BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 06/2015/TT-BTTTT	*Hà Nội, ngày 23 tháng 3 năm 2015*

THÔNG TƯ
Quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số

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

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 15 tháng 02 năm 2007 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, Nghị định số 106/2011/NĐ-CP ngày 23 tháng 11 năm 2011 và Nghị định số 170/2013/NĐ-CP ngày 13 tháng 11 năm 2013;

Căn cứ Nghị định số 132/2013/NĐ-CP ngày 16 tháng 10 năm 2013 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.

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 (Phụ lục kèm theo).

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với:

1. Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia;

2. Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng;

3. Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng được Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số;

4. Tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được Bộ Thông tin và Truyền thông cấp giấy công nhận.

Điều 3. Tổ chức thực hiện

1. Theo từng thời kỳ, Bộ Thông tin và Truyền thông xem xét, sửa đổi, bổ sung Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số 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. Vụ Khoa học và Công nghệ có trách nhiệm chủ trì định kỳ rà soát, cập nhật Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số quy định tại Điều 1 của Thông tư này.

3. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn 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 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 15 tháng 9 năm 2015.

2. Quyết định số 59/2008/QĐ-BTTTT ngày 31 tháng 12 năm 2008 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số hết hiệu lực kể từ ngày Thông tư này có hiệu lực, trừ quy định về "Hàm băm bảo mật" tại mục 2.3 của Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số ban hành kèm theo Quyết định số 59/2008/QĐ-BTTTT tiếp tục có hiệu lực đến hết ngày 31 tháng 3 năm 2016.

3. Trong trường hợp có sự khác nhau giữa quy định của Thông tư này với quy định của Thông tư 22/2013/TT-BTTTT ngày 23 tháng 12 năm 2013 ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin

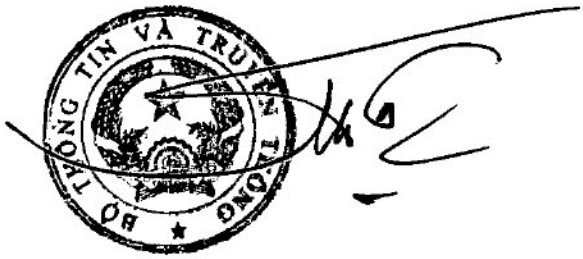
trong cơ quan nhà nước về cùng một tiêu chuẩn liên quan đến sử dụng chữ ký số và dịch vụ chứng thực chữ ký số do các tổ chức cung cấp dịch vụ chứng thực chữ ký số cung cấp trong cơ quan nhà nước thì áp dụng quy định của Thông tư này.

4. 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 và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

5. 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 và các Phó Thủ tướng Chính phủ;
- Văn phòng TW Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội;
- Văn phòng Chính phủ;
- Ủy ban quốc gia về ứng dụng CNTT;
- Ban Chỉ đạo CNTT của cơ quan Đảng;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan Trung ương của các đoàn thể;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc CP;
- Ủy ban nhân dân các tỉnh, TP trực thuộc TW;
- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các tổ chức cung cấp dịch vụ chứng thực chữ ký số;
- 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;
- Lưu: VT, KHCN (5b).

BỘ TRƯỞNG



Nguyễn Bắc Son

Phụ lục

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

(Ban hành kèm theo Thông tư số: 06/2015/TT-BTTTT ngày 23 tháng 3 năm 2015 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 bảo mật cho HSM và thẻ mật mã**			
1.1	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Yêu cầu tối thiểu mức 3 (level 3)
1.2	Yêu cầu an ninh đối với thẻ Token và Smart card	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Yêu cầu tối thiểu mức 2 (level 2)
2	**Tiêu chuẩn mật mã và chữ ký số**			
2.1	Mật mã phi đối xứng và chữ ký số	PKCS #1	RSA Cryptography Standard	- Phiên bản 2.1 - Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký
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	Áp dụng một trong hai tiêu chuẩn
		NIST 800-67	Recommendation for the Triple Data Encryption Algorithem (TDEA) Block Cipher	
2.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong sáu hàm băm: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
3	**Tiêu chuẩn thông tin, dữ liệu**			
3.1	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	
3.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
3.3	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
3.4	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
3.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
3.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
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	
5	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**			
5.1	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 X.509 Certificates	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
5.2	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	
6	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**			
6.1	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
6.2	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	
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)	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
7.2	Dịch vụ cấp dấu thời gian	TCVN 7818-1:2007 (ISO/IEC 18014-1:2002)	Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ tem thời gian - Phần 1: Khung tổng quát	Áp dụng bộ ba tiêu chuẩn: TCVN 7818-1:2007 TCVN 7818-2:2007 TCVN 7818-3:2010
		TCVN 7818-2:2007 (ISO/IEC 18014 - 2: 2002)	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	