BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 59/2008/QĐ-BTTTT	*Hà Nội, ngày 31 tháng 12 năm 2008*

QUYẾT ĐỊNH

Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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;

Căn cứ Nghị định số 187/2007/NĐ-CP ngày 25 tháng 12 năm 2007 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 và Cục trưởng Cục Ứng dụng Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số".

Điều 2. Tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia; 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 được Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số; tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được Chính phủ Việt Nam công nhận phải tuân thủ các tiêu chuẩn trong Danh mục tiêu chuẩn ban hành bởi Quyết định này.

Điều 3. Danh mục tiêu chuẩn này được định kỳ xem xét cập nhật, sửa đổi, bổ sung phù hợp với điều kiện thực tế của Việt Nam.

Điều 4. Quyết định này có hiệu lực thi hành sau 15 (mười lăm) ngày, kể từ ngày đăng Công báo.

Điều 5. Chánh Văn phòng, Vụ trưởng Vụ Khoa học và Công nghệ, Cục trưởng Cục Ứng dụng Công nghệ thông tin, Thủ trưởng các cơ quan, đơn vị thuộc Bộ, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Ban Chỉ đạo Quốc gia về CNTT (để b/c);
- Ban Chỉ đạo CNTT của cơ quan Đảng;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc CP;
- Uỷ ban nhân dân các tỉnh, TP trực thuộc TW;
- Đơn vị chuyên trách về CNTT các Bộ, ngành;
- Sở Thông tin và Truyền thông các tỉnh, TP trực thuộc TW;
- Cục Kiểm tra văn bản (Bộ Tư pháp);
- TTĐT, Công báo;
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng, TTĐT;
- Lưu: VT, KHCN, UDCNTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

(đã ký)

Nguyễn Minh Hồng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

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
Ngày 31 tháng 12 năm 2008 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	**Chuẩn bảo mật cho HSM**			
1.1	Bảo mật cho khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu level 3
2	**Chuẩn mã hóa**			
2.1	Mã hoá 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	Mã hoá đối xứng	FIPS PUB 197	Advanced Encryption Standard (AES)	Áp dụng AES hoặc 3DES
		FIPS PUB 46-3	Data Encryption Standard (DES)	
2.3	Hàm băm bảo mật	FIPS PUB 180-2	Secure Hash Standard	Áp dụng một trong bốn hàm băm an toàn: SHA-1, SHA-256, SHA-384, SHA-512
3	**Chuẩn tạo yêu cầu và trao đổi chứng thư số**			
3.1	Định dạng chứng thư số và danh sách thu hồi chứng thư số	RFC 3280	Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile	
3.2	Cú pháp thông điệp mã hoá	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
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	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
4	**Chuẩn về chính sách và quy chế chứng thực chữ ký số**			
4.1	Khung quy chế chứng thực và chính sách chứng thư	RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework	
5	**Chuẩn về lưu trữ và truy xuất chứng thư số**			
5.1	Giao thức lưu trữ và truy xuất chứng thư số	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng RFC 2587 hoặc RFC 4523
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
		RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng 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	**Chuẩn về kiểm tra trạng thái chứng thư số**			
6.1	Giao thức cho kiểm tra trạng thái chứng thư số	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP