê bao	MST: [mã số thuế] hoặc MNS: [mã quan hệ ngân sách] hoặc

				BHXH: [mã số bảo hiểm xã hội] hoặc CMND: [số chứng minh nhân dân] hoặc HC: [số hộ chiếu] hoặc CCCD: [số thẻ căn cước công dân] hoặc CC: [số thẻ căn cước] <i>Các trường hợp khác theo thỏa thuận giữa thuê bao và tổ chức cung cấp dịch vụ chứng thực chữ ký số.</i>
		commonName	Tên của thuê bao	Tên của thuê bao được cấp chứng thư chữ ký số
		organizationName	Tên của tổ chức/đơn vị quản lý thuê bao	Tên của tổ chức/đơn vị quản lý thuê bao (nếu có)
		stateOrProvinceName	Tên tỉnh/TP nơi sống/làm việc của thuê bao	Tên của tỉnh/TP nơi sống/làm việc của thuê bao bằng tiếng Việt, có dấu, các chữ cái đầu viết hoa.
		countryName	Tên nước	VN
7	Subject Public Key Info	algorithm	Thuật toán sinh khóa	Theo quy định của Bộ Khoa học và Công nghệ về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
		subjectPublicKey	Khóa công khai của thuê bao	Theo quy định của Bộ Khoa học và Công nghệ về tiêu chuẩn bắt buộc áp dụng về chữ ký điện tử và dịch vụ tin cậy đang có hiệu lực
8	Enhanced Key Usage		Tên dịch vụ sử dụng	OID của dịch vụ sử dụng
9	signatureAlgorithm	Thuật toán ký chứng thư chữ ký số của CA	Cùng thuật toán tại trường số 3	
10	signatureValue	Chữ ký số của CA trên chứng thư chữ ký số	Chữ ký số của CA trên chứng thư chữ ký số	