|  |  |
| --- | --- |
| BỘ THÔNG TIN VÀ TRUYỀN THÔNG | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAMĐộc lập – Tự do – Hạnh phúc |
| Số: /2019/TT-BTTTT | *Hà Nội, ngàythángnăm 2019* |

**DỰ THẢO 1.0**

THÔNG TƯ

Quy định Danh mục tiêu chuẩn bắt buộc áp dụng

về chữ ký số và dịch vụ chứng thực chữ ký số trên thiết bị di động

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 trên thiết bị di động.*

**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 sốtrên thiết bị di động (Phụ lục kèm theo).

**Điều 2.Đối tượng áp dụng**

1. Thông tư này áp dụng đối với tổ chức cung cấp dịch vụ chứng thực chữ ký số trên thiết bị di động, bao gồm:

a)Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng;

b)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;

c) 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.

2. Thông tư này cũng áp dụng đối với tổ chức, cá nhân phát triển ứng dụng sử dụng chữ ký số trên thiết bị di động và tổ chức, cá nhân cung cấp giải pháp chữ ký số trên thiết bị di động.

**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 sốtrên thiết bị di động 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 trìđịnh kỳ rà soát, cập nhật Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký sốtrên thiết bị di động quy định tạiĐiều 1 của Thông tư này.

3. Trung tâm Chứng thực điện tử quốc gia có trách nhiệm hướng dẫn, kiểm tra, đánh giáviệc áp dụng các tiêu chuẩn thuộc Danh mục tiêu chuẩn bắt buộc áp dụngvề chữ ký số và dịch vụ chứng thực chữ ký sốtrên thiết bị di động quy định tạiĐiều 1 của Thông tư này.

**Điều 4.Điều khoản thi hành**

1.Thông tư này có hiệu lực thi hành kể từ ngày 15tháng01 năm 2020.

2. Trong trường hợp có sự khác nhau giữa quy định của Thông tư này với quy định của Thông tư 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 và 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 (để b/c);  - Văn phòng 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;- 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;  - Lưu: VT, KHCN (250). | **BỘ TRƯỞNG****Nguyễn Mạnh Hùng** |

**Phụ lục**

# DANH MỤC TIÊU CHUẨN BẮT BUỘC ÁP DỤNGVỀ CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

*(Ban hành kèm theo Thông tư số /2019/TT-BTTTTngày tháng năm 2019của 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 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:- Đôi với tiêu chuẩn RSA: + Phiên bản 2.1+ Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký.- Đối với tiêu chuẩn ECDSA: Độ dài khóa tối thiểu 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 | Áp dụng một trong hai tiêu chuẩn |
| NIST 800-67 | Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher |
| 1.3 | 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  |
| **2** | **Tiêu chuẩn thông tin, dữ liệu** |
| 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 | 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 số** |
| 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 X.509 Certificates |
| 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 |
| **5** | **Tiêu chuẩn kiểm tra trạng thái chứng thư số** |
| 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 |
| 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 |  |
| **6. Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số di động (Mobile PKI)** |
| 6.1 | 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 ISO/IEC 15408: Yêu cầu tối thiểu mức 4 (level 4) |
| Common Criteria (ISO/IEC 15408) | Common Criteria for Information Technology Security Evaluation |
| 6.2 | 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 |
| 6.3 | Giao diện dịch vụ Web | ETSI TS 102 204 | Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface | Phiên bản V1.1.4 |
| 6.4 | Khung bảo mật | ETSI TR 102 206  | Mobile Commerce (M-COMM);Mobile Signature Service;Security Framework | Phiên bản V1.1.3 |
| 6.5 | 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 |
| **7. Tiêu chuẩn 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)** |
| 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 (2018-12) |
| 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 |
| 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(2019-03) |
| 7.3 | Ứng dụng ký trên máy chủ ký số | CEN EN 419 241-1 | Security Requirements for Trustworthy Systems Supporting Server Signing; |  |
| 7.4 | Yêu cầu cho mô đun ký số | CEN EN 419 241-2 | Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing | Phiên bản V0.16 |
| 7.5 | Yêu cầu an ninh đối với khối an ninh phần cứng HSM | CEN EN 419 221-5 | Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services | Phiên bản V0.15(2016-11) |