**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**THUYẾT MINH**

**DANH MỤC TIÊU CHUẨN VỀ CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG**

|  |  |
| --- | --- |
|  |  |

**Hà Nội, 9/2019**

**MỤC LỤC**

**MỤC LỤC**

[DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT 4](#_Toc18421506)

[I. TỔNG QUAN 6](#_Toc18421507)

[1. Tổng quan về chữ ký số và dịch vụ chứng thực chữ ký số trên thiết bị di động (Mobile PKI) 6](#_Toc18421508)

[2. Nhu cầu triển khai dịch vụ và tiêu chuẩn hóa Mobile PKI tại Việt Nam 6](#_Toc18421509)

[II. TÌNH HÌNH XÂY DỰNG TIÊU CHUẨN MOBILE PKI 7](#_Toc18421510)

[1. Một số văn bản quy định có liên quan do Bộ TTTT ban hành 7](#_Toc18421511)

[2. Tình hình xây dựng tiêu chuẩn về Mobile PKI trên thế giới 8](#_Toc18421512)

[2.1. Các tổ chức ban hành tiêu chuẩn về PKI 8](#_Toc18421513)

[2.2. Tình hình xây dựng tiêu chuẩn về Mobile PKI 8](#_Toc18421515)

[2.2.1. Hiện trạng xây dựng tiêu chuẩn Mobile PKI của Châu Âu 8](#_Toc18421516)

[2.2.2. Hiện trạng xây dựng tiêu chuẩn Mobile PKI của Mỹ 10](#_Toc18421517)

[III. ĐỀ XUẤT DANH MỤC TIÊU CHUẨN CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG 11](#_Toc18421518)

[1. Các tiêu chuẩn về chữ ký số và dịch vụ chứng thực 12](#_Toc18421520)

2. Các tiêu chuẩn cho hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số di động (SIMPKI)…..………….………………………………………………………………122

[2.1. Tổng quan về mô hình SIM PKI 13](#_Toc18421521)

[2.1.1. Mô hình tổng quan 13](#_Toc18421522)

[2.1.2. Thành phần chính 16](#_Toc18421523)

[2.1.3. Hoạt động 19](#_Toc18421524)

[2.2. Các đối tượng cần chuẩn hóa 28](#_Toc18421525)

[2.3. Kinh nghiệm quốc tế 29](#_Toc18421526)

[2.4. Đề xuất tiêu chuẩn 30](#_Toc18421527)

3. Các tiêu chuẩn cho hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số từ xa (RemoteSigning)...………………..…………………………………………………122

[3. 1. Tổng quan mô hình ký số từ xa (remote signing) 31](#_Toc18421528)

[3.1.1. Mô hình tổng quan 31](#_Toc18421529)

[3.1.2. Thành phần chính 32](#_Toc18421530)

3.1.3. Mô tả các tiêu chuẩn….…………………………………………………………………………..[36](#_Toc18421531)

[3.1.4. Hoạt động 36](#_Toc18421532)

[3.2. Các đối tượng cần chuẩn hóa 38](#_Toc18421533)

[3.3. Kinh nghiệm quốc tế 38](#_Toc18421534)

[3.4. Đề xuất tiêu chuẩn 39](#_Toc18421535)

# DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

|  |  |
| --- | --- |
| PKI | Cơ sở hạ tầng khóa công khai(Public Key Infrastructure) |
| ETSI | Viện Tiêu chuẩn Viễn Thông Châu Âu(European Telecommunications Standards Institute) |
| CEN | Ủy ban Tiêu chuẩn Châu Âu |
| ANSI | Viện Tiêu chuẩn Quốc gia Hoa Kỳ (American National Standards Institute) |
| NIST | Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ |
| ECDSA | Thuật toán ký số dựa trên đường cong eliptic (Elliptic Curve Digital Signature Algorithm) |
| TS | Đặc tả kỹ thuật(Technical Specification) |
| TR | Báo cáo kỹ thuật(Technical Report) |
| AP | Nhà cung cấp ứng dụng(Application Provider) |
| MSSP | Nhà cung cấp dịch vụ chữ ký di động(Mobile Signature service provider) |
| CA | Tổ chức cung cấp dịch vụ Chứng thực chữ ký số(Certification Authority) |
| RA | Đại lý(Registration Agent) |
| OCSP | Giao thức kiểm tra chứng thư số trực tuyến (Online Certificate Status Protocol) |
| RFC | Tài liệu công nghệ Internet (Request for Comments) |
| Root CA | Tổ chức cung cấp dịch vụ chứng thực chữ ký số gốc |
| RSA | Thuật toán mật mã hóa khóa công khai (Ron Rivest, Adi Shamir và Len Adleman). |
| PP | Hồ sơ bảo vệ(Protection Profile) |
| FIPS | Tiêu chuẩn xử lý liên bang(Federal Information Processing Standards) |
| EAL | Mức đảm bảo đánh giá(Evaluation Assurance Level) |
| CC | Tiêu chí chung đánh giá an toàn thôngtin (Common Criteria for Information Technology Security Evaluation) |
| IEEE | Viện kỹ nghệ điện và điện tử (Institute of Electrical and Electronic Engineers) |
| IETF | Nhóm đặc trách kỹ thuật Internet (Internet Engineering Task Force) |

# I. TỔNG QUAN

## 1. Tổng quan về chữ ký số và dịch vụ chứng thực chữ ký số trên thiết bị di động (Mobile PKI)

Ngày nay, thiết bị di động (máy tính bảng, điện thoại di động, laptop...) đang phát triển rất mạnh và là một thiết bị không thể thiếu trong xã hội. Việc sử dụng các thiết bị di động để trao đổi thông tin, thực hiện các giao dịch điện tử như tài chính, hành chính công ngày càng trở nên phổ biến. Chỉ với thiết bị di động có khả năng kết nối Internet qua Wifi, 3G, 4G..., người dùng có thể thực hiện giao dịch mọi lúc, mọi nơi.

Hiện nay, việc sử dụng mật mã khoá công khai và dịch vụ chứng thực điện tử để đảm bảo an toàn thông tin trong các hoạt động giao dịch điện tử là giải pháp được nhiều quốc gia trên thế giới sử dụng. Để triển khai chữ ký số trên thiết bị di động, trên thế giới đã sử dụng nhiều giải pháp khác nhau, tùy thuộc vào trình độ phát triển CNTT và hiện trạng ứng dụng PKI của từng nước. Dựa trên phương thức lưu trữ khóa bí mật trên thiết bị di động, có thể phân loại Mobile PKI theo 02 hình thức như sau:

- Khóa bí mật lưu trên thiết bị di động (SIM based)

- Khóa bí mật lưu trên máy chủ tập trung (Cloud-based)

## 2. Nhu cầu triển khai dịch vụ và tiêu chuẩn hóa Mobile PKI tại Việt Nam

Ở Việt Nam, chữ ký số và dịch vụ chứng thực chữ ký số truyền thống trên các máy tính đã được triển khai rộng rãi.Cùng với việc chuyển các ứng dụng từ trên máy tính sang các thiết bị di động thì chữ ký số cũng không nằm ngoài xu thế đó. Việc ứng dụng chữ ký số qua thiết bị di động đang cõ nhu cầu rất lớn do tính thuận tiện cho nghiệp vụ kinh doanh, giao dịch điện tử.

Nghị định số 130/2018/NĐ-CP (điểm b khoản 4 Điều 13; khoản 5 Điều 41; và điểm b khoản 2 Điều 46) đã quy định: tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng được cấp phép; tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng của cơ quan, tổ chức được cấp giấy chứng nhận đảm bảo an toàn; tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được công nhận phải tuân thủ các quy chuẩn kỹ thuật, tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số do Bộ TTTT ban hành.

- Đối với việc cung cấp dịch vụ chứng thực chữ ký số truyền thống, Bộ TTTT đã ban hành Thông tư 06/2015/TT-BTTTTngày 23/3/2015 quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

- Đối với việc cung cấp dịch vụ chứng thực chữ ký số qua thiết bị di động, do Mobile PKI có những đặc thù riêng, nhiều giải pháp triển khai; tương ứng với mỗi giải pháp là các tiêu chuẩn kỹ thuật riêng.Thông tư 06/2015/TT-BTTTT chưa bao quát các giải pháp công nghệ và tiêu chuẩn này.

Do vậy Bộ TTTT đã tổ chức nghiên cứu, xây dựng quy định Danh mục quy chuẩn kỹ thuật, tiêu chuẩn bắt buộc áp dụng về chữ ký số trên thiết bị di động để áp dụng cho các tổ chức cung cấp dịch vụ chứng thực chữ ký số qua thiết bị di động, đảm bảo tính an toàn, giá trị pháp lý của chữ ký số; làm căn cứ để cấp phép, cấp giấy chứng nhận, công nhận cho tổ chức cung cấp dịch vụ chứng thực chữ ký số và thúc đẩy triển khai dịch vụ chữ ký số qua thiết bị di động tại Việt Nam.

# II. TÌNH HÌNH XÂY DỰNG TIÊU CHUẨN MOBILE PKI

## 1. Một số văn bản quy định có liên quan do Bộ TTTT ban hành

Hiện tại, các văn bản quy định do Bộ TTTT ban hành có liên quan đến tiêu chuẩn chữ ký số và dịch vụ chứng thực chữ ký số tại Việt Nam bao gồm:

- Thông tư số 06/2015/TT-BTTTT ngày 23/3/2015 quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

- Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

- Thông tư số 41/2017/TT-BTTTT ngày 19/12/2017 quy định về sử dụng chữ ký số trên văn bản điện tử trong cơ quan nhà nước.

## 2. Tình hình xây dựng tiêu chuẩn về Mobile PKI trên thế giới

## 2.1. Các tổ chức ban hành tiêu chuẩn về PKI

## Theo nghiên cứu, hầu hết các nước trên thế giới đều dựa vào các tiêu chuẩn mà các tổ chức quốc tế đưa ra để áp dụng toàn bộ hoặc chọn lọc một số tiêu chuẩn để áp dụng cho nước mình.Một số nước phát triển (như Mỹ) cũng tự xây dựng các tiêu chuẩn về mật mã và cũng được các nước khác lựa chọn, chấp nhận áp dụng.Việc lựa chọn áp dụng tiêu chuẩn phụ thuộc vào trình độ phát triển CNTT và hiện trạng ứng dụng PKI của mỗi nước.

Các Tổ chức ban hành các tiêu chuẩn liên quan PKI trên thế giới gồm có:

- ISO:Tổ chức tiêu chuẩn hóa thế giới

- NIST: Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ

- ANSI: Viện tiêu chuẩn quốc gia Hoa Kỳ

- ETSI: Viện tiêu chuẩn viễn thông Châu Âu

- CEN: Ủy ban tiêu chuẩn Châu Âu

- IEEE: Viện kỹ nghệ điện và điện tử

- IETF: Nhóm đặc trách về kỹ thuật Internet

- PKIX: Nhóm làm việc về khóa công khai của IETF

- RSA PKCS: Tập các tiêu chuẩn về PKI của RSA

## 2.2. Tình hình xây dựng tiêu chuẩn về Mobile PKI

### 2.2.1. Hiện trạng xây dựng tiêu chuẩn Mobile PKI của Châu Âu

Đối với Liên minh châu Âu (EU), thương mại điện tử là cơ hội tuyệt vời để thúc đẩy các chương trình hội nhập kinh tế.Cách tiếp cận như vậy đòi hỏi một cơ chế bảo mật thích hợp để cho phép hoàn thành các tương tác 'từ xa' giữa các bên một cách tin cậy.Để giải quyết vấn đề này, Chỉ thị của Nghị viện và Hội đồng Châu Âu về Chữ ký điện tử (European Parliament and Council Directive on Electronic Signatures -1999/93 / EC) đã được ban hành vào ngày 13 tháng 12 năm 1999.Trong ngữ cảnh của Chỉ thị EU 1999, quy định hiện tại tập trung vào chữ ký điện tử được tạo bằng một phương tiện mã hóa trong một "thiết bị tạo chữ ký an toàn".

***- Tiêu chuẩn chữ ký số trên thiết bị di động:***

Vào tháng 6 năm 2003, các điều khoản bảo mật cho các hệ thống tạo và xác minh chữ ký là các bên muốn cung cấp chữ ký yêu cầu thiết bị “đặc biệt”. Thông thường, điều này liên quan đến thẻ thông minh (smart card) và đầu đọc thẻ có đủ khả năng xử lý và khả năng hiển thị để trình bày chi tiết đầy đủ về giao dịch sẽ được "ký". Ủy ban Châu Âu đã phân bổ ngân sách cho ETSI để thành lập Nhóm chuyên trách Specialist Task Force (STF-221) để xây dựng một bộ tiêu chuẩn cho dịch vụ chữ ký di động.Nhóm này đã tham gia hỗ trợ công việc đã được thực hiện bởi một nhóm khác của ETSI, ETSI Project M-Commerce (EP M-Comm) từ cuối năm 2000.Nhiệm vụ của EP M-COMM là phân tích nhu cầu kinh doanh của người dùng, các nhà cung cấp nội dung, các ngân hàng và các tổ chức thanh toán để bảo mật hệ thống di động. Nó cũng hợp tác chặt chẽ với các cơ quan khác như Hiệp hội di động toàn cầu (GSM), Liên minh di động mở (OMA) và Radicchio…

Đến tháng 7/2013, Dự án EP- M-Comm kết thúc, kết quả Nhóm đã hoàn thành 04 tiêu chuẩn dạng báo cáo (TR) và thông số kỹ thuật (TS) cho dịch vụ chữ ký di động, bao gồm:

* **TR 102 203**: Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements.
* **TS 102 204**: Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface
* **TR 102 206**: Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework.
* **TS 102 207**: Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services

Bộcác tiêu chuẩn TR và TS trên cho phép thiết kế và triển khai giải pháp chữ ký điện tử di động có thể tương tác với nhau, được chấp nhận, sử dụng rộng rãi tại Châu Âu và các nước khác.

* ***Tiêu chuẩn chữ ký số trên nền tảng điện toán đám mây:***

Tháng 4/2019, Ủy ban kỹ thuật về Cơ sở hạ tầng chữ ký điện tử (TC ESI) của ETSIban hành một bộ 3tiêu chuẩn kỹ thuật cho chữ ký số trên nền tảng điện toán đám mây (cloud-based) để hỗ trợ triển khai dịch vụ chứng thực chữ ký số trên các thiết bị di động, bao gồm các tiêu chuẩn:

* **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
* **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
* **ETSI TS 119 432**:Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation

Bộ tiêu chuẩn mới này tạo điều kiện để triển khai dịch vụ chứng thực chữ ký số trên Cloud, trong đó người dùng không phụ thuộc vào các phần mềm chuyên dụng hoặc thiết bị mã hóa (token).Người ký ủy quyền cho bên thứ ba để quản lý khóa ký và ký điện tử các tài liệu dưới sự kiểm soát của họ. Để đảm bảo rằng môi trường tạo chữ ký dựa trên đám mây là đáng tin cậy và khóa bí mậtchỉ được sử dụngdưới sự kiểm soát của người ký, tổ chức cung cấp dịch vụ chữ ký số phải áp dụng các quy trình quản lý và bảo mật quản trị cụ thể và sử dụng các hệ thống, thiết bị mã hóa đáng tin cậy, bao gồm cả các kênh truyền thông điện tử an toàn.

### 2.2.2. Hiện trạng xây dựng tiêu chuẩn Mobile PKI của Mỹ

Ngày 30/12/2014, Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) ban hành tài liệu hướng dẫn:**NIST SP PUB 800-157 Guideline for Derived PIV Credential**.Hướng dẫn này cung cấp các tiêu chuẩn kỹ thuật cho một hệ thống mà các thiết bị di động như điện thoại thông minh, máy tính bảng được cung cấp các thẻ PIV (PIV credential: thẻ xác minh danh tính cá nhân, được Chính phủ liên bang Hoa Kỳ sử dụng để truy cập các cơ sở và hệ thống thông tin do Liên bang kiểm soát ở cấp độ bảo mật thích hợp), cho phép thiết bị di động thay thế thẻ thông minh (Smard card) để xác thực từ xa cho các hệ thống CNTT Liên bang. Tài liệu này cũng mô tả cách người dùng có thẻ PIV hợp lệ có thể nhận được mã thông báo PIV được tích hợp, có nguồn gốc với thông tin liên quan bằng cách sử dụng các mô-đun mã hóa phần cứng hoặc phần mềm. Cách tiếp cận này nhằm đáp ứng với thông tin xác thực thiết bị di động được nêu trong Tiêu chuẩn xử lý thông tin liên bang (Trin) 201-2, Xác minh danh tính cá nhân (PIV) của nhân viên và nhà thầu liên bang, được công bố vào tháng 8 năm 2013.

NIST (SP) 800-157 không đề cập đến việc sử dụng PIV card với thiết bị di động, mà thay vào đó cung cấp một giải pháp thay thế cho PIV card, trong trường hợp sử dụng PIV là không thực tế. Thay vì PIV card, SP 800-157 cung cấp token thay thế, có thể được triển khai và triển khai trực tiếp với các thiết bị di động (như điện thoại thông minh và máy tính bảng). PIV credential được liên kết với Token thay thế này được gọi là **Derived PIV Credential**.

Nội dung của NIST SP 800-157 gồm có quy định các tiêu chuẩn về chính sách chứng thư (CP), thiết bị mã hóa -cryptographic token(loại token như Bluetooth smart card, SIM, Microsoft , thông số của token…); chữ ký số và quản lý khóa…Dựa trên NIST SP 800-157, đến thời điểm hiện tại, chính phủ Hoa Kỳ sử dụng Bluetooth smart card là phương thức chủ yếu để ký số trên các thiết bị di động.

# III. ĐỀ XUẤT DANH MỤC TIÊU CHUẨN CHỮ KÝ SỐ VÀ DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

## Tiêu chuẩn chữ ký số và dịch vụ chứng thực chữ ký số trên thiết bị di động bao gồm:

-***Các tiêu chuẩn về chữ ký số và dịch vụ chứng thực chữ ký số:***đây là các tiêu chuẩn áp dụng chung để cung cấp dịch vụ chứng thực chữ ký số (tiêu chuẩn mật mã và chữ ký số; tiêu chuẩn thông tin, dữ liệu;tiêu chuẩn chính sách và quy chế chứng thực chữ ký số, tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số; tiêu chuẩn kiểm tra trạng thái chứng thư số).

- ***Các tiêu chuẩn cho hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số di động (SIM PKI):*** đây là các tiêu chuẩn cho phần thiết bị cung cấp chức năng lưu trữ khóa bí mật, chứng thư số, chức năng tạo chữ ký số sử dụng SIM điện thoại của nhà mạng di động theo mô hình SIM PKI.

***- Các tiêu chuẩn cho 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):*** đây là các tiêu chuẩn cho phần thiết bị cung cấp chức năng lưu trữ khóa bí mật, chứng thư số, chức năng tạochữ ký số trên máy chủ kýsố (mô hình cloud-based hay remote signing).

## 1. Các tiêu chuẩn về chữ ký số và dịch vụ chứng thực

- Tiêu chuẩn thuật toán tạo chữ ký số:

Để ứng dụng hạ tầng PKI cho thiết bị di động, cần đáp ứng một số yêu cầu sau: Tối ưu thuật toán ký số; tối ưu kích thước dữ liệu (tối ưu các trường dữ liệu trong chứng thư số) được lưu trên thiết bị di động và dữ liệu được truyền trên mạng di động; tối ưu hóa giao thức quản lý chứng thư số; tối ưu lược đồ kiểm tra chứng thư số.

Với dịch vụ chứng thực chữ ký số, việc tính toán tạo cặp khóa công khai - bí mật, ký số và xác thực chữ ký số trên thiết bị di động là không thể thiếu.Thuật toán mã hóa khóa công khai dựa vào thuật toán RSA được lựa chọn cho thuật toán ký số của PKI. Tuy nhiên, việc tạo cặp khóa dựa trên thuật toán RSA trên thiết bị di động tốn nhiều thời gian hoặc không thể xảy ra do thiếu bộ nhớ và hiệu suất CPU nhỏ. Do đó, cần có một thuật toán phù hợp để tính toán tạo ra cặp khóa sử dụng cho thiết bị di động.

Đề xuất bổ sung thuật toán ECDSA: Thuật toán tạo chữ ký số này có ưu điểm là kích thước khóa nhỏ dựa vào độ khó của bài toán logarit rời rạc trên đường cong elliptic (ECDLP). Nó cần ít thời gian để tạo cặp khóa công khai trong thiết bị di động hơn thuật toán RSA. Vì kích thước khóa ECDSA 256 bit, nhỏ hơn RSA 2048-bit nên kích thước chứng thư số cũng giảm. So với RSA, việc triển khai ECDSA có những hiệu quả sau: tăng tốc độ, yêu cầu khả năng tính toán thấp hơn, tiết kiệm bộ nhớ, tiết kiệm băng thông đường truyền, tăng hiệu quả lưu trữ, tiết kiệm năng lượng. Như vậy, với ECDSA, độ dài khóa là 256-bit, tương đương với RSA độ dài 2048-bit, tốn ít thời gian hơn để sinh ra cặp khóa công khai trên thiết bị di động so với sử dụng RSA. Hơn nữa, với việc sử dụng khóa ECDSA 256-bit, kích cỡ của chứng thư số cũng được giảm đi.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Số TT | Loại  tiêu chuẩn | Ký hiệu  tiêu chuẩn | Tên đầy đủ  của tiêu chuẩn | Quy định  áp dụng |
| **Bổ sung tiêu chuẩn về thuật toán tạo chữ ký số** | | | | |
| 1.1 | Mật mã phi đối xứng và chữ ký số | PKCS #1 | RSA Cryptography Standard | - Áp dụng một rong 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 bits |
| ANSI X9.62-2005 | Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) |

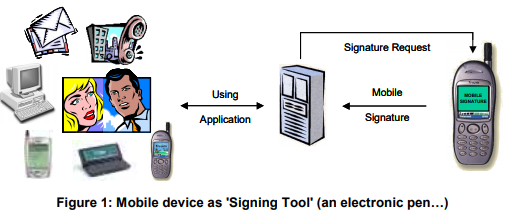
- Tiêu chuẩn khác: Ngoài việc bổ sung tiêu chuẩn về thuật toán tạo chữ ký số ký ECDSA, hệ thống thiết bị cung cấp dịch vụ của tổ chức chứng thực chữ ký số trên thiết bị di động cũng cần đáp ứng các tiêu chuẩn chung được quy định tại **Thông tư số 06/2015/TT-BTTTT** quy định Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

**2. Các tiêu chuẩn cho hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số di động (SIM PKI)**

### 2.1. Tổng quan về mô hìnhSIM PKI

### 2.1.1. Mô hình tổng quan

Chữ ký trên di động có thể được sử dụng trên tất cả các ứng dụng chứ không chỉ dành riêng cho các ứng dụng chạy trên thiết bị di động.Thiết bị di động có thể coi là một công cụ ký - tương đương với một cây bút điện tử dùng để ký số.Việc ký số từ yêu cầu của 1 ứng dụng qua mạng di động và các kênh điện tử tương đương trên di động sẽ cần có sự cho phép của công dân.



1. **Thiết bị di động trở thành công cụ ký số**

Trong triển khai dựa trên SIM PKI, việc tạo chữ ký đạt được bằng cách sử dụng bộ xử lý mã hóa trên thẻ SIM.



1. **Xử lý mã hóa ký số trên thẻ SIM trong SIM PKI**

Yêu cầu ký số nhận được tại thiết bị di động của công dân kích hoạt ứng dụng "ký" trên thẻ SIM.Điều này cho phép hiển thị văn bản giao dịch trên màn hình thiết bị di động và cung cấp tùy chọn cho công dân nhập mã PIN ký tên của mình.Hành động nhập mã PIN ký chính xác sẽ bắt đầu tạo chữ ký di động trong thẻ SIM và truyền chữ ký đến dịch vụ chữ ký di động.Bằng cách nhập mã PIN ký chính xác, công dân được coi là đã xác nhận ý định của mình để tiến hành các chi tiết giao dịch được hiển thị trên màn hình thiết bị di động của họ.



1. **Mô hình tổng quan giải pháp SIM PKI**

Các thành phần chính gồm:

- MSSP: Nhà cung cấp dịch vụ chữ ký di động.

- AP: Nhà cung cấp ứng dụng.

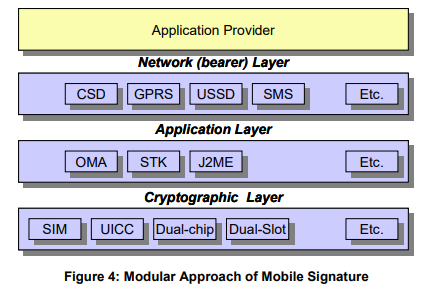
- RA: Nhà cung cấp dịch vụ đăng ký sử dụng.

- CA: Nhà cung cấp dịch vụ chứng chữ ký số.

- SIM CA: Thiết bị thẻ thông minh trong thiết bị di động.

- MNO: Nhà mạng di động.

Kiến trúc giữa Nhà mạng di động và thiết bị SIM CA có thể được module/lớp hóa và lựa chọn các công nghệ khác nhau gồm:



1. **Kiến trúc lớp giữa nhà mạng di động và thiết bị SIM CA**

* Lớp mạng: Giao thức/tiêu chuẩn tương tác giữa nhà mạng di động và thiết bị SIM CA. Có thể lựa chọn các công nghệ khác nhau nhưng thường sử dụng SMS.
* Lớp ứng dụng: ứng dụng ký trên thiết bị SIM CA. Có thể lựa chọn các công nghệ khác nhau nhưng thường sử dụng STK và J2ME.
* Lớp mật mã: chính là thiết bị thẻ thông minh có bộ phần cứng hỗ trợ mã hóa khóa công khai – SIM CA.

Tại lớp mạng cần có phương án bảo mật đường truyền cho các dữ liệu giữa nhà mạng di động và thiết bị SIM CA.

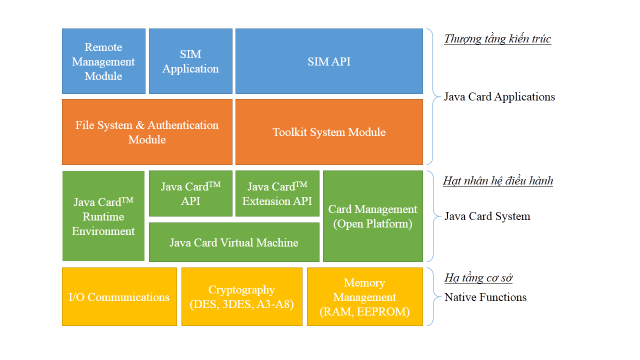
Giải pháp sử dụng SMS để giao tiếp giữa MSSP với SIM CA thông qua nhà mạng di động:

* Quá trình truyền nhận SMS qua SMSC được tuân theo chuẩn mã hóa tin nhắn GSM 03.48 (tin nhắn thông thường dạng văn bản, tuân theo chuẩn GSM 03.40);
* Dữ liệu truyền nhận giữa SIM – MSSP thông qua nhà mạng di động được mã khóa bằng thuật toán.

### 2.1.2. Thành phần chính

Hệ thống bao gồm các thành phần chính như sau:

**a)Thẻ SIM – Thiết bị tạo chữ ký di động (Mobile SCD)**



1. **Kiến trúc tổng thể hệ điều hành PKI SIM**

PKI SIM sử dụng hệ điều hành với kiến trúc 3 lớp:

+ Hạt nhân hệ điều hành: xây dựng theo Java Framework.

+ Hạ tầng cơ sở: phát triển hoàn toàn độc lập, hỗ trợ các thuật toán 3DES, AES và RSA sử dụng cho thượng tầng kiến trúc, và sẵn sàng sử dụng được mọi loại chip trên thế giới và cả Việt Nam trong tương lai.

+ Thượng tầng kiến trúc: phát triển mở sẵn sàng cho các loại ứng dụng thẻ thông minh trên lĩnh vực chữ ký số.

SIM PKI phát triển sử dụng thư viện RSA cứng hóa bên trong chip đã được cấp chứng chỉ CC EAL5+ như chip của Infineon, SAM SUNG, … PKI SIM Applet dựa trên thuật toán mã hóa RSA với cặp khóa công khai và bí mật sử dụng mã hóa, giải mã, ký điện tử và xác thực ngay bên trong chip với khóa bí mật chỉ được lưu trữ bên trong chip như hộp đen tuyệt đối. PKI SIM Applet với thẻ SIM để tạo ra PKI SIM sử dụng với Handset hoặc USB 3G/4G…

SIM PKI sử dụng Applet gồm 5 module:

+ Module sinh khóa: cặp khóa bí mật và khóa công khai được sinh ngay trong thẻ.

+ Module lưu khóa: lưu trữ khóa bí mật bên trong thẻ để giải mã hoặc ký điện tử.

+ Module mã hóa và giải mã: mã hóa bằng khóa công khai và giải mã bằng khóa bí mật.

+ Module ký điện tử: ký chuỗi dữ liệu thành một đoạn dữ liệu gửi kèm cùng với thông tin.

+ Module xác thực: xác thực chữ ký và dữ liệu được truyền vào

**b) Nhà cung cấp ứng dụng (AP)**

Nhà cung cấp ứng dụng chịu trách nhiệm bảo đảm ứng dụng phải an toàn và tin cậy để thúc đẩy việc sử dụng chữ ký điện tử. AP đảm bảo rằng dữ liệu cần ký phải chính xác theo yêu cầu từ người sử dụng. Các biện pháp bảo mật đảm bảo gồm:

- Giao tiếp MSSP với các AP của các đối tác và hệ thống nghiệp vụ của nhà cung cấp dịch vụ khác được bảo mật bởi giao thức https với tính năng SSL mã hóa 2 chiều;

- Mỗi AP được cấp một mã định danh người sử dụng và chứng thư số để mã hóa dữ liệu giao tiếp với MSSP. Giao tiếp giữa AP và MSSP được xác thực mạnh dựa trên chứng thư số. AP muốn sử dụng dịch vụ phải ký số lên yêu cầu trước khi gửi sang MSSP. Khi nhận được yêu cầu từ AP, MSSP thực hiện xác thực chữ ký để xác định AP. Nếu chữ ký hợp lệ, MSSP sẽ xử lý yêu cầu và trả về kết quả cho AP. Ngược lại, MSSP sẽ bỏ qua yêu cầu của AP.

**c) Hệ thống cung cấp dịch vụ ký (MSSP)**

MSSP là hệ thống là trung tâm của giải pháp, thực hiện các chức năng chính sau:

- Quản lý và cấp phép truy cập cho các hệ thống nghiệp vụ của các nhà cung cấp dịch vụ được kết nối và thực hiện các yêu cầu nghiệp vụ;

- Trung tâm chung chuyển yêu cầu cấp pháp chứng thư số với hệ thống RA, yêu cầu ký điện tử giữa AP, hạ tầng mạng với điện thoại người dùng và chứng thực chữ ký số với hệ thống CORE-CA của CA công cộng.

- MSSP giúp đảm bảo rằng “những gì người sử dụng nhìn thấy là những gì họ ký” và bảo mật của hệ thống đối với khách hàng, đối tác; ngăn ngừa, phát hiện truy nhập trái phép vào cơ sở dữ liệu cũng như xử lý, theo dõi các điểm yếu dễ bị tấn công;

- Ghi lịch sử giao dịch, lưu và báo cáo các thông tin về truy nhập hệ thống để phục vụ kiểm tra, giám sát hệ thống.

### 2.1.4. Hoạt động

**a) Kích hoạt dịch vụ**

Quy trình nghiệp vụ này mô tả các bước thực hiện trên hệ thống khi người sử dụng vừa mới lắp SIM PKI vào thiết bị di động để sử dụng dịch vụ.

Điều kiện: SIM mới chưa kích hoạt dịch vụ. Tham gia vào quy trình có các tác nhân: Người dùng, SIM, MSSP.



1. **Quy trình nghiệp vụ đăng ký dịch vụ**

Chi tiết luồng quy trình nghiệp vụ:

(1) Khi người dùng lắp SIM vào thiết bị di động, SIM tự động gửi thông tin kích hoạt dịch vụ - khóa ZMK, ICCID lên MSSP.

(2) MSSP lưu lại thông tin kích hoạt của SIM.

(3) MSSP gửi kết quả kích hoạt.

(4) SIM hiển thị thông báo kích hoạt dịch vụ thành công cho NSD.

(5) Sau khi đã kích hoạt dịch vụ thành công, mọi dữ liệu trao đổi giữa SIM và MSSP được mã hóa và giải mã sử dụng khóa ZMK theo phương thức mã hóa 3DES.

**b) Đăng ký cấp mới CTS**

Quy trình nghiệp vụ này mô tả các bước thực hiện trên hệ thống khi khách hàng đăng ký cấp mới chứng thư số.

Hình 7. Quy trình nghiệp vụ đăng ký mới chứng thư số

Chi tiết luồng quy trình nghiệp vụ:

(1) NSD làm thủ tục đăng ký sử dụng dịch vụ chữ ký số tại RA

(2) Nhân viên RA thông qua giao diện phần mềm điền đầy đủ thông tin của người muốn đăng kí. Sau đó, nhân viên có thẩm quyền kiểm tra xác thực thông tin người dùng tương ứng với hồ sơ đi kèm (để đảm bảo chính xác thông tin).Nếu thông tin là chính xác, nhân viên này thực hiện phê duyệt yêu cầu.

(3) Sau khi yêu cầu được phê duyệt, nhân viên đấu nối qua giao diện phần mềm thực hiện gửi yêu cầu tới MSSP để yêu cầu tạo mới CTS.

(4) MSSP phản hồi ngay cho RA thông báo đã nhận dữ liệu, yêu cầu chờ xử lý.

(5) MSSP căn cứ vào yêu cầu gửi từ RA thực hiện đóng gói SMS để gửi xuống SIM.

(6) MSSP gửi SMS cho SIM qua SMSC bằng định dạng SMS để SIM thực hiện sinh cặp khóa.

(7) Nhận được lệnh yêu cầu của MSSP, SIM thực hiện sinh cặp khóa.

(8) Sau khi sinh cặp khóa, SIM đóng gói tin nhắn chứa CSR gửi lên MSSP.

(9) MSSP kiểm tra CSR từ SIM gửi lên, nếu chính xác, MSSP lưu lại CSR.

(10) RA gửi yêu cầu truy vấn kết quả CSR định kỳ.

(11) MSSP gửi thông tin CSR cho RA thông qua webservice.

(12) RA dựa trên thông tin người dùng trong CSR nhận được từ MSSP, tương tác với Core CA để sinh ra chứng thư số.

(13) RA gửi chứng thư số về cho MSSP thông qua webservice.

(14) Máy chủ MSSP lưu lại thông tin chứng thư số.

(15) Máy chủ MSSP trích xuất các thông tin từ chứng thư, sau đó đóng gói tin nhắn gửi xuống SIM.

(16) SIM lưu lại các thông tin về chứng thư số.

(17) SIM gửi thông báo kết quả lưu chứng thư thành công lên MSSP.

(18) Căn cứ vào kết quả lưu chứng thư, MSSP gửi phản hồi lại thông báo cho RA.

(19) Căn cứ vào kết quả lưu thông tin CTS từ SIM phản hồi lên, MSSP thông báo kết quả đăng kí CTS vào inbox cho người dùng.

**c) Nghiệp vụ ký số**

Quy trình nghiệp vụ này mô tả các bước thực hiện trên hệ thống khi người sử dụng muốn ký điện tử sử dụng chứng thư số trên SIM PKI.

Điều kiện: Người dùng sử dụng SIM PKI đã đấu nối chứng thư số, chứng thư số đang hoạt động. Người sử dụng đăng ký dịch vụ chữ ký số di động với nhà cung cấp dịch vụ AP, đồng thời các AP đăng ký kết nối với dịch vụ chữ ký số của CA

Tham gia vào quy trình có các tác nhân: Người dùng, SIM PKI, AP, MSSP.

Hình 8. Quy trình nghiệp vụ ký điện tử

Chi tiết luồng quy trình nghiệp vụ:

(1) NSD dùng dịch vụ của nhà cung cấp dịch vụ thông qua giao diện người sử dụng của nhà cung cấp như website trực tuyến, ví dụ giao dịch chuyển khoản bằng Internet banking, hoặc mua hàng qua mạng... Nhà cung cấp dịch vụ có thể đưa ra lựa chọn trên giao diện để người sử dụng lựa chọn phương pháp ký điện tử trên di động.

(2) Máy chủ cung cấp dịch vụ - AP, kiểm tra NSD có sử dụng chữ ký số hay không thông qua việc khai báo thông tin liên quan đến việc sử dụng chữ ký số hoặc nhà cung cấp dịch vụ liên kết với nhà cung cấp chữ ký số (RA/CA hoặc MSSP) để biết một NSD có dùng chữ ký số trên di động hay không (ví dụ bằng số điện thoại đã khai báo với nhà cung cấp dịch vụ) để quyết định việc gửi yêu cầu ký điện tử tới người sử dụng.

(3) Căn cứ vào loại dữ liệu cần ký, AP có thể chuyển đổi về dữ liệu phù hợp để ký. Đối với các giao dịch điện tử yêu cầu NSD ký trực tiếp vào nội dung thì AP chuyển toàn bộ nội dung sang cho MSSP. Trong trường hợp dữ liệu là dạng văn bản dài hoặc cần ký lên trên file dữ liệu, thì AP cần chuyển đổi thành mã băm – hash, và phần thông tin mô tả để đóng gói ở bước kế tiếp.

(4) Máy chủ cung cấp dịch vụ - AP, chuẩn bị dữ liệu theo định dạng chuẩn để gửi dữ liệu yêu cầu ký tới MSSP.

(5) Dữ liệu cần ký được đóng gói và gửi xuống điện thoại của NSD. Dữ liệu được đảm bảo đường truyền được bảo mật theo chuẩn viễn thông.

(6) Thông tin cần ký hoặc dữ liệu mô tả thông tin cần ký được ứng dụng trên SIM hiển thị tới NSD – Đảm bảo nguyên tắc “Ký trên những gì bạn thấy”. Sau đó, màn hình hiển thị để NSD nhập mã PIN xác nhận việc ký.

(7) Dữ liệu đã ký được đóng gói và gửi trở lại MSSP. Dữ liệu được đảm bảo đường truyền được bảo mật theo chuẩn viễn thông.

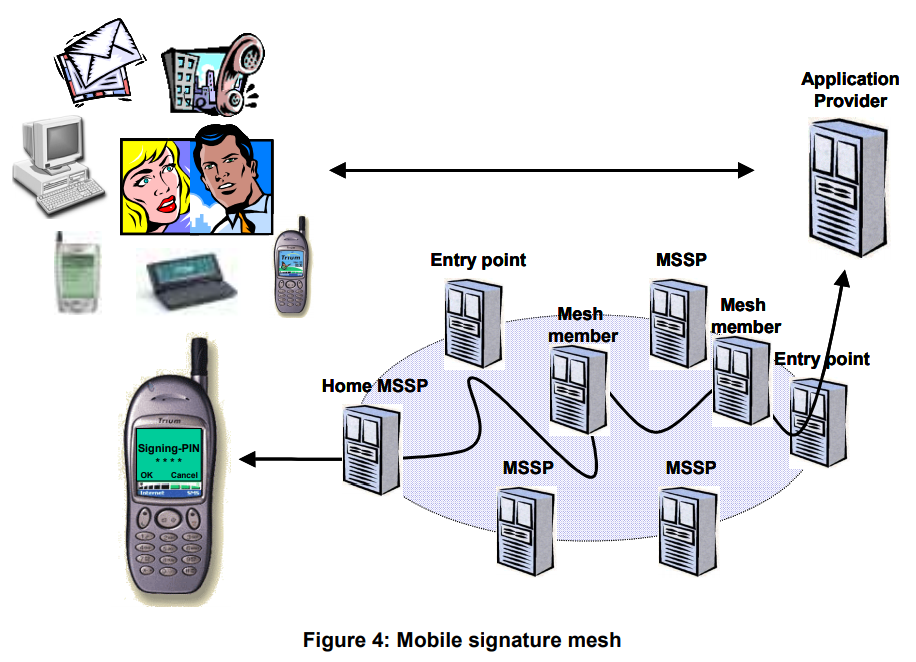
(8) MSSP gửi về AP dữ liệu đã ký.

(9) Trong trường hợp dữ liệu gửi tới MSSP là dạng mã băm – cho dữ liệu dưới dạng file dữ liệu hoặc văn bản dài, thì AP làm nhiệm vụ “dán” chữ ký vào bên trong văn bản.

(10) AP gửi phản hồi xác nhận việc nhận chữ ký thành công.

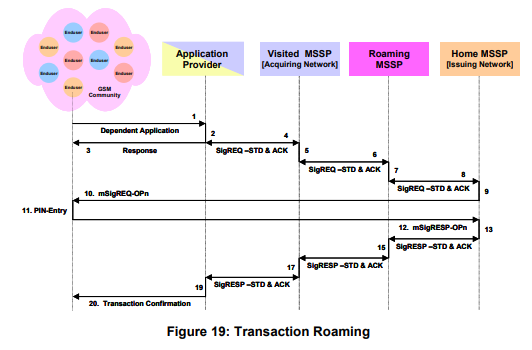
**d) Chuyển vùng trong chữ ký di động**

AP sẽ có thể nhận được yêu cầu ký từ bất kỳ người ký nào, ngay cả khi AP và MSSP không có kết nối với nhau.Do đó ứng dụng AP sẽ phải kết nối với càng nhiều MSSP càng tốt và điều này có thể là một gánh nặng (về chi phí, phát triển, duy trì, nâng cấp hệ thống). Từ đây yêu cầu có một giải pháp được gọi là chuyển vùng chữ ký di động để khi tiếp nhận yêu cầu từ người ký thì AP có thể liên hệ với MSSP phù hợp (MSSP cung cấp dịch vụ cho người ký – Home MSSP).



**Hình 9. Chuyển vùng chữ ký di dộng**

Chuyển vùng chữ ký di động có nhiều giải pháp được cụ thể hoá trong tài liệu ETSI TR 102 207. Dưới đây là một quy trình tổng quát:



**Hình 10. Lược đồ luồng chuyển vùng chữ ký di dộng**

1) Người ký gửi yêu cầu ký.

2) AP xác nhận giao dịch ký.

3) AP thông báo cho người ký để xác nhận giao dịch ký.

4) AP gửi giao dịch ký tới MSSP.

5) MSSP xác định người ký là thuê bao của một MSSP khác.

6) MSSP chuyển tiếp tới Roaming-MSSP (một hệ thống hay giải pháp Roaming).

7) Roaming-MSSP xác định Home MSSP cung cấp dịch vụ cho người ký.

8) Roaming-MSSP chuyển tiếp giao dịch ký đến Home-MSSP.

9) MSSP xử lý giao dịch ký.

10) MSSP chuyển tiếp yêu cầu ký đến thiết bị di động của người ký.

11) Người ký xem xét thông báo văn bản hiển thị sẽ được ký, nhập mã PIN để xác nhận thì SIM tính toán để tạo ra chữ ký số.

12) Thiết bị di động trả về kết quả ký cho MSSP.

13) MSSP xử lý kết quả ký.

14-18) Luồng trả kết quả chữ ký được truyền trở lại AP.

19) AP xử lý kết quả ký.

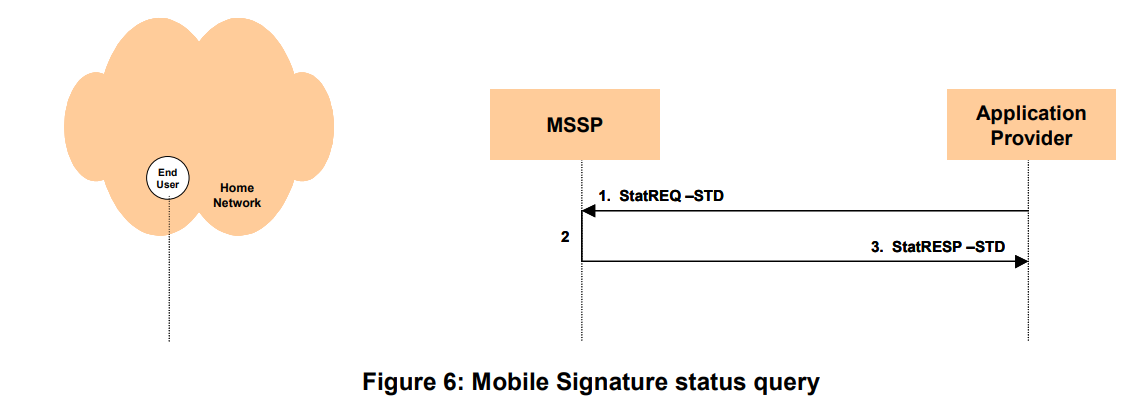
20) AP xác nhận kết quả của quá trình chữ ký di động và trạng thái của giao dịch (ví dụ: đã hoàn thành, không thành công - với mã lý do,...).

*(Theo mục 13.2.3 Transaction Roaming tài liệu ETSI TR 102 203)*

#### e) Các giao dịch khác

###### - Truy vấn trạng thái chữ ký di động (Mobile Signature status query)

Được AP sử dụng để nhận thông tin về giao dịch chữ ký di động.

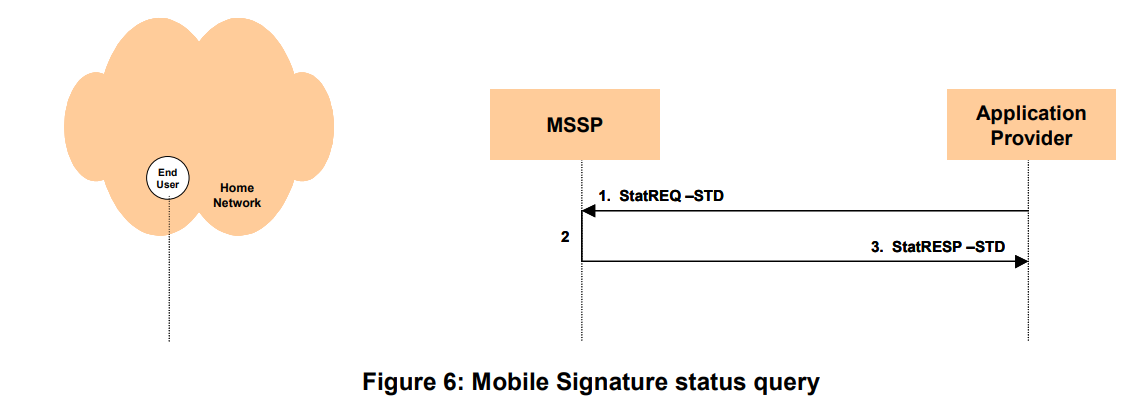


**Hình 11.Lược đồ luồng truy vấn trạng thái chữ ký di động**

*(Theo mục 6.2 Mobile Signature status query tài liệu ETSI TR 102 204)*

###### - Truy vấn hồ sơ chữ ký di động (Mobile Signature profile query)

Được AP sử dụng để nhận thông tin về giao dịch chữ ký di động.

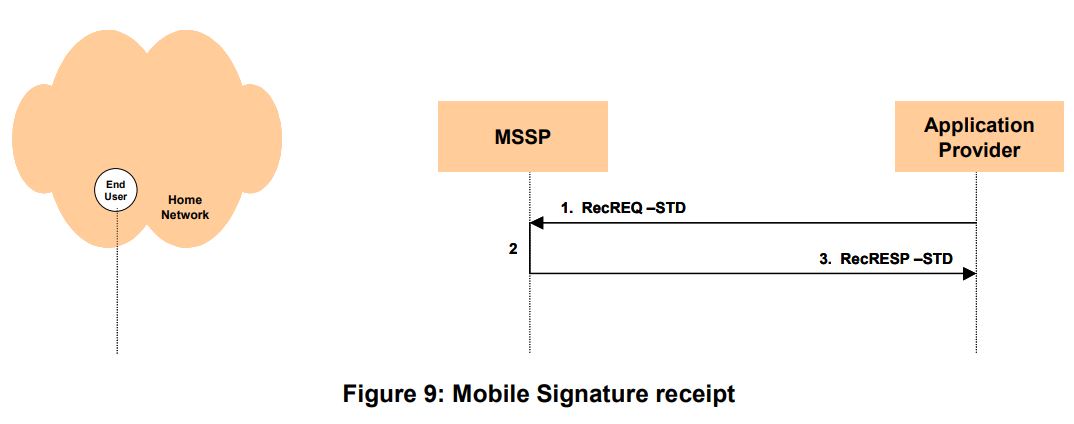


**Hình 12.Lược đồ luồng truy vấn hồ sơ chữ ký di động**

*(Theo mục 6.3 Mobile Signature profile query tài liệu ETSI TR 102 204)*

###### - Biên nhận chữ ký di động (Mobile Signature receipt)

Nhà cung cấp ứng dụng sử dụng phương thức này vào cuối giao dịch để cung cấp enduser với một số loại "biên nhận" thông báo cho enduser về việc tiến hành giao dịch. Điều này tương ứng với gọi một "Phương thức nhận chữ ký di động (Mobile Signature Receipt Method)" . Nội dung của một biên lai là khác nhau theo AP. Mỗi AP có quy tắc riêng để xử lý biên lai. Tuy nhiên, giao diện này cung cấp khả năng cho AP đặt văn bản và / hoặc XML chữ ký (biên nhận được ký điện tử bởi AP) trong RecReq-STD.

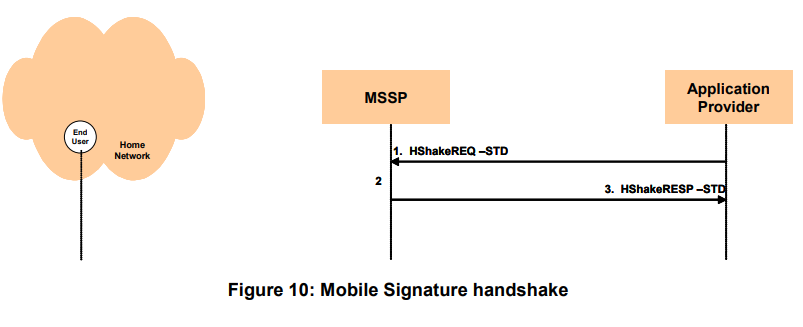


**Hình 13.Lược đồ luồng biên nhận chữ ký di động**

*(Theo mục 6.5 Mobile Signature receipt tài liệu ETSI TR 102 204)*

###### - Bắt tay chữ ký di động (Mobile Signature handshake)

Được cả MSSP và AP sử dụng để đồng ý sử dụng chữ ký XML trong giao tiếp.



**Hình 14.Lược đồ luồng bắt tay chứ ký di động**

*(Theo mục 6.6 Mobile Signature handshake tài liệu ETSI TR 102 204)*

### 2.2. Các đối tượng cần chuẩn hóa

Các đối tượng cần chuẩn hóa bao gồm:

- Thẻ SIM PKI: Khóa bí mật được lưu trên SIM, cần đáp ứng tiêu chuẩn bảo mật về thiết bị lưu trữ.

- Thuật toán ký số: Thuật toán ký số cần được tối ưu tương ứng với hiệu năng của thiết bị di động.

- Giao tiếp giữa MSSP và AP.

- Giao tiếp giữa các MSSP của các CA khác nhau (Roanming).

### 2.3. Kinh nghiệm quốc tế

SIM PKI bắt đầu thử nghiệm đầu tiên tại Vương Quốc Anh với mạng di động Vodafone vào năm 2001. Sau đó đã được áp dụng nhiều nơi tại châu Âu và tiêu chuẩn hóa bởi Viện Tiêu chuẩn Viễn thông châu Âu qua việc ban hành các chuẩn ETSI cho Mobile PKI.Tới nay, khá nhiều nước trên thế giới đã triển khai giải pháp này: Estonia, Phần Lan, Moldova, Nauy, Thụy Sỹ, Iceland, Thổ Nhĩ Kỳ, Orman:

- **Estonia:** Từ năm 2007 danh tính di động trên thẻ SIM có thể ứng dụng sử dụng như chứng minh nhân dân điện tử. Có thể sử dụng ký điện tử và di động xác thực bằng SIM PKI thậm chí sử dụng cho bỏ phiếu điện tử. Sự nhanh chóng hiện đại hóa của chính phủ chính quyền và tư nhân ngành ở Estonia rõ ràng chứng minh những lợi ích của định danh kỹ thuật số an toàn. Tới tháng 9 năm 2014, Mobile ID đã được chấp nhận bởi 90% dịch vụ trực tuyến có sẵn trong đất nước Estonia.

**- Moldova:** Bắt đầu nghiên cứu từ năm 2011, ra mắt dịch vụ chữ ký điện tử SIM PKI từ cuối năm 2012, quá trình đăng ký chỉ mất 15 phút. Các nhà mạng (MNO)đã đầu tư hệ thống và thu phí người dùng.

**- Phần Lan:** Triển khai dịch vụ dưới dạng tiêu chuẩn quốc gia Mobile-ID được hỗ trợ bởi ba nhà khai thác năm 2010 rất nhanh chóng. Để mua một Thẻ SIM từ nhà mạng rất đơn giản chỉ cần: gặp mặt trước tiếp và có thể đăng ký trực tuyến trước. Mobile-ID với SIM PKI là phương pháp của xác thực phát triển nhanh.Tới 2014 có50.000 điện thoại di động lắp SIM PKI thường xuyên hoạt động.

**- UAE:** Mobile-ID được thử nghiệm trong năm 2014.

- **Iceland:**Mạng SIM PKI triển khai năm 2008. Năm 2014, triển khai Mobile-ID quốc gia với sự giúp đỡ của các ngân hàng.

### 2.4. Đề xuất tiêu chuẩn

- Tiêu chuẩn bảo mật cho thẻ SIM: FIPS 140 level 2 hoặc EAL 4+.

- Tiêu chuẩn về cung cấp dịch vụ:Lựa chọn bộ tiêu chuẩn M-COMM do Viện tiêu chuẩn viễn thông Châu Âu (ETSI) ban hành.

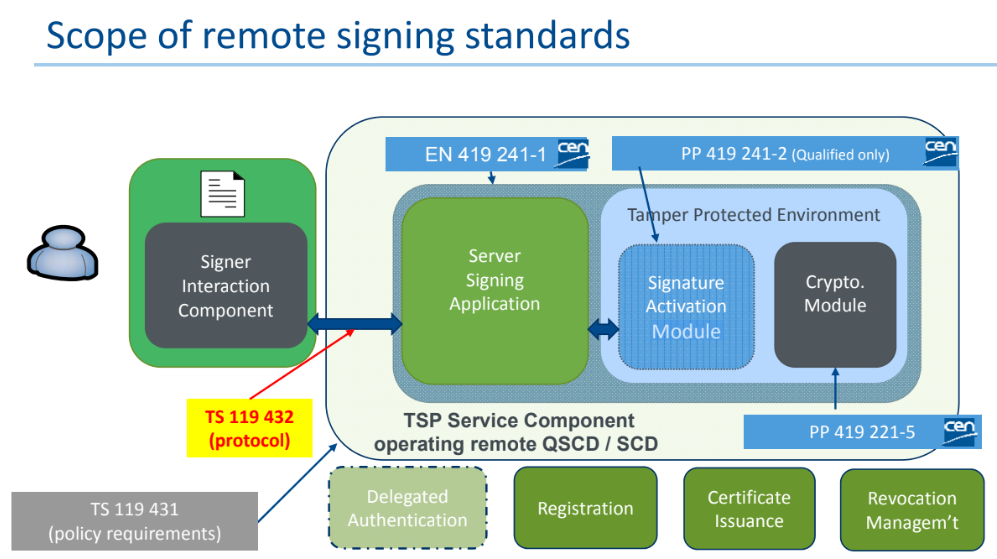
| **Số TT** | **Loại  tiêu chuẩn** | **Ký hiệu  tiêu chuẩn** | **Tên đầy đủ  của tiêu chuẩn** | **Quy định  áp dụng** |
| --- | --- | --- | --- | --- |
| **Tiêu chuẩn cung cấp dịch vụ chứng thực chữ ký số trên mạng viễn thông di động** | | | | |
| 1 | Yêu cầu bảo mật cho thẻ SIM | FIPS PUB 140-2 | Security Requirements for Cryptographic Modules | - Áp dụng một trong hai tiêu chuẩn  - Đối với tiêu chuẩn FIPS PUB : 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 |
| 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 |
| 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 |
| 4 | Khung bảo mật | ETSI TR 102 206 | Mobile Commerce (M-COMM);Mobile Signature Service;Security Framework | Phiên bản V1.1.3 |
| 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 |

**3. Các tiêu chuẩn cho phần 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)**

## 3.1. Tổng quan mô hình ký số từ xa (remote signing)

Chữ ký số dựa trên đám mây (cloud-based digital signature), hoặc “chữ ký từ xa – Remote signature” là một thế hệ chữ ký số mới có thể hoạt động trên các thiết bị máy tính để bàn, thiết bị di động và web - và đáp ứng mức độ tuân thủ và đảm bảo cao nhất cho xác thực người ký. Mỗi người ký được cấp ID số dựa trên chứng thư số cấp bởi các nhà cung cấp dịch vụ tin cậy (TSP). Khi ký số một tài liệu, ID người dùng được sử dụng với mã PIN cá nhân và các bước xác minh khác để chứng minh danh tính của người ký.

## 3.1.1. Mô hình tổng quan



**Hình 15. Mô hình tổng quan Cloud PKI**

## 3.1.2. Thành phần chính

**Nhà cung cấp dịch vụ CA:**

- Cung cấp module Server Signing Application (máy chủ ứng dụng ký số). Module này cần tuân thủ tiêu chuẩn bảo mật EN 419 241-1.

- Cung cấp module Signature Activation Module (SAM) có chức năng điều khiển việc truy cập khóa bí mật người dung. Module này cần tuân thủ tiêu chuẩn 419 241-2.

- Cung cấp Crypto Module. Đây còn gọi là module HSM có chức năng sinh khóa và mã hóa khóa người dùng.Module này cần tuân thủ tiêu chuẩn bảo mật PP (Protection Profile) 419 221 -5.

**Người sử dụng:**

- Đăng ký sử dụng, được cấp chứng thư số cho dịch vụ ký số từ xa.

- Xác thực quyền ký số trên thiết bị di động cá nhân (Signer Interaction Component).

- Thực hiện ký số từ xa theo dịch vụ.

Thông tin trao đổi giữa thiết bị di động cá nhân (Signer Interaction Component) và máy chủ ứng dụng ký số (Server Signing Application) cần tuân theo giao thức TS 119 432.

Quy trình tạo chữ ký đưa ra các kịch bản mà chữ ký số AdES và / hoặc chữ ký số (DSV) được tạo ra bằng cách sử dụng khóa mật mã tạo chữ ký số được lưu giữ quản lý trong một mô-đun mật mã gọi là Thiết bị tạo chữ ký số (SCDev) và được vận hành bởi Nhà cung cấp dịch vụ tạo chữ ký số (SCSP).

Dựa trên phân loại quản lý dữ liệu khác nhau trong các lệnh và phản hồi, hai cấu phần chính trong sơ đồ quy trình trên cung cấp các giao diện khác nhau choquá trình ký số: Thành phần dịch vụ ứng dụng máy chủ ký số (SSASC) và Thành phần dịch vụ ứng dụng tạo chữ ký số (SCASC) được đặc tả sau đây:

***+ SSASC*** là thành phần hỗ trợ tạo chữ ký số (DVS). SSASC có khả năng tương tác với SCDev đang quản lý khóa riêng của người ký. Khi SSASC sử dụng SCDev, người ký có khả năng kiểm soát khóa mật mã tạo chữ ký số với các cấp độ tin cậy xác định.

Đầu vào chính cho giao diện SSASC làĐại diện dữ liệu cần ký số (DTBSR) và các tham số khác hỗ trợ và đầu ra chính là chữ ký số (DVS).

***+ SCASC*** là cấu phần hỗ trợ tạo chữ ký số AdES và thực hiện một số chức năng cụ thể của quy trình tạo chữ ký số. SCASC có khả năng tương tác với SSASC cholệnh tạo chữ ký số (DVS).

Giao tiếp với SCASC là các tài liệu cần được ký số (SD) hoặc đại diện của các tài liệu cần được ký số (SDR) và các tham số khác là đầu vào chính và các tài liệu đã ký số hoặc các chữ ký số(DVS) là đầu ra chính.

SCS chỉ dịch vụ TSP triển khai Ứng dụng Tạo chữ ký số (SCA) và / hoặc ứng dụng máy chủ ký số (SSA).

Một số tùy chọn giao tiếp tùy thuộc vào sự phân chia chức năng giữa SCS và phía hệ thống cục bộ từ người ký.

**3.1.3. Mô tả các tiêu chuẩn**

*Tiêu chuẩn bảo mật 419 241-1*

Tiêu chuẩn bảo mật 419 241-1 định nghĩa một tập hợp các yêu cầu và đề xuất bảo mật để có một hệ thống đáng tin cậy được tạo ra ở phía máy chủ ứng dụng ký số(Trustworthy System Supporting Server Signing (TW4S)).Định nghĩa chi tiết trong tài liệu prEN 419 241-1.

Tài liệu prEN 419 241-1 cung cấp các mô hình chức năng thường được công nhận của TW4S, chỉ định các yêu cầu tổng thể áp dụng trên tất cả các dịch vụ được xác định trong mô hình chức năng, chỉ định các yêu cầu bảo mật cho từng dịch vụ được xác định trong SSA, chỉ định các yêu cầu bảo mật cho các thành phần hệ thống nhạy cảm có thể được SSA sử dụng (ví dụ: Thiết bị tạo chữ ký (SCDev)).

Lưu ý: Các khía cạnh sau đây được coi là ngoài phạm vi của tài liệu prEN 419 241-1: Các dịch vụ đáng tin cậy khác có thể được sử dụng cùng với dịch vụ này như dịch vụxác thực chữ ký, dịch vụ đánh dấu thời gian và dịch vụ bảo quản thông tin, bất kỳ ứng dụng hoặc hệ thống nào bên ngoài SSA, giải thích pháp lý của bất kỳ hình thức chữ ký nào (ví dụ: ý nghĩa của chữ ký, của nhiều chữ ký và chữ ký bao gồm các cấu trúc thông tin phức tạp có chứa các chữ ký khác).

*Tiêu chuẩn bảo mật 419 241-2*

Tiêu chuẩn 419 241-2 đặc tả cấu hình bảo vệ cho Signature Activation Module (SAM), module này có chức năng điều khiển việc truy cập khóa bí mật cho người dùng, nhằmđáp ứng các yêu cầu của QSCD như được chỉ định trong Quy định (EU) số 910/2014[eIDAS] (Định nghĩa chi tiết trong tài liệu prEN 419 241-2:2017 được trình bày bởi Technical Committee CEN/TC 224).

*Tiêu chuẩn bảo mật 119 431*

Tiêu chuẩn ETSI TS 119 431 -1 v1.1.1 chỉ định các yêu cầu về chính sách và bảo mật cho TSP nhằm triển khai hệ thống dịch vụ vận hành tạo chữ ký số từ xa (SCDev).Những yêu cầu này áp dụng cho khi thiết bị là QSCD được quy định trong (EU) No 910/2014. Tiêu chuẩn ETSI EN 319 411-1 phù hợp các yêu cầu chính sách và tài liệu tuyên bố thực hành áp dụng cho các TSPs.

Các yêu cầu về chính sách và bảo mật được xác định theo việc tạo, duy trì, quản lý vòng đời và việc sử dụng key trong tạo chữ ký số.

Tiêu chuẩn này được sử dụng cho các cơ quan độc lập làm cơ sở cho việc đánh giá sự phù hợp của TSP để có thể tin cậy vận hành QSCD/SCDev từ xa.

Tiêu chuẩn không chỉ định giao thức truy cập SSASC.Tiêu chuẩn hiện tại xác định các kiểm soát cụ thể cần thiết để giải quyết các rủi ro liên quan đến các dịch vụ hoạt động từ xa QSCD / SCDev.

Tiêu chuẩn có tham chiếu tới tiêu chuẩn CEN EN 419 214-1 (chỉ định mức độ an toàn cho việc kiểm soát duy nhất). Thuật ngữ “sole control – kiểm soát duy nhất” không có nghĩa chỉ áp dụng cho chữ ký điện tử theo quy định (EU) No 910/2014 được giải thích trong tiêu chuẩn CEN EN 4190241 – 1 điều 5.3. Các yêu cầu này còn có thể áp dụng cho con dấu điện tử.

*Tiêu chuẩn bảo mật 119 432*

Tài liệu ETSI TS 119 432 đặc tả các giao thức và các giao tiếp đối với quy trình tạo chữ ký số chuẩn AdES (Được định nghĩa trong tài liệu ETSI TS 119 102-1 [i.7]) và / hoặc chữ ký số DSV (Digital Signature Value) là kết quả của Đại diện cho tài liệu cần ký số DTBSR (Data To Be Signed Representation). Được thực hiện trên máy chủ dịch vụ ký số đặt từ xa, sử dụng giải pháp phân tán Cloud PKI bao gồm hai hoặc nhiều hệ thống / dịch vụ / thành phần.

Đặc tả kỹ thuật của tiêu chuẩn ETSI TS 119 432 chỉ giới hạn ở việc ký số tạo chữ ký số trên máy chủ đặt từ xa, tức là khóa mật mã để ký được lưu giữ quản lý từ một hệ thống dịch vụ chia sẻ ở xa người ký.

LƯU Ý: Việc ký số từ xa nhưng quá trình tạo chữ ký số được thực hiện bởi trạm đầu cuối (thiết bị cá nhân của người ký), như là khóa mật mã để ký được lưu giữ quản lý ở tại thiết bị đầu cuối của người ký còn các bước thực hiện thủ tục ký số được thực hiện từ các dịch vụ trên mạng Internet không thuộc phạm vi tài liệu này.

Tài liệu ETSI TS 119 432 đặc tả các giao thức với hai định dạng: XML và JSON.

Giao thức cho phép yêu cầu tạo và trả về kết quả cho các định dạng chữ ký số AdES sau đây:

* Dạng Digital Signature Values (General)
* Dạng CadES (CMS)
* Dạng PadES (PDF)
* Dạng XadES (XML)

Giao thức hỗ trợ cả hai phương thức đồng bộ và dị bộ cho quản lý các yêu cầu và phản hồi.

Giao thức hỗ trợ tạo ra chữ ký số đính kèm và không đính kèm nội dung.

Các giao thức trong tài liệu này sử dụng lại hệ thống cấu trúc theo những đặc tả XML CSC JSON và OASIS DSS-X. Những trường hợp không thể sử dụng lại, tài liệu này xây dựng thêm đặc tả ngữ nghĩa và cú pháp theo hai định dạng: XML và JSON. Cho các thành phần mới.

Việc xác thực quyền sử dụng khóa mật mã tạo chữ ký số của người ký yêu cầu cơ chế kiểm tra nhiều lớp để đảm bảo sự kiểm soát người ký hợp lệ. Cách thức quy trình xác thực người ký được thực hiện bởi nhà cung cấp dịch vụ bằng các cơ chế xác thực đa nhân tố không thuộc phạm vi tài liệu này

*Tiêu chuẩn bảo mật 419 221-5*

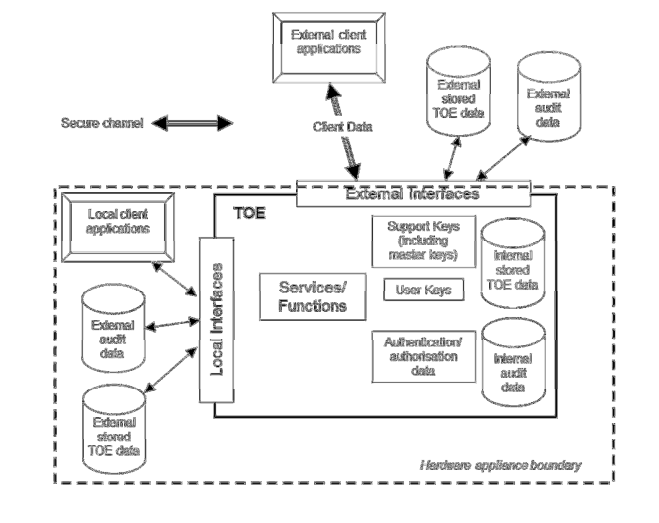
Đây là tiêu chuẩn bảo mật áp dụng cho mô đun mật mã HSM.

Protection Profile (PP) - Hồ sơ bảo vệ, xác định yêu cầu bảo mật cho các mô-đun mật mã sử dụng bởi nhà cung cấp dịch vụ tin cậy, hỗ trợ ký điện tử và dịch vụ xác thực. Nó bao gồm hỗ trợ tùy chọn để sao lưu khóa được bảo vệ.

Protection Profile hỗ trợ các nhà cung cấp dịch vụ tin cậy được xác định theo quy định đề xuất của Nghị viện Châu Âu và của Hội đồng về nhận dạng điện tử và dịch vụ tin cậy cho các giao dịch điện tử trên thị trường nội bộ châu Âu (eIDAS).

TOE (Target of Evaluation) là mô đun bảo mật, tạo và/hoặc bảo vệ khóa bí mật cũng như các dữ liệu nhạy cảm khác và cho phép việc kiểm soát các dữ liệu hoặc các service mật mã được hỗ trợ bởi nhà cung cấp d.vụ.

Có thể xem kiến trúc của TOE là định hướng chung mà các nhà sản xuất HSM phải tuân thủ để đạt chứng nhận PP-5.TOE là một tập các phần mềm và phần cứng được cấu hình. Kiến trúc TOE chung được hiển thị trong sơ đồ:



## Hình 16. Kiến trúc TOE của HSM

## 3.1.4. Hoạt động

**a) Quy trình sinh khóa:**

- Người dùng xác thực quyền trên ứng dụng của thiết bị di động cá nhân

- Ứng dụng trên thiết bị di động cá nhân gửi thông tin và yêu cầu sinh khóa về server

- Server tiếp nhận và sử dụng thông tin, sinh cặp khóa tại HSM và chia sẻ với ứng dụngtrên thiết bị di động cá nhân.

- Hệ thống đồng bộ thông tin, xác nhận sinh khóa thành công, lưu trữ thông tin người dùngvào CSDL và công bố chính thức cặp khóa

- Sử dụng cặp khóa đã được hệ thống công bố để tạo request và cấp chứng thư số

**b)Quy trình ký số:**

- Người dùng gửi yêu cầu ký số dữ liệu về hệ thống

- Hệ thống xử lý yêu cầu và bắt buộc người dùng xác thực quyền qua ứng dụng trên thiết bịdi động cá nhân

- Hệ thống kiểm tra tính hợp lệ và thực hiện ký số đối với dữ liệu của người dùng

- Hệ thống trả về dữ liệu đã được ký số, thông báo đến người dùng ký số thành công.

Bảng dưới đây so sánh tất cả các quy trình hoạt động của CA theo mô hình chữ ký số truyền thống và mô hình chữ ký số sử dụng máy chủ ký (remote signing):

|  |  |
| --- | --- |
| **Quy trình hoạt động của CA mô hình chữ ký số truyền thống** | **Quy trình hoạt động của CA mô hình máy chủ ký (remote signing)** |
| - Máy chủ cấp và quản lý CTS: sử dụng tất cả các hệ thống (Microsoft CA, EJBCA…) | - Máy chủ cấp và quản lý CTS: sử dụng tất cả các hệ thống (Microsoft CA,EJBCA…) |
| - Lưu trữ khóa riêng của CA trên tất cả các loại HSM (Utimaco, nCipher, SafeNet…) | - Lưu trữ khóa riêng của CA trên tất cả các loại HSM (Utimaco, nCipher, SafeNet…) |
| - Cơ chế sinh khóa đơn trên thiết bị lưu trữ khóa người dùng (token, smartcard, sim…) | - Cơ chế sinh khóa phức trên HSM (server) và xác thực từ thiết bị di động cá nhân (client), có sự liên kết logic chặt chẽ giữa các thành phần của khóa) |
| - Công bố chứng thư sử dụng LDAP, AD | - Công bố chứng thư sử dụng LDAP, AD |
| - Ký số và xác thực theo mô hình khóa đơn | - Ký số và xác thực theo mô hình ký server, có sự xác thực từ thiết bị di động cá nhân |
| - Chứng thực theo CRL, OCSP | - Chứng thực theo CRL, OCSP |
| - Thu hồi chứng thư theo hệ thống quản lý chứng thư | - Thu hồi chứng thư theo hệ thống quản lý chứng thư |

## 3.2. Các đối tượng cần chuẩn hóa

Các đối tượng cần chuẩn hóa bao gồm:

- Chính sách và yêu cầu an ninh cho Tổ chức cung cấp dịch vụ chứng thực chữ ký số

- Giao thức tạo chữ ký số;

- Module ký số (PP);

- Ứng dụng ký trên server;

- HSM ký số tập trung.

## 3.3. Kinh nghiệm quốc tế

Quy định eIDAS ban hành năm 2014 của EU cho phép chữ ký điện tử được tạo từ xa (remote qualified signature) bằng các khóa bí mật của người dùng, phương thức này còn được gọi là ký số tập trung (Central signing), ký số phía máy chủ (Server signing) hoặc ký sốtrên đám mây (Cloud signing). Chữ ký số tạo ra theo phương thức này được chấp nhận về mặt pháp lý tương đương với chữ viết tay trên toàn EU.

Với những lợi thế của giải pháp ký số từ xa mang lại cho người dùng cuối (cá nhân và doanh nghiệp, tổ chức).quy định của eIDAS đã mở đường cho một loạt các công ty hoạt động trong lĩnh vực chứng thực điện tử (CA, doanh nghiệp cung cấp thiết bị HSM) phát triển và cung cấp các giải pháp chữ ký số từ xa không chỉ trong phạm vi EU mà còn cả các nước khác trên thế giới.

Các hãng nổi tiếng có thể kể đến gồm: Adobe, Docusign (Mỹ), Cryptomathic (Đan Mạch), Ascertia,n-Cipher (Anh), SK solution…

## 3.4. Đề xuất tiêu chuẩn

Đề xuất lựa chọn áp dụng bộ tiêu chuẩn của Châu Âu cho dịch vụ chứng thực chữ ký số trên nền tảng điện toán đám mây

| **Số TT** | **Loại  tiêu chuẩn** | **Ký hiệu  tiêu chuẩn** | **Tên đầy đủ  của tiêu chuẩn** | **Quy định  áp dụng** |
| --- | --- | --- | --- | --- |
| **Tiêu chuẩn cung cấp dịch vụ chứng thực chữ ký số theo mô hình điện toán đám mây** | | | | |
| 1 | Chính sách và yêu cầu an ninh cho Tổ chức cung cấp dịch vụ chứng thực chữ 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 |
| 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 | 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 |
| 3 | Ứng dụng ký trên server | CEN EN 419 241-1 | Security Requirements for Trustworthy Systems Supporting Server Signing; |  |
| 4 | Yêu cầu cho module ký | CEN EN 419 241-2 | Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing | Phiên bản V0.16 |
| 5 | Yêu cầu cho HSM | CEN EN 419 221-5 | Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services | Phiên bản V0.15 |