TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN XXXXX:2026

Xuất bản lần XX

GIAO DỊCH ĐIỆN TỬ – YÊU CẦU VỀ KHUNG BẢO MẬT CHO MÔ HÌNH KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG (MOBILE PKI)

Electronic transactions – Security framework requirements for the digital signing model on mobile devices (Mobile PKI)

DỰ THẢO THẨM ĐỊNH

HÀ NỘI – 2026

Nội dung **Trang**

Lời nói đầu

TCVN XXXXX:2026 do do Trung tâm Chứng thực điện tử Quốc gia đề nghị, biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ tại Việt Nam, chữ ký số ngày càng đóng vai trò thiết yếu trong các giao dịch điện tử của cơ quan nhà nước, tổ chức và cá nhân. Sự phổ biến của thiết bị di động thông minh cùng với nhu cầu ký số mọi lúc, mọi nơi đã thúc đẩy sự hình thành và phát triển của mô hình ký số trên nền tảng di động (Mobile PKI) - một hướng triển khai hạ tầng khóa công khai linh hoạt, tiện lợi và có tiềm năng ứng dụng rộng rãi trong nhiều lĩnh vực.

Tuy nhiên, chính sự linh hoạt của môi trường di động cũng đặt ra những thách thức bảo mật đặc thù mà các mô hình PKI truyền thống trên thiết bị cố định chưa phải đối mặt đầy đủ. Thiết bị di động hoạt động trong các môi trường mạng không đồng nhất, dễ bị mất hoặc đánh cắp vật lý, chịu nhiều rủi ro từ phần mềm độc hại và thường xuyên phụ thuộc vào các nền tảng hệ điều hành, phần cứng của bên thứ ba. Bên cạnh đó, việc lưu trữ và bảo vệ khóa bí mật (private key) của người ký trên thiết bị di động đòi hỏi các cơ chế kỹ thuật nghiêm ngặt nhằm đảm bảo tính toàn vẹn, bí mật và không thể phủ nhận của chữ ký số theo đúng quy định pháp luật.

Thực tiễn triển khai dịch vụ chứng thực chữ ký số công cộng tại Việt Nam trong những năm gần đây cho thấy nhu cầu cấp thiết phải có một khung tiêu chuẩn thống nhất, quy định rõ các yêu cầu kỹ thuật và bảo mật áp dụng cho mô hình Mobile PKI. Việc thiếu vắng một tiêu chuẩn quốc gia về lĩnh vực này dẫn đến tình trạng các nhà cung cấp dịch vụ tin cậy triển khai theo các phương thức khác nhau, tiềm ẩn nguy cơ không tương thích và khó bảo đảm mức độ an toàn đồng đều.

Tiêu chuẩn này được xây dựng trên cơ sở tham chiếu các tiêu chuẩn và khuyến nghị quốc tế có liên quan, bao gồm nhưng không giới hạn ở ETSI TS 102 206. Đồng thời, tiêu chuẩn này được xây dựng có tính đến đặc điểm hạ tầng kỹ thuật, khung pháp lý về chữ ký điện tử và dịch vụ tin cậy tại Việt Nam, đặc biệt là các quy định tại Luật Giao dịch điện tử năm 2023 và Nghị định số 23/2025/NĐ-CP của Chính phủ.

Tiêu chuẩn này dùng cho các tổ chức cung cấp dịch vụ chứng thực chữ ký số, các nhà phát triển ứng dụng ký số trên nền tảng di động, các cơ quan quản lý nhà nước trong lĩnh vực giao dịch điện tử và chữ ký số, cũng như các tổ chức, doanh nghiệp triển khai ứng dụng chữ ký số vào quy trình nghiệp vụ trên thiết bị di động.

Giao dịch điện tử – Yêu cầu về khung bảo mật cho mô hình ký số trên thiết bị di động (Mobile PKI)

Electronic transactions – Security framework requirements for the digital signing model on mobile devices (Mobile PKI)

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu liên quan đến khung bảo mật cho mô hình ký số trên thiết bị di động (Mobile PKI) áp dụng cho tất cả các cơ quan, tổ chức, doanh nghiệp phát triển, ứng dụng dịch vụ theo mô hình ký số trên thiết bị di động (Mobile PKI).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi (nếu có).

- ETSI TR 102 206 V1.1.3 (2003-08): “Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework”.

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1 Thuật ngữ và định nghĩa

3.1.1

Mã hoá không đối xứng (Asymmetric cryptography)

Phương pháp mã hóa sử dụng một cặp khóa có quan hệ toán học với nhau (khóa công khai và khóa bí mật), trong đó dữ liệu được mã hóa bằng khóa này chỉ có thể được giải mã bằng khóa còn lại và không thể suy ra khóa bí mật từ khóa công khai. Theo đó, thực thể thực hiện mã hóa không cần biết khóa được sử dụng để giải mã thông điệp.

3.1.2

Loại cam kết (commitment type)

Thể hiện chính xác ý định của chữ ký điện tử.

3.1.3

Định dạng nội dung (content format)

Thuộc tính chữ ký thể hiện cách mã hóa tài liệu của chủ thể ký.

3.1.4

Chữ ký điện tử (electronic signature)

Chữ ký được tạo lập dưới dạng dữ liệu điện tử gắn liền hoặc kết hợp một cách lô gíc với thông điệp dữ liệu để xác nhận chủ thể ký và khẳng định sự chấp thuận của chủ thể đó đối với thông điệp dữ liệu.

[NGUỒN: Điều 3, Luật số 20/2023/QH15]

3.1.5

Chữ ký trên thiết bị di động (mobile signature)

Phương thức tổng quát sử dụng thiết bị di động để xác nhận ý định của người dùng nhằm thực hiện một giao dịch.

3.1.6

Thuộc tính chữ ký (signature attributes)

Thông tin bổ sung được ký cùng với tài liệu chủ thể ký.

3.1.7

Cổng chữ ký (signature gateway)

Nền tảng do nhà cung cấp dịch vụ ký số trên thiết bị di động vận hành để kích hoạt chức năng ký số trên thiết bị di động.

3.1.8

Yêu cầu chữ ký (signature request)

Thông điệp gửi từ nhà cung cấp ứng dụng đến nhà cung cấp dịch vụ ký số trên thiết bị di động, yêu cầu tạo một chữ ký di động.

3.1.9

Phản hồi chữ ký (signature response)

Thông điệp gửi từ nhà cung cấp dịch vụ ký số trên thiết bị di động đến nhà cung cấp ứng dụng để phản hồi một yêu cầu tạo chữ ký di động.

3.1.10

Chủ thể ký (signer)

Cá nhân hoặc thực thể tạo ra chữ ký trên thiết bị di động.

3.1.11

Tài liệu của chủ thể ký (signer's document)

Tài liệu mà chủ thể ký dự định tạo chữ ký trên thiết bị di động.

3.1.12

Mời ký (signature invocation)

Hành động mà ứng dụng hoặc thiết bị tạo chữ ký thực hiện để bắt đầu quá trình ký.

3.1.13

Chính sách chữ ký (signature policy)

Tập hợp các quy tắc cho việc tạo và xác thực chữ ký, làm cơ sở để xác định tính hợp lệ của chữ ký.

3.1.14

Thẻ SIM (SIM-Card)

Thẻ thông minh nằm bên trong thiết bị di động được sử dụng để quản lý quyền truy cập của thuê bao vào mạng di động.

CHÚ THÍCH: Thẻ SIM (SIM-Card) là một trong các phương án triển khai MSCD. Phù hợp với nguyên tắc trung lập công nghệ nêu tại 5.1, các phương án khác như phần cứng bảo mật tích hợp trong chip thiết bị hoặc giải pháp ký số từ xa dựa trên HSM phía máy chủ cũng được chấp nhận là MSCD hợp lệ, miễn là đáp ứng đầy đủ các yêu cầu bảo mật quy định tại Điều 6.4 của tiêu chuẩn này.

3.1.15

Kênh truyền tin cậy (trusted channel)

Cơ chế mà qua đó các sản phẩm công nghệ thông tin từ xa có thể giao tiếp với nhau một cách an toàn.

3.1.16

Đường dẫn tin cậy (trusted path)

Cơ chế mà qua đó một người dùng và một chức năng bảo mật có thể giao tiếp với nhau một cách an toàn.

3.2 Chữ viết tắt

AP	Application Provider	Nhà cung cấp ứng dụng
API	Application Programming Interface	Giao diện lập trình ứng dụng
CA	Certification Authority	Tổ chức cung cấp dịch vụ chứng thực
CEN	European Committee for Standardization	Ủy ban Tiêu chuẩn Châu Âu
CSP	Certification Service Provider	Tổ chức cung cấp dịch vụ chứng thực
CSPC	CSP interaction Component	Thành phần tương tác CSP
CWA	CEN Workshop Agreement	Thỏa thuận hội thảo CEN
DAC	MSCD/MSCA Communicator	Bộ giao tiếp MSCD/MSCA
DHC	Data Hashing Component	Thành phần băm dữ liệu
DTBS	Data To Be Signed	Dữ liệu cần ký
DTBSF	DTBS Formatted	Dữ liệu cần ký đã định dạng
DTBSR	DTBS Representation	Bản thể hiện dữ liệu cần ký
DTBSV	DTBS Verifier	Xác minh dữ liệu cần ký
EESSI	European Electronic Signature Standardization Initiative	Sáng kiến Tiêu chuẩn chữ ký điện tử Châu Âu
ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn viễn thông Châu Âu
MSA	Mobile Signature Application	Ứng dụng ký số trên thiết bị di động
MSCA	Mobile Signature Creation Application	Ứng dụng tạo chữ ký trên thiết bị di động
MSCD	Mobile Signature Creation Device	Thiết bị tạo chữ ký số di động
MSCE	Mobile Signature Creation Environment	Môi trường tạo chữ ký trên thiết bị di động
MSCS	Mobile Signature Creation System	Hệ thống tạo chữ ký trên thiết bị di động
MSE	Mobile Signature Environment	Môi trường ký số trên thiết bị di động
MSSP	Mobile Signature Service Provider	Tổ chức cung cấp dịch vụ ký số trên thiết bị di động

PAC	MSSP/MSCA Communicator	Bộ giao tiếp MSSP/MSCA
PIN	Personal Identification Number	Mã nhận dạng cá nhân
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
PPC	MSSP/AP Communicator	Bộ giao tiếp MSSP/AP
SAC	Signer Authentication Component	Thành phần xác thực chủ thể ký
SAD	Signer Authentication Data	Dữ liệu xác thực chủ thể ký
SAV	Signature Attribute Viewer	Trình xem thuộc tính chữ ký
SCC	Signature Creation Component	Thành phần tạo chữ ký
SCD	Signature Creation Data	Dữ liệu tạo chữ ký
SDO	Signer Data Object	Đối tượng dữ liệu chủ thể ký
SDOC	Signed Data Object Composer	Thành phần đối tượng dữ liệu chủ thể ký
SDP	Signer Document Presentation	Trình bày tài liệu chủ thể ký
SDPC	SDP Component	Thành phần trình bày tài liệu chủ thể ký
SIC	Signer Interaction Component	Thành phần tương tác chủ thể ký
SLC	Signature Logging Component	Thành phần ghi nhật ký chữ ký
SMS	Short Message Service	Dịch vụ tin nhắn ngắn
SSCD	Secure Signature Creation Device	Thiết bị tạo chữ ký an toàn
UAC	User Authentication Component	Thành phần xác thực người dùng
XML	eXtensible Markup Language	Ngôn ngữ đánh dấu mở rộng

4 Giới thiệu về chữ ký số trên thiết bị di động

4.1 Tổng quan

4.1.1 Chữ ký số trên thiết bị di động

Định nghĩa sau được đề xuất cho khái niệm chữ ký số trên thiết bị di động:

"Phương thức tổng quát sử dụng thiết bị di động để xác nhận ý định của người dùng nhằm thực hiện một giao dịch."

Khi xây dựng định nghĩa này, các khái niệm sau được xem xét:

Phương thức tổng quát:

- trải nghiệm người dùng cuối nhất quán;
- cộng đồng tương tác lớn nhất cho người dùng cuối và nhà cung cấp ứng dụng;
- kiến trúc thúc đẩy khả năng tương tác và chi phí triển khai thấp nhất;
- kiến trúc cung cấp chi phí giao dịch thấp nhất.

Thiết bị di động:

- bất kỳ thiết bị nào sử dụng mạng di động làm kênh truyền thông;
- điện thoại di động, thiết bị cầm tay, máy tính xách tay;
- thẻ thông minh tích hợp và bên ngoài;
- có hoặc không có thẻ thông minh.

Ý định của người dùng:

- một lệnh giao dịch hợp lệ;

- sự cho phép hoặc đồng ý của người dùng để tiến hành giao dịch;

- được thiết kế sao cho người dùng không thể bị nhầm lẫn hoặc bị dẫn dắt sai;

- tuân thủ các quy định về hiệu lực pháp lý theo Luật Giao dịch điện tử 2023 và Nghị định 23/2025/NĐ-CP.

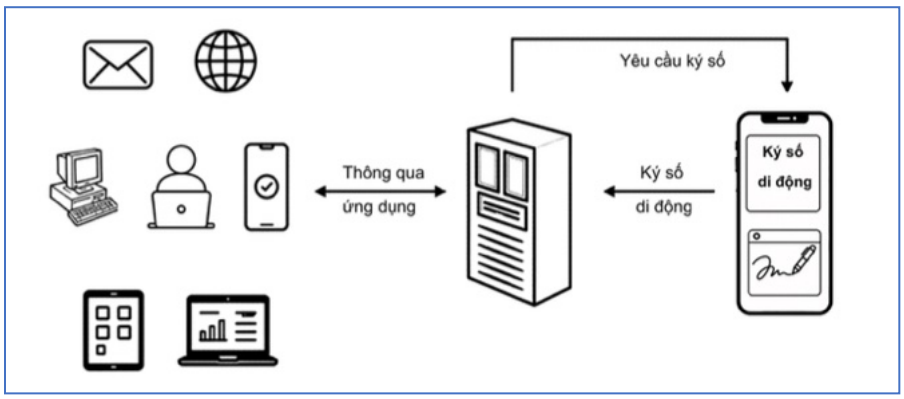
Giao dịch:

- một tương tác yêu cầu sự xác nhận của người dùng để tiến hành, nội dung giao dịch được truyền đến thiết bị di động của người dùng và hiển thị trên màn hình thiết bị di động trước khi người dùng xác nhận.

4.1.2 Sử dụng chữ ký số trên thiết bị di động

Chữ ký số trên thiết bị di động là khái niệm có thể áp dụng cho tất cả các loại ứng dụng chứ không chỉ những ứng dụng có thể truy cập qua thiết bị di động. Việc sử dụng phù hợp cho các ứng dụng yêu cầu sự cho phép của người dùng để hoàn tất giao dịch, có thể được khởi tạo qua cuộc gọi thoại, hệ thống phản hồi thoại tương tác, qua internet và các kênh truyền thông điện tử khác, thậm chí trong các tình huống trực tiếp.

Trong đó, thiết bị di động được coi là công cụ ký.



Hình 1. Thiết bị di động như một công cụ để ký.

Khi xem xét việc sử dụng chữ ký trên thiết bị di động, chúng ta chỉ tập trung vào quy trình khởi tạo một chữ ký điện tử liên quan đến thông điệp được hiển thị cho công dân. Quy trình này loại trừ cụ thể việc kiểm soát ở cấp độ ứng dụng đối với thông điệp đã ký. Việc cung cấp một chữ ký trên thiết bị di động chỉ cho biết rằng công dân đó mong muốn tiến hành giao dịch như đã được mô tả, bất kể việc công dân đó có được phép hoặc có quyền thực hiện giao dịch đó hay không.

4.1.3 Dịch vụ ký số trên thiết bị di động

Việc điều phối và quản lý quy trình ký số trên thiết bị di động tạo ra dịch vụ ký số trên thiết bị di động dành cho cả người dân và các nhà cung cấp ứng dụng. Cách tiếp cận như vậy có thể bao gồm:

- Thúc đẩy nhanh việc áp dụng chữ ký trên thiết bị di động bởi AP.

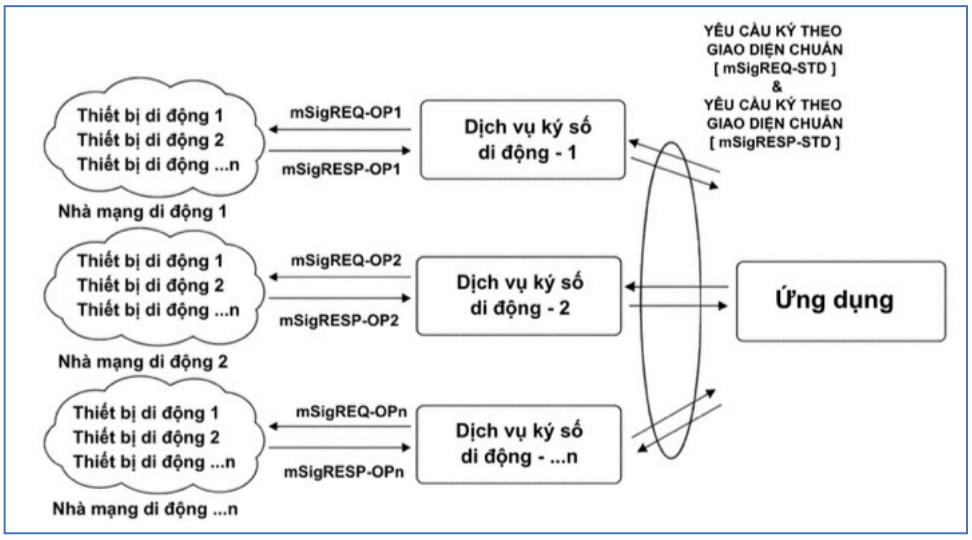
- Cho phép triển khai một API dùng chung.

- Tận dụng sẵn tập người dùng đã có thẻ thông minh và đầu đọc thẻ.

- Điều phối việc kích hoạt chức năng ký số trên thiết bị di động cho người dùng.

- Điều phối xử lý các yêu cầu ký từ phía ứng dụng.
- Gia tăng giá trị cho dịch vụ ký số trên thiết bị di động cốt lõi
- Tận dụng hệ thống chăm sóc khách hàng và kênh liên lạc sẵn có.
- Giải quyết các vấn đề của mô hình các CA truyền thống.
- Giảm chi phí triển khai dịch vụ.
- Tránh trùng lặp hệ thống.
- Tập trung lưu lượng ký.
- Quản lý rủi ro hiệu quả hơn.
- Thúc đẩy khả năng tương tác.

Dịch vụ ký số trên thiết bị di động có thể được cung cấp theo thỏa thuận thương mại giữa MSSP và các bên sử dụng ký số trên thiết bị di động.



Hình 2. Dịch vụ chữ ký điện tử trên thiết bị di động.

Dịch vụ ký số trên thiết bị di động có một giao diện chuẩn hóa, có thể được triển khai dưới dạng một dịch vụ Web trên Internet. Về khía cạnh này, MSSP đóng vai trò là bên trung gian giữa người dùng cuối và các AP, thực hiện việc cung cấp và triển khai dịch vụ Web cho ký số trên thiết bị di động này.

4.2 Khai báo lược đồ XML

Định danh chuẩn XML sau đây được sử dụng cho dịch vụ ký số trên thiết bị di động:

http://uri.etsi.org/2000/v1.00#

Các khai báo định danh sau đây được áp dụng cho các định nghĩa sơ đồ XML xuyên suốt tiêu chuẩn này:

```
<xs:schema
        targetNamespace="http://uri.etsi.org/2000/v1.00#"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:mss="http://uri.etsi.org/2000/v1.00#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        elementFormDefault="qualified"
>
```

Điều này có nghĩa rằng tiền tố ‘ds’ được sử dụng trong toàn bộ tài liệu để biểu thị không gian tên của đặc tả W3C XML-Signature, trong khi tiền tố ‘xs’ biểu thị không gian tên của đặc tả XML-Schema.

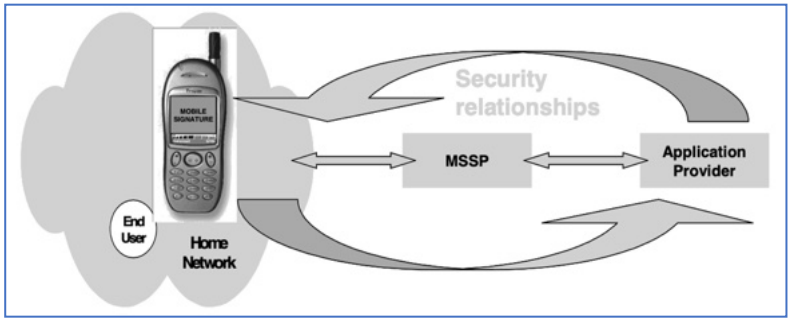
5 Phân tích an toàn thông tin tổng thể

5.1 Kiến trúc

Từ các mô tả tổng quát về dịch vụ, chúng ta xác định được ba thực thể chính:

- Người dùng cuối (End-user);
- Tổ chức cung cấp dịch vụ chữ ký trên thiết bị di động (MSSP);
- Nhà cung cấp ứng dụng (AP).

Các mối đe dọa an ninh có thể được xác định cho từng thực thể và các mối quan hệ an ninh giữa các thực thể cũng cần được xác định.



Hình 3. Phân tích bảo mật của kiến trúc hệ thống ký số trên thiết bị di động.

Người đọc phải nhớ rằng lựa chọn không phụ thuộc vào công nghệ đã được đưa ra trong tài liệu yêu cầu kinh doanh và chức năng. Các tính năng bảo mật khác nhau sẽ được triển khai tùy thuộc vào thiết bị di động, kỹ thuật mã hóa và các yếu tố khác. Do đó, trong khi vẫn giữ tính trung lập về công nghệ, chất lượng của dịch vụ chữ ký trên thiết bị di động có thể thay đổi giữa các phương thức triển khai khác nhau tùy theo việc cung cấp các biện pháp bảo mật.

Nhà cung cấp ứng dụng và người dùng cuối phải có khả năng cung cấp và yêu cầu mức độ bảo mật phù hợp. Điều này có nghĩa là MSSP phải công bố cho AP và người dùng cuối các khả năng bảo mật của mình.

Về khía cạnh này, tài liệu hiện tại xác định các yêu cầu bảo mật liên quan đặc thù cho dịch vụ ký số trên thiết bị di động. Các yêu cầu này là cơ sở để quy định các tiêu chí chung nhằm mô tả chất lượng chữ ký trên thiết bị di động, giúp xác định sự phân cấp của các cấp độ bảo mật.

5.2 Chữ ký điện tử

Chữ ký điện tử theo Luật Giao dịch điện tử số 20/2023/QH15 được phân loại như sau:

Theo khoản 1 Điều 22 Luật GDĐT 2023, chữ ký điện tử được phân loại theo phạm vi sử dụng gồm ba loại: (i) chữ ký điện tử chuyên dùng (do cơ quan, tổ chức tạo lập, sử dụng riêng cho hoạt động nội bộ); (ii) chữ ký số công cộng (bảo đảm bởi chứng thư chữ ký số công cộng, dùng trong hoạt động công cộng); (iii) chữ ký số chuyên dùng công vụ (bảo đảm bởi chứng thư chữ ký số chuyên dùng công vụ). Đây là trục phân loại theo phạm vi, đối tượng sử dụng, khác với trục phân loại chữ ký điện tử thông thường, chữ ký điện tử an toàn và chữ ký số tại mục này vốn mô tả cấp độ bảo mật kỹ thuật của chữ ký theo mức độ ràng buộc, khả năng xác

định chủ thể ký. Hai trục phân loại này không loại trừ nhau, một chữ ký số công cộng hoặc chữ ký số chuyên dùng công vụ đều có thể đồng thời đáp ứng các điều kiện của chữ ký điện tử an toàn hoặc chữ ký số. Việc đổi tên trực tiếp theo ba loại tại Điều 22 khoản 1 có thể gây nhầm lẫn giữa hai trục phân loại khác bản chất; do đó, tiêu chuẩn giữ nguyên cấu trúc theo cấp độ bảo mật và bổ sung chú thích đối chiếu này để tránh mâu thuẫn pháp lý.

Luật GDĐT 2023 (Việt Nam)	Căn cứ pháp lý	Chỉ thị 1999/93/EC (hết hiệu lực)	eIDAS - Quy định (EU) 910/2014 (hiện hành)
Chữ ký điện tử thông thường	Điều 23 Luật GDĐT 2023	Electronic signature	Electronic signature
Chữ ký điện tử an toàn	Điều 22 Luật GDĐT 2023	Advanced electronic signature	Advanced electronic signature (AdES)
Chữ ký số công cộng	Điều 22, Điều 24 Luật GDĐT 2023	Qualified electronic signature	Qualified electronic signature (QES)
Chữ ký số chuyên dùng công vụ	Điều 25 Luật GDĐT 2023	Không có khái niệm tương đương trực tiếp	Không có khái niệm tương đương trực tiếp

Bảng 1. Đối chiếu thuật ngữ phân loại chữ ký điện tử giữa Luật GDĐT 2023 và pháp luật Châu Âu.

5.2.1 Chữ ký điện tử thông thường (Điều 23 Luật GDĐT 2023)

… là dữ liệu dưới dạng điện tử được gắn kèm hoặc kết hợp logic với thông điệp dữ liệu, được sử dụng như một phương thức xác thực danh tính. Chữ ký điện tử thông thường không bị phủ nhận hiệu lực pháp lý, nhưng cũng không được tự động công nhận là tương đương với chữ ký viết tay.

5.2.2 Chữ ký điện tử an toàn (Điều 22 Luật GDĐT 2023)

… là chữ ký điện tử đáp ứng đồng thời các yêu cầu: (i) được tạo ra trong thời gian ký thông điệp dữ liệu; (ii) được tạo ra bằng dữ liệu tạo chữ ký điện tử chỉ gắn duy nhất với nội dung của thông điệp dữ liệu được chấp thuận và chỉ thuộc sự kiểm soát của chủ thể ký tại thời điểm ký; (iii) có khả năng xác định được chủ thể ký và ý chí của chủ thể ký với thông điệp dữ liệu được ký; (iv) có khả năng phát hiện sự thay đổi của thông điệp dữ liệu sau thời điểm ký. Chữ ký điện tử an toàn tương đương với chữ ký viết tay về giá trị pháp lý theo Nghị định 23/2025/NĐ-CP.

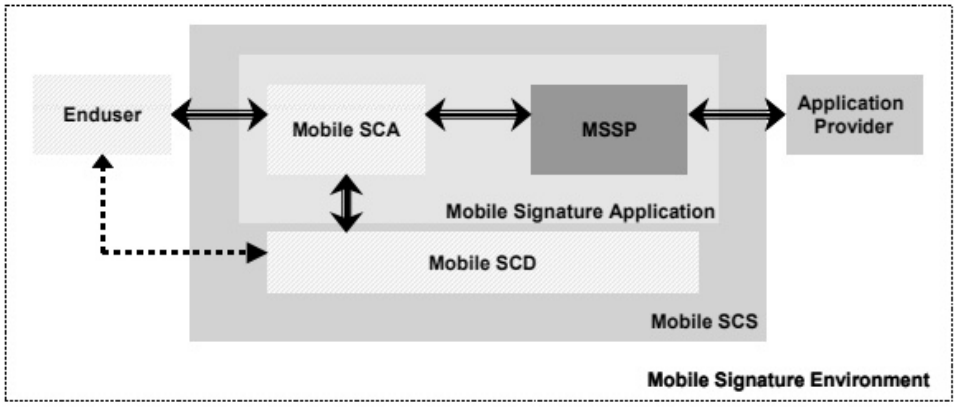
5.2.3 Chữ ký số (chữ ký điện tử dựa trên chứng thư chữ ký số)

… là chữ ký điện tử sử dụng thuật toán khóa không đối xứng (PKI), gồm khóa bí mật dùng để ký và khóa công khai dùng để kiểm tra chữ ký, đáp ứng đầy đủ các điều kiện quy định tại khoản 3 Điều 22 Luật GDĐT 2023 và được bảo đảm bởi chứng thư chữ ký số do tổ chức cung cấp dịch vụ chứng thực chữ ký số được cấp phép cấp. Chữ ký số có giá trị pháp lý đầy đủ, độc lập với khái niệm "chữ ký điện tử an toàn", và được ưu tiên sử dụng trong các giao dịch điện tử yêu cầu độ tin cậy cao, trong đó có mô hình ký số trên thiết bị di động.

Trong bối cảnh Luật Giao dịch điện tử 2023 và Nghị định 23/2025/NĐ-CP, tiêu chuẩn này tập trung vào chữ ký điện tử được tạo ra bằng phương tiện mật mã trong một quy trình liên quan đến thiết bị di động (có thể là điện thoại di động). Kết quả – "ký số trên thiết bị di động" – có thể được thực hiện bằng cách tận dụng khả năng của thiết bị di động (bao gồm hạ tầng SIM/UICC) và hạ tầng mạng di động theo nhiều cách khác nhau. Dù triển khai theo cách nào, nguyên tắc cơ bản là thu được xác nhận từ người dùng rằng họ muốn tiến hành giao dịch, chi tiết của giao dịch đã được hiển thị cho người dùng trên màn hình điện thoại di động của họ.

5.3 Xác định môi trường ký số trên thiết bị di động (MSE)

Để bám sát nhất có thể các khái niệm và phương pháp luận của EESSI, chúng tôi định nghĩa các thành phần sau đây của hệ thống tạo chữ ký số trên thiết bị di động.



Hình 4. Môi trường chữ ký trên thiết bị di động.

Giải thích thuật ngữ:

- Người dùng cuối (Enduser): Theo thuật ngữ được sử dụng xuyên suốt các tiêu chuẩn kỹ thuật về ký số trên thiết bị di động, người dùng cuối chính là chủ thể ký.

- Môi trường ký số trên thiết bị di động (MSE): Là môi trường vật lý, địa lý và công nghệ của hệ thống tạo chữ ký số trên thiết bị di động.

- Hệ thống tạo chữ ký trên thiết bị di động (MSCS): Là hệ thống tổng thể thực hiện việc tạo ra ký số trên thiết bị di động, bao gồm MSCD và MSA.

- Thành phần tạo chữ ký trên thiết bị di động (MSCD): Là thiết bị/môi trường thực thi việc tạo chữ ký, tương đương với SSCD (Secure Signature Creation Device - Thiết bị tạo chữ ký an toàn) trong môi trường di động; không đồng nhất với SCD (Signature Creation Data - Dữ liệu tạo chữ ký), là dữ liệu (khóa bí mật) được lưu giữ và sử dụng bên trong MSCD.

- Ứng dụng ký số trên thiết bị di động (MSA): Là ứng dụng di động nằm trong MSCS thực hiện việc tạo chữ ký, không bao gồm MSCD. Ứng dụng ký số trên thiết bị di động bao gồm MSCA và MSSP.

- Ứng dụng tạo chữ ký trên thiết bị di động (MSCA): Là ứng dụng nằm trong MSCS thực hiện tạo chữ ký trên thiết bị di động bằng cách sử dụng các dịch vụ từ MSSP và MSCD.

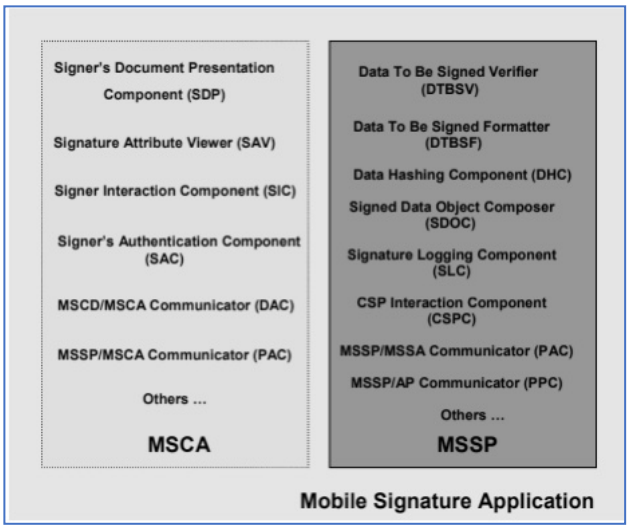
- Nhà cung cấp dịch vụ ký số trên thiết bị di động (MSSP): Cung cấp các dịch vụ ký số trên thiết bị di động cho chủ thể ký thông qua MSCA và cung cấp cho AP.

- Nhà cung cấp ứng dụng (AP): Là cá nhân hoặc tổ chức sử dụng các ký số trên thiết bị di động do chủ thể ký tạo ra. Thuật ngữ sẽ xuyên suốt tiêu chuẩn này, AP đóng vai trò là Bên thứ ba tin cậy (Bên tiếp nhận/sử dụng chữ ký).

5.4 Vận hành của ứng dụng ký số trên thiết bị di động (MSA)

Chủ thể ký phối hợp cùng các thành phần của MSA và MSCD để tạo ra một ký số trên thiết bị di động thông qua một chuỗi các bước. Mỗi thành phần này được phân bổ cho MSCA hoặc cho MSSP. Tuy nhiên, vì tiêu chuẩn này không phụ thuộc vào công nghệ cụ thể, nó không mặc định bất kỳ sự phân bổ cố định nào của các thành phần cho MSCA hay MSSP. Chẳng hạn, tùy thuộc vào khả năng của thiết bị di động, một số thành phần sẽ có nhiều khả năng được triển khai bởi MSSP ở phía máy chủ.

Trong sơ đồ dưới đây, các thành phần được trình bày theo một cách triển khai điển hình của một MSA. Trong cách triển khai này, MSSP hỗ trợ MSCA trong việc định dạng thông điệp cần được ký bởi MSCD. Tuy nhiên, việc định dạng này cũng có thể được thực hiện bởi MSCA. Mặt khác, tất cả các tác vụ được thực hiện bởi các thành phần liên kết với MSCA cũng đều có thể được thực hiện bởi MSSP.



Hình 5. Cấu trúc bên trong của một ứng dụng ký số trên thiết bị di động.

Hình trên cung cấp một cái nhìn tổng quan ngắn gọn về các thành phần được phân bổ cho MSCA và MSSP.

Để tạo ra một ký số trên thiết bị di động, các bước sau đây có thể được thực hiện nếu có DTBS được gửi từ AP tới MSSP:

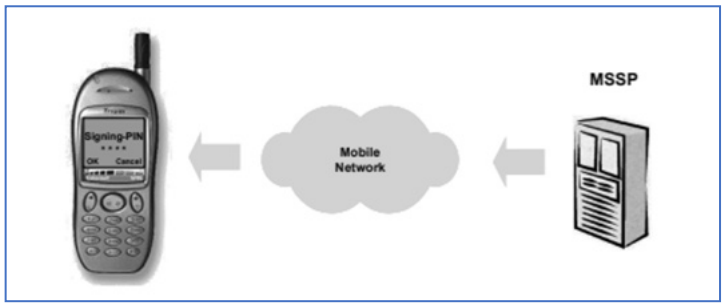
- MSSP kiểm tra để đảm bảo rằng DTBS hợp lệ về mặt cú pháp và ngữ nghĩa. Tuy nhiên, theo CEN và ESI, DTBS có thể bao gồm: tài liệu ký số, mã định danh chính sách chữ ký, mã định danh chứng thư, loại cam kết và các thông tin khác. Dù vậy, yêu cầu chữ ký dịch vụ chữ ký trên thiết bị di động (MSS Signature Request) vẫn có thể chứa các thông tin bổ sung này. Do đó, MSSP sở hữu dữ liệu tương đương với DTBS theo định nghĩa của CEN và ESI.

- MSSP định dạng DTBS bằng cách sử dụng bộ định dạng, kết quả thu được gọi là DTBSF. Bước này tương ứng với việc định dạng DTBS theo chuẩn ASN.1 để đảm bảo tuân thủ cấu trúc PKCS#7.

- DHC sau đó sẽ tiếp nhận DTBSF và tính toán ra DTBSR thông qua quá trình băm (hash). Trong một số trường hợp, toàn bộ quá trình băm được thực hiện bởi MSSP hoặc MSCA. Trong các trường hợp khác, một số bước của quá trình băm có thể được thực hiện bởi MSCD.

- DTBSR sau đó có thể được chuyển tới MSCA thông qua bộ giao tiếp MSSP/MSCA (PAC) theo yêu cầu của MSCA.

- MSCA được khởi tạo sang chế độ vận hành bằng cách khởi động phần mềm MSCA. MSCA và MSSP thực hiện xác thực lẫn nhau, và bộ giao tiếp MSSP/MSCA (PAC) phía MSCA sẽ thiết lập một kênh truyền tin cậy để truyền tải DTBSR.



Hình 6. Mạng di động: Kênh truyền tin cậy cho môi trường ký số trên thiết bị di động.

- MSCA phải cho phép chủ thể ký xem xét DTBSR thông qua việc sử dụng thành phần trình bày tài liệu chủ thể ký (SDPC) và SAV, nhằm đảm bảo rằng toàn bộ thông tin trong DTBSR là chính xác và không bị thiếu sót.

- MSCA và MSCD sau đó có thể xác thực lẫn nhau để đảm bảo với chủ thể ký rằng MSCA đáng tin cậy. Việc xác thực lẫn nhau này là cần thiết nếu MSCA nằm dưới sự kiểm soát của nhà cung cấp dịch vụ, nhưng không cần thiết nếu MSCA hoàn toàn nằm dưới sự kiểm soát của chủ thể ký.

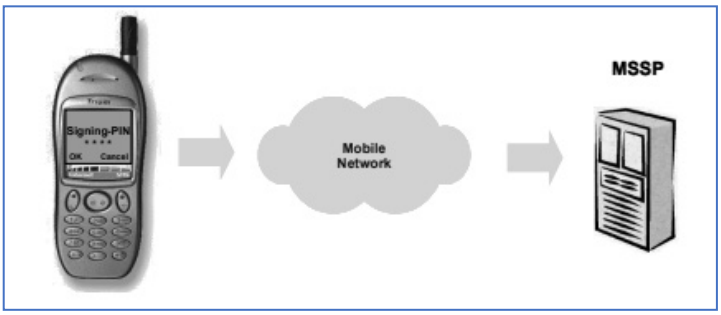
- Sau đó, MSCA phải tương tác với chủ thể ký thông qua SIC để nhận lệnh gọi ký, lệnh này hướng dẫn MSCA và MSCD bắt đầu quá trình ký.

- Chủ thể ký sau đó cung cấp SAD thông qua SAC, có thể gửi trực tiếp tới MSCA hoặc tới MSCD. Dữ liệu SAD này được truyền qua bộ giao tiếp MSCD/MSCA (DAC), thiết lập đường dẫn tin cậy (trusted path) giữa các thành phần này nếu dữ liệu không được nhập trực tiếp vào chính thiết bị tạo chữ ký số di động (MSCA).

- Bộ giao tiếp MSCD/MSCA (DAC) sau đó có thể khởi tạo một kênh truyền tin cậy để truyền tải DTBSR.

- MSCD sau đó thực hiện tạo chữ ký số trên thiết bị di động dựa trên DTBSR, sử dụng dữ liệu tạo chữ ký (SCD) của chủ thể ký.

- Ký số trên thiết bị di động sau đó được chuyển ngược lại cho MSCA thông qua bộ giao tiếp MSCD/MSCA (DAC) và được chuyển tới hệ thống MSSP.



Hình 7. Mạng di động: Kênh truyền tin cậy cho môi trường ký số trên thiết bị di động.

- Thành phần đối tượng dữ liệu chủ thể ký (SDOC) sau đó thường tiếp nhận các thành phần của DTBSF, kết hợp chúng với chuỗi bit đại diện cho ký số trên thiết bị di động do MSCD cung cấp, và soạn thảo thành một SDO.

- MSSP nhúng SDO này vào phản hồi chữ ký và chuyển giao cho AP thông qua bộ giao tiếp MSSP/AP (PPC). Tất cả các hoạt động này có thể được ghi lại bởi thành phần ghi nhật ký chữ ký (SLC).

- Nếu MSCA hoặc MSSP có thể xác minh chữ ký, thì kết quả xác minh chữ ký sẽ được hiển thị.

6 Yêu cầu bảo mật đối với hệ thống tạo chữ ký số trên thiết bị di động (MSCS)

6.1 Yêu cầu bảo mật tổng thể của MSCS

MSCS phải đảm bảo rằng chữ ký được tạo ra phản ánh đúng ý chí và nhận thức của người dùng, đồng thời ngăn ngừa mọi hành vi giả mạo hoặc tạo chữ ký trái phép.

6.1.1 Yêu cầu đối với dữ liệu cần ký (DTBS)

Dữ liệu cần ký là yếu tố cốt lõi quyết định giá trị pháp lý của chữ ký, việc xử lý dữ liệu cần ký phải tuân thủ các yêu cầu sau:

- MSCS-01: DTBS phải chứa tài liệu của chủ thể ký.
- MSCS-02: DTBS phải chứa chứng thư chữ ký của chủ thể ký liên quan đến dữ liệu tạo chữ ký mà MSCD sử dụng để tạo chữ ký số trên thiết bị di động và theo ý định của chủ thể ký.
- MSCS-03: DTBS phải chứa chính sách chữ ký (hoặc tham chiếu đến chính sách chữ ký).
- MSCS-04: DTBS phải chứa thuộc tính loại cam kết nếu chính sách chữ ký định nghĩa nhiều hơn một loại cam kết.
- MSCS-05: Nếu quy định hiện hành cho phép nhiều hơn một định dạng nội dung tài liệu của chủ thể ký thì DTBS phải chứa định dạng nội dung tài liệu của chủ thể ký.

6.1.2 Yêu cầu về kênh truyền tin cậy (Trusted channel)

Các yêu cầu đối với kênh truyền tin cậy nhằm đối phó với mối đe dọa về việc các thành phần của DTBS, DTBSF, DTBSR, ký số trên thiết bị di động và SDO có thể bị hư hỏng hoặc bị sửa đổi trong khi chúng nằm trong MSCA hoặc MSSP, cũng như trong quá trình truyền tải giữa MSCA và MSSP hoặc giữa MSCA và thiết bị tạo chữ ký số di động (MSCD). Các yêu cầu này cũng nhằm đối phó với mối đe dọa về việc vi phạm tính bảo mật của các đối tượng nêu trên:

- MSCS-06: MSCA, MSSP và MSCD phải duy trì tính toàn vẹn của các thành phần DTBS, DTBSF, DTBSR, ký số trên thiết bị di động và SDO.

- MSCS-07: MSCA, MSSP và MSCD phải duy trì tính toàn vẹn của tất cả dữ liệu giao thức truyền tải giữa ứng dụng tạo chữ ký số trên thiết bị di động và nhà cung cấp dịch vụ ký số trên thiết bị di động cũng như giữa ứng dụng tạo chữ ký số trên thiết bị di động và thiết bị tạo chữ ký số di động.
- MSCS-08: MSCA, MSSP và MSCD phải duy trì tính bí mật của các thành phần DTBS, DTBSF, DTBSR, ký số trên thiết bị di động và SDO.
- MSCS-09: Hệ thống phải đảm bảo rằng các thành phần DTBS được sử dụng để tạo DTBSF và DTBSR là giống hệt với những thành phần đã được trình bày cho chủ thể ký trong quá trình trình bày và chúng đồng nhất với những gì chủ thể ký đã ký.

6.1.3 Yêu cầu phát sinh từ các tiến trình và cổng giao tiếp không tin cậy

Yêu cầu sau nhằm đối phó với nguy cơ bị can thiệp từ các tiến trình và cổng giao tiếp không tin cậy trong hệ thống:

- MSCS-10: Tất cả các hệ thống, tiến trình ứng dụng, thiết bị ngoại vi và kênh truyền thông không tin cậy phải bị ngăn chặn không được can thiệp vào các tiến trình ký.

6.1.4 Kiểm soát đầu vào (Input control)

Giao diện đầu vào luôn tiềm ẩn rủi ro vì, ví dụ kẻ xâm nhập có thể cố gắng sửa đổi các thành phần hệ thống hoặc virus xâm nhập có thể làm hỏng dữ liệu và phần mềm. Các yêu cầu sau đây nhằm đối phó với mối đe dọa từ các thành phần hệ thống bị xâm nhập hoặc bị giả mạo:

- MSCS-11: Phải trang bị giải pháp phòng chống mã độc đối với MSCS hoặc đảm bảo rằng hệ thống tạo chữ ký số trên thiết bị di động bị tấn công tấn công bởi mã độc có thể được phục hồi đúng cách.
- MSCS-12: MSCS phải bảo vệ tính toàn vẹn của các thành phần chức năng chính nó nhằm tránh khả năng bị tấn công làm hỏng chúng.
- MSCS-13: MSCS chỉ cho phép cài đặt các thành phần chức năng khác thông qua một quy trình tải xuống bảo mật.

6.2 Ứng dụng tạo chữ ký trên thiết bị di động (MSCA)

Nội dung này xác định các yêu cầu bảo mật tối thiểu áp dụng cho từng thành phần cấu thành nên MSCA.

6.2.1 Thành phần trình bày tài liệu của chủ thể ký (SDP)

Các yêu cầu sau đây nhằm đối phó với mối đe dọa về việc ký một tài liệu mà chủ thể ký không có ý định ký (ký nhầm hoặc ký sai nội dung):

- MSCA-01: SDP phải cảnh báo chủ thể ký nếu tài liệu của chủ thể ký không phù hợp với cú pháp được quy định bởi định dạng nội dung và cho phép chủ thể ký hủy khỏi quá trình ký.
- MSCA-02: SDP phải cảnh báo chủ thể ký nếu định dạng nội dung được chỉ định trong tài liệu của chủ thể ký không được thành phần trình bày tài liệu của chủ thể ký hỗ trợ đầy đủ hoặc không được thành phần trình bày tài liệu của chủ thể ký chấp nhận và cho phép chủ thể ký hủy bỏ quá trình ký.

- MSCA-03: SDP phải thông báo cho chủ thể ký rằng các SDO khác được nhúng trong tài liệu của chủ thể ký (điều này sẽ ngăn chủ thể ký vô tình ký các đối tượng có chữ ký sai hoặc không hợp lệ do người khác tạo ra).
- MSCA-04: SDP không cho phép chủ thể ký thay đổi bất kỳ phần nào trong tài liệu của chủ thể ký.
- MSCA-05: SDP phải cảnh báo chủ thể ký về sự hiện diện của các văn bản ẩn, thư viện lệnh hoặc mã thực thi và cho phép chủ thể ký hủy khỏi quá trình ký.

6.2.2 Trình xem thuộc tính chữ ký (SAV)

Các yêu cầu sau đây nhằm đối phó với mối đe dọa về việc ký một tài liệu bao gồm các thuộc tính mà chủ thể ký không chủ ý đưa vào:

- MSCA-06: Quy trình hiển thị thuộc tính chữ ký phải cho phép chủ thể ký xem được các thuộc tính chữ ký
- MSCA-07: Quá trình xem thuộc tính sẽ cảnh báo chủ thể ký về sự hiện diện sự hiện diện của các văn bản ẩn, thư viện lệnh (macro) được nhúng trong các thuộc tính chữ ký.
- MSCA-08: SAV cho phép chủ thể ký có thể kiểm tra các thành phần chính của chứng thư chữ ký có trong DTBS.

6.2.3 Thành phần tương tác chủ thể ký (SIC)

Các yêu cầu sau đây nhằm đối phó với mối đe dọa về việc tạo chữ ký ngoài ý muốn:

- MSCA-09: Trước khi bắt đầu quá trình ký, SIC sẽ yêu cầu chủ thể ký thực hiện một tương tác kích hoạt chữ ký phức tạp với SAC, điều này ngăn chặn việc khai thác bởi các chương trình tự động (bot).
- MSCA-10: SIC phải đặt ra giới hạn về thời gian hết hạn trong việc cung cấp SAD từ lúc gửi lời mời đến lúc hoàn thành ký kết..
- MSCA-11: Nếu thời hạn này hết hạn, toàn bộ quá trình ký sẽ bị chấm dứt và chủ thể ký sẽ phải bắt đầu lại quá trình ký bằng cách nhập lại thông tin SAD.

6.2.4 Thành phần xác thực chủ thể ký (SAC)

Các yêu cầu sau đây nhằm đối phó với mối đe dọa về việc sử dụng thiết bị MSCD trái phép:

- MSCA-12: MSCA phải cung cấp phương thức để chủ thể ký nhập SAD thông qua MSCA đến MSCD.
- MSCA-13: MSCA phải duy trì tính bí mật của SAD và phải xóa bỏ ngay khi không còn sử dụng nữa.
- MSCA-14: Nếu SAD nhập sai liên tiếp nhiều lần, hệ thống phải gửi thông báo lỗi cho chủ thể ký và cho phép thử lại nếu phương thức xác thực của chủ thể ký nếu chưa bị MSCA khoá.
- MSCA-15: MSCA phải cung cấp một đường dẫn tin cậy cho việc chuyển đổi SAD sang dữ liệu tạo chữ ký bảo mật (SSCD).
- MSCA-16: Phải cung cấp chức năng thay đổi SAD dựa trên thông tin đã biết (Ví dụ PIN, mật khẩu), trừ trường hợp việc sử dụng chức năng này bị cấm bởi chính sách bảo mật.

- MSCA-17: Thông tin SAD không được hiển thị, ứng dụng tạo chữ ký số trên thiết bị di động (MSCA) phải cung cấp một phương thức khác ví dụ nhập PIN/Mật khẩu hiển thị **** hoặc • • • •) mà không tiết lộ thông tin SAD.
- MSCA-18: MSCA phải yêu cầu trình bày SAD mới hai lần và kiểm tra cả hai bản trình bày phải giống nhau trước khi gửi SAD mới cho MSCD.

6.2.5 Bộ giao tiếp MSCD/MSCA (DAC)

Các yêu cầu sau đây đối phó với mối đe dọa về việc tạo ra các chữ ký sai từ phía thiết bị MSCD:

- MSCA-19: Bộ giao tiếp MSCD/MSCA (DAC) phải hỗ trợ tất cả các mục liên quan đến giao diện vật lý trong phạm vi đã định hoặc theo các đặc tính đã được chỉ định, nhằm đảm bảo hoạt động đúng của các loại MSCD mà nó tuyên bố hỗ trợ.
- MSCA-20: Bộ giao tiếp MSCD/MSCA (DAC) phải đảm bảo rằng chức năng MSCD chính xác được chọn, nếu nền tảng nơi chức năng MSCD được triển khai yêu cầu việc lựa chọn.
- MSCA-21: Trường hợp bộ giao tiếp MSCD/MSCA (DAC) sử dụng kênh truyền thông qua mạng viễn thông (OTA/SMS) để truyền dữ liệu cần ký (DTBS/DTBSR) giữa MSSP và MSCD, kênh truyền này phải áp dụng cơ chế mã hóa và toàn vẹn dữ liệu bắt buộc (theo chuẩn bảo mật 3GPP TS 03.48 hoặc tương đương), không được để ở mức khuyến nghị hoặc chỉ nêu trong ví dụ minh họa, nhằm phòng chống nguy cơ tấn công xen giữa (MiTM) từ hạ tầng viễn thông trung gian. Ranh giới trách nhiệm bảo mật giữa tổ chức cung cấp dịch vụ ký số (CA/MSSP) và nhà mạng viễn thông (MNO) đối với kênh truyền này phải được quy định rõ trong thỏa thuận cung cấp dịch vụ.

6.2.6 Bộ giao tiếp MSSP/MSCA (PAC)

Yêu cầu về tính và toàn vẹn của dữ liệu trao đổi giữa MSSP và MSCA:

- MSCA-22: MSCA và MSSP phải xác thực lẫn nhau, để đảm bảo với chủ thể ký rằng MSSP và yêu cầu ký số trên thiết bị di động này được tin tưởng.

6.3 Tổ chức cung cấp dịch vụ ký số trên thiết bị di động (MSSP)

Nội dung này xác định các yêu cầu bảo mật tối thiểu tổng thể áp dụng cho từng thành phần cấu thành nên MSSP.

6.3.1 Thành phần xác minh dữ liệu cần ký (DTBSV)

Các yêu cầu sau đây đối phó với những mối đe dọa đối với cả chủ thể ký và nhà cung cấp dịch vụ (AP) liên quan đến các định dạng nội dung và thuộc tính chữ ký không phù hợp:

- MSSP-01: MSSP phải xác minh tất cả các thành phần DTBS được trích xuất từ yêu cầu chữ ký theo các yêu cầu MSCA-01, MSCA-02, MSCA-03, MSCA-05 và MSCA-07.
- MSSP-02: MSSP phải cảnh báo chủ thể ký bằng cách tạo ra cảnh báo như được mô tả trong điều khoản 6.2.1.
- MSSP-03: MSSP phải thông báo cho chủ thể ký về những hệ quả của tài liệu chủ thể ký nếu cần thiết.
- MSSP-04: MSSP phải từ chối yêu cầu ký số nếu cần thiết.

- MSSP-05: MSSP không được thay đổi DTBS từ AP mà không có sự đồng ý của AP.

6.3.2 Thành phần định dạng dữ liệu cần ký (DTBSF)

Yêu cầu sau đây đối phó với nguy cơ dẫn đến việc tạo ra DTBS sai lệch hoặc không đầy đủ:

- MSSP-06: MSSP phải tạo ra định dạng DTBSF theo yêu cầu ký số.

6.3.3 Thành phần băm dữ liệu (DHC)

Các yêu cầu sau đây đối phó với mối đe dọa từ việc sử dụng các thuật toán không đủ mạnh và tạo ra cấu trúc DTBSR không đầy đủ:

- MSSP-07: MSSP phải đảm bảo rằng chỉ sử dụng các thuật toán băm thuộc một tập hợp các thuật toán và tham số được phê duyệt cho ký số trên thiết bị di động, cụ thể tại Phụ lục A của tiêu chuẩn này, phù hợp Quy chuẩn kỹ thuật quốc gia QCVN 137:2025/BKHCN hoặc hướng dẫn thuật toán mật mã hiện hành của Ban Cơ yếu Chính phủ.
- MSSP-08: MSSP phải đảm bảo rằng chỉ sử dụng các định dạng đầu vào chữ ký được cho phép bởi các thuật toán và tham số được phê duyệt cho ký số trên thiết bị di động, cụ thể tại Phụ lục A của tiêu chuẩn này.
- MSSP-09: MSSP phải đảm bảo việc tạo ra DTBSR chính xác cho ký số trên thiết bị di động.

6.3.4 Thành phần đối tượng dữ liệu chủ thể ký (SDOC)

SDOC liên kết với đầu ra của MSCD với DTBSF theo định dạng chuẩn được xác định bởi loại SDO và tạo ra SDO.

Không có yêu cầu bảo mật nào được quy định cho SDOC. Tuy nhiên, điều cần thiết là SDO thu được phải có cấu trúc giống với DTBS, ví dụ: trình tự của tài liệu chủ thể ký và thuộc tính chữ ký phải giống nhau. Nếu không, ký số trên thiết bị di động sẽ không hợp lệ.

6.3.5 Thành phần tương tác với CSP (CSPC)

CSPC sẽ tương tác với các CSP để nhập chứng thư chữ ký số của chủ thể ký và kiểm tra trạng thái của chúng.

Không có yêu cầu bảo mật nào dành riêng cho thành phần tương tác với CSP. Tuy nhiên, nên thường xuyên kiểm tra tính hợp lệ của chứng thư chữ ký số của chủ thể ký.

6.3.6 Thành phần ghi nhật ký chữ ký (SLC)

Đối với chủ thể ký, việc nhận được hỗ trợ từ MSSP liên quan đến việc ghi nhật ký chữ ký là rất hữu ích, tức là MSSP có thể lưu trữ một bản ghi nhật ký cho mỗi chữ ký được tạo ra. Rõ ràng, bản ghi nhật ký không được phép sửa đổi.

Không có yêu cầu bảo mật cụ thể nào dành cho thành phần ghi nhật ký chữ ký (SLC). Tuy nhiên, nên duy trì số lượng chữ ký được ghi lại.

6.3.7 Bộ giao tiếp MSSP/MSCA (PAC)

Yêu cầu này nhằm đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu trao đổi giữa MSSP và MSCA:

- MSSP-10: MSCA và MSSP phải xác thực lẫn nhau, để đảm bảo với chủ thể ký rằng MSSP và yêu cầu ký số trên thiết bị di động này được tin tưởng (MSCA-21)

6.3.8 Bộ giao tiếp MSSP/AP (PPC)

Yêu cầu này nhằm đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu trao đổi giữa MSSP và AP:

- MSSP-11: AP và MSSP phải xác thực lẫn nhau.

6.4 Thiết bị tạo chữ ký số di động (MSCD)

Trong phạm vi tiêu chuẩn này, các yêu cầu bảo mật đối với MSCD và SAC sẽ được xác định cụ thể:

6.4.1 Yêu cầu bảo mật tổng thể cho MSCD

Các yêu cầu bảo mật tổng thể đối với MSCD liên quan đến cơ chế tự kiểm tra các thành phần nội bộ của MSCD, chống rò rỉ thông tin, ngăn ngừa các trạng thái không an toàn và phát hiện các cuộc tấn công vật lý:

- MSCD-01: MSCD phải thực hiện một bộ các phép kiểm thử để chứng minh việc vận hành đúng của các giả định an toàn được cung cấp bởi máy mô hình làm nền tảng cho các chức năng bảo mật.
- MSCD-02: MSCD phải thực hiện một bộ các phép kiểm thử để chứng minh rằng các chức năng bảo mật hoạt động đúng.
- MSCD-03: MSCD phải cung cấp cho người dùng được ủy quyền khả năng kiểm tra tính toàn vẹn của dữ liệu thuộc các chức năng bảo mật.
- MSCD-04: MSCD phải cung cấp cho người dùng được ủy quyền khả năng kiểm tra tính toàn vẹn của mã thực thi được lưu trữ của các chức năng bảo mật.
- MSCD-05: MSCD không được tạo ra dữ liệu dư thừa để tránh việc kẻ tấn công có thể truy cập vào SAD hoặc dữ liệu tạo chữ ký (SCD).
- MSCD-06: MSCD phải đảm bảo rằng kẻ tấn công không thể lợi dụng các giao diện để truy cập vào SAD hoặc dữ liệu tạo chữ ký (SCD).
- MSCD-07: MSCD phải duy trì trạng thái an toàn khi xảy ra các lỗi liên quan đến bảo mật.
- MSCD-08: MSCD phải cung cấp khả năng phát hiện rõ ràng đối với các hành vi can thiệp vật lý có thể làm ảnh hưởng đến các chức năng bảo mật.
- MSCD-09: MSCD phải cung cấp khả năng xác định có xảy ra hành vi can thiệp vật lý hay không.
- MSCD-10: MSCD phải chống lại việc can thiệp (can thiệp vật lý hoặc tấn công phần cứng) bằng cách tự động phản ứng sao cho an ninh không bị vi phạm.

6.4.2 Thành phần xác thực người dùng (UAC)

Nếu MSCD sở hữu giao diện người dùng (HI) riêng, các yêu cầu sau đây phải được đáp ứng:

- MSCD-11: MSCD phải cung cấp một giao diện người dùng (HI) để nhập SAD
- MSCD-12: MSCD phải đảm bảo tính bí mật của SAD và xóa an toàn dữ liệu này ngay khi không còn cần thiết.
- MSCD-13: Nếu SAD nhập sai nhiều lần liên tiếp (ví dụ 03 lần liên tiếp), hệ thống phải gửi thông báo lỗi cho chủ thể ký và cho phép thử lại nếu phương thức xác thực của chủ thể ký nếu chưa bị MSCD khóa.

- MSCD-14: Phải cung cấp chức năng thay đổi SAD dựa trên thông tin đã biết (Ví dụ PIN, mật khẩu), trừ trường hợp việc sử dụng chức năng này bị cấm bởi chính sách bảo mật. (MSCA-16)
- MSCD-15: Thông tin SAD không được hiển thị, phải cung cấp một phương thức khác (ví dụ nhập PIN/Mật khẩu hiển thị **** hoặc • • • •) mà không tiết lộ thông tin SAD. (MSCA-17)
- MSCD-16: MSCD phải yêu cầu nhập SAD mới hai lần và kiểm tra xem hai lần nhập có giống nhau hay không.
- MSCD-17: Khi số lần nhập sai SAD liên tiếp vượt quá số lần tối đa cho phép (mặc định 03 lần, có thể cấu hình), MSCD phải tạm khóa chức năng xác thực trong một khoảng thời gian tối thiểu quy định (hoặc yêu cầu quy trình mở khóa qua kênh khác) nhằm phòng chống tấn công dò đăng nhập tự động (brute-force).
- MSCD-18: MSCA và MSCD phải áp dụng cơ chế quản lý phiên an toàn, bao gồm: (i) thiết lập thời gian timeout khi không có hoạt động và tự động khóa/đăng xuất khi hết thời gian; (ii) xóa an toàn dữ liệu SAD khỏi bộ nhớ khi kết thúc phiên; (iii) buộc xác thực lại khi bắt đầu phiên mới hoặc sau khi hết timeout.

6.4.3 Thành phần tạo chữ ký (SCC)

Các yêu cầu sau đây nhằm đối phó với các mối đe dọa về việc sử dụng thuật toán không phù hợp và việc tạo chữ ký trái phép:

- MSCD-19: Thành phần tạo chữ ký (SCC) phải yêu cầu chủ thể ký được xác thực thành công trước khi cho phép tạo chữ ký hoặc thực hiện bất kỳ hành động nào khác theo phân quyền.
- MSCD-20: Thành phần tạo chữ ký (SCC) phải đảm bảo rằng chỉ người dùng có vai trò là chủ thể ký mới có thể ký DTBSR.
- MSCD-21: Thành phần tạo chữ ký (SCC) phải thực hiện việc tạo chữ ký theo các thuật toán mật mã và độ dài khóa mật mã đã được quy định, được cho phép bởi các thuật toán và tham số được phê duyệt cho ký số trên thiết bị di động. Danh mục thuật toán mật mã và độ dài khóa tối thiểu được chấp nhận phải được quy định cụ thể tại Phụ lục A của tiêu chuẩn này; không sử dụng các thuật toán/độ dài khóa đã bị khuyến cáo loại bỏ.
- MSCD-22: Thành phần tạo chữ ký (SCC) phải có khả năng hủy dữ liệu tạo chữ ký (SCD) theo yêu cầu của chủ thể ký hoặc quản trị viên, phù hợp với phương pháp hủy khóa đã được quy định.

7 Hồ sơ chữ ký số trên thiết bị di động

7.1 Cơ sở lý luận

Như đã mô tả trong phần 6 của tiêu chuẩn này, có thể có nhiều cách thức triển khai dịch vụ ký số trên thiết bị di động khác nhau nhưng vẫn cung cấp cùng một mức độ bảo mật. Dưới góc độ bảo mật, câu hỏi quan trọng nhất không phải là các chức năng bảo mật được liên kết vào thành phần nào của hệ thống. Quan trọng hơn là liệu tất cả các chức năng bảo mật được xác định trong phần 6 có

được thiết lập đầy đủ hay không. Hơn nữa, cách thức thực hiện các chức năng bảo mật đó cũng là một vấn đề cần lưu ý.

Bên cạnh bản thân MSCS, cần phải tính đến môi trường của hệ thống và các khía cạnh vận hành. Một phần của môi trường này là CSP. Việc thực thi của CSP thiếu đảm bảo có thể dẫn đến sự suy giảm độ tin cậy của ký số trên thiết bị di động. Điều này cũng có thể xuất phát từ việc nhân viên của các CSP không tuân thủ các chính sách bảo mật tổ chức.

Các loại hình ký số trên thiết bị di động được sắp xếp một cách tương đối theo cấp độ bảo mật tăng dần. Khi so sánh hai trường hợp ký số trên thiết bị di động không phải lúc nào cũng rõ ràng đâu là chữ ký có cấp độ cao hơn. Do đó, không thể xác định một thứ tự rõ ràng ký số trên thiết bị di động. Điều này càng làm cho việc xác định các cấp độ phù hợp trở nên khó khăn hơn.

Tuy nhiên, trong một môi trường khép kín, nơi tất cả các tác nhân đều có thỏa thuận hợp tác với nhau, một tập hợp các quy tắc có thể được thiết lập để xác định thứ tự cho các hồ sơ chữ ký số trên thiết bị di động khác nhau.

7.2 Khung cấu trúc

Dựa trên các phân tích về bảo mật đã thực hiện tại khoản 6 và các cơ sở lý luận nêu trên, chúng ta có thể kết luận rằng mặc dù việc xác định một tiêu chuẩn khách quan để xếp hạng các Hồ sơ ký số trên thiết bị di động là rất khó khăn, nhưng hoàn toàn có thể thiết lập một khung cấu trúc cho các hồ sơ chữ ký số trên thiết bị di động này.

Dưới đây là danh sách các thông tin cần thiết của khung cấu trúc dành cho bộ cấu hình cho hệ thống chữ ký trên di động:

Đăng ký và chứng thực:

- Đăng ký: Trực tiếp hoặc từ xa, mức độ tin cậy của thông tin, định nghĩa về danh tính.
- Chứng thực: Quy chế chứng thực; Chính sách chứng thư; Quản lý và sử dụng danh tính.

Hệ thống ký số trên thiết bị di động:

- Các quy tắc xử lý ký số trên thiết bị di động:
    - Chính sách chữ ký
    - Bên tin tưởng (RP) cần phải chắc chắn rằng chính sách mà chủ thể ký áp dụng là phù hợp với các nhu cầu kinh doanh cụ thể của họ. Chủ thể ký được yêu cầu “cung cấp thông báo về các điều kiện ký kết áp dụng cho mỗi giao dịch với đối tác kinh doanh của mình”.
    - Chính sách chữ ký phải bao gồm các quy trình quản lý đối với các điều kiện ký kết và các quy tắc kỹ thuật, ví dụ như:
        - Quản lý và sử dụng định danh cũng như thuộc tính của chứng thư
        - Chứng thư đủ điều kiện hoặc không đủ điều kiện
        - Quy trình tạo chữ ký
        - Thuật toán và độ dài khóa
- Biện pháp bảo vệ kỹ thuật cho MSCS:

- Yêu cầu bảo mật chung:
  + Yêu cầu đối với dữ liệu cần ký (DTBS)
  + Yêu cầu về kênh truyền tin cậy (Trusted channel)
  + Yêu cầu phát sinh từ các tiến trình và cổng giao tiếp không tin cậy
  + Kiểm soát đầu vào.
- MSCA:
  - Sự công nhận hoặc tuyên bố tuân thủ
  - Yêu cầu đối với từng thành phần:
    + Thành phần trình bày tài liệu của chủ thể ký (SDP)
    + Trình xem thuộc tính chữ ký (SAV)
    + Thành phần tương tác chủ thể ký (SIC)
    + Thành phần xác thực chủ thể ký (SAC)
    + Bộ giao tiếp MSCD/MSCA (DAC)
    + Bộ giao tiếp MSSP/MSCA (PAC)
- MSSP:
  - Sự công nhận hoặc tuyên bố tuân thủ
  - Yêu cầu đối với từng thành phần:
    + Thành phần xác minh dữ liệu cần ký (DTBSV)
    + Thành phần định dạng dữ liệu cần ký (DTBSF)
    + Thành phần băm dữ liệu (DHC)
    + Thành phần đối tượng dữ liệu chủ thể ký (SDOC)
    + Thành phần ghi nhật ký chữ ký (SLC)
    + Tương tác với nhà cung cấp dịch vụ chứng thực (CSPC)
    + Bộ giao tiếp MSSP/MSCA (PAC)
    + Bộ giao tiếp MSSP/AP (PPC)
- MSCD
  - Sự công nhận hoặc tuyên bố tuân thủ
  - Yêu cầu đối với từng thành phần:
    + Thành phần xác thực người dùng (UAC)
    + Thành phần tạo chữ ký (SCC)

Một số thông tin đã được quy định bởi các tổ chức tiêu chuẩn hóa khác, chẳng hạn như nhóm ESI đối với các chính sách chữ ký.

7.3 XML Schema

Tương tự như lược đồ XML được ESI quy định cho các chính sách chữ ký, một XML Schema dành cho hồ sơ chữ ký số trên thiết bị di động cũng có thể được thiết lập. Trong tiêu chuẩn này, chúng tôi chỉ tập trung vào phần biện pháp kỹ thuật bảo mật của hồ sơ chữ ký số trên thiết bị di động trên di động. Trên phương diện đó, chúng tôi đề xuất sử dụng XML Schema sau đây:

```
<xs:schema
    targetNamespace="http://uri.etsi.org/2000/v1.00#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:mss="http://uri.etsi.org/2000/v1.00#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="qualified"
>
    <xs:complexType name="technicalComponent_Type">
    <annotation>
        This is a generic description of the protection features of a technical component.
    </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
                <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSCA_Type">
        <annotation>
            This is a generic description of the protection features of a Mobile Signature Creation Application.
                SDP : Signer's Document Presentation
                SAV : Signature Attribute Viewer
                SIC : Signer Interaction
                SAC : Signer's Authentication
                DAC : MSCD/MSCA Communicator
                PAC : MSSP/MSCA Communicator
            An example of a voluntary declaration of conformity for Signature Creation Applications can be found
            in CEN CWA 14172-4
        </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="SDP" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SAV" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SIC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="SAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSSP_Type">
        <annotation>
            This is a generic description of the protection features of a Mobile Signature Service Provider.
                DTBSV : Data to Be Signed Verifier
                DTBSF : Data To Be Signed Formatter
                DHC : Data Hashing Component
                SDOC : Signed Data Object Composer
                SLC : Signature Logging Component
```

```
            CSPC : CSP Interaction Component
            PAC : MSSP/MSCA Communicator
            PPC: MSSP/AP Communicator
        </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="DTBSV" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DTBSF" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="DHC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PPC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="PAC" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="MSCD_Type">
        <annotation>
            This is a generic description of the protection features of a Mobile Signature Creation Device.
        </annotation>
        <xs:sequence>
            <xs:element name="conformityDeclaration" type="xs:string" minOccurs="0"/>
            <xs:element name="Accreditation" type="xs:string" minOccurs="0"/>
            <xs:element name="userAuthentication" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:element name="signatureCreation" type="mss:technicalComponent_Type" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:complexType name="technicalProtection_Type">
        <annotation>
            This is a generic description of a Mobile Signature Service Technical Protection. This structure
            denotes the security analysis of clause 6. MSCS elememt denotes the overall security requirements
            for a MSCS. MSCA, MSSP and MSCD are used to go further in the description of the security features
            of a MSCS.
        </annotation>
        <xs:sequence>
            <xs:element name="MSCA" type="mss:MSCA_Type"/>
            <xs:element name="MSSP" type="mss:MSSP_Type"/>
            <xs:element name="MSCD" type="mss:MSCD_Type"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional" />
    </xs:complexType>

    <xs:element name="MSS_Profile" type="mss:ProfileType"/>
        <annotation>
            This is a generic description of a Mobile Signature Profile. As we focus only on the technical
            protection aspect, this is the only element we mention. However, extensions can be added thanks to
            the "any" element.
        </annotation>
        <xs:complexType name="ProfileType">
```

```
            <xs:sequence>
                <xs:element name="MSS_technicalProtection" type="mss:technicalProtection_Type"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
```

7.3.1 Ví dụ 1

Đây là mô tả về một dịch vụ ký số trên thiết bị di động truyền thống tương tự như các hệ thống đã được triển khai thực tế trên thế giới:

- MSCD: Sử dụng Thẻ SIM tích hợp ứng dụng SIM Toolkit và thuật toán mã hóa công khai (PKI). Thiết bị này đạt chứng nhận tiêu chuẩn ISO EAL 4+ dựa trên hồ sơ dành cho thiết bị tạo chữ ký an toàn loại 3.

- Nhà cung cấp dịch vụ chữ ký số trên thiết bị di động (MSSP): Là hệ thống máy chủ có khả năng triển khai đầy đủ tất cả các tính năng bảo mật.

- MSCA: Sử dụng chính điện thoại di động có hỗ trợ chuẩn SIM Toolkit.

- Giao tiếp giữa ứng dụng tạo chữ ký số trên thiết bị di động (SCA) và nhà cung cấp dịch vụ chữ ký số trên thiết bị di động (MSSP): Được thực hiện qua kênh SMS kết hợp với các tính năng bảo mật của tiêu chuẩn TS 101 181 bao gồm: mã hóa, kiểm tra lỗi và kiểm soát dư thừa.

- Giao tiếp giữa nhà cung cấp dịch vụ chữ ký số trên thiết bị di động (MSSP) và AP: Được thực hiện qua giao thức HTTP kết hợp với SSL/TLS.

```
<MSS_Profile>
    <MSS_technicalProtection>
        <MSCA>
            <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSCA>
        <MSSP>
            <DTBS Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSV />
            <DTBSF Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSF />
            <DHC Profile=http://uri.etsi.org/TS102206/v1.1.3#DHC />
            <PPC Profile=http://uri.etsi.org/TS102206/v1.1.3#PPC />
            <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSSP>
        <MSCD Profile= http://uri.etsi.org/TS102206/v1.1.3#MSCD >
            <Accreditation>
                CC EAL4+ PP - Secure Signature-Creation Device Type 3 Version 1.05
            </Accreditation>
        </MSCD>
    </MSS_technicalProtection>
    ...
</MSS_Profile>
```

7.3.2 Ví dụ 2

Dưới đây là mô tả về một dịch vụ ký số trên thiết bị di động tự tuyên bố tuân thủ các quy định của Chỉ thị EU về chữ ký điện tử đủ điều kiện

```
<MSS_Profile>
    <MSS_technicalProtection Profile=http://uri.etsi.org/TS102206/v1.1.3#MSCS >
        <MSCA>
            <conformityDeclaration>
                Manufacturer's Declaration of conformity for a Signature Creation Application
                We "manufacturer's name" of "manufacturer's address" do hereby declare under our sole
                responsibility...
            </conformityDeclaration>
        </MSCA>
        <MSSP>
            <DTBS Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSV />
            <DTBSF Profile=http://uri.etsi.org/TS102206/v1.1.3#DTBSF />
            <DHC Profile=http://uri.etsi.org/TS102206/v1.1.3#DHC />
            <PPC Profile=http://uri.etsi.org/TS102206/v1.1.3#PPC />
            <PAC Profile=http://uri.etsi.org/TS102206/v1.1.3#PAC />
        </MSSP>
        <MSCD>
            <Accreditation>
                CC EAL4+ PP - Secure Signature-Creation Device Type 3 Version 1.05
            </Accreditation>
        </MSCD>
    </MSS_technicalProtection>
    ...
</MSS_Profile>
```

Phụ lục A. Yêu cầu về thuật toán mật mã và độ dài khóa

A.1 Thuật toán băm

- Bắt buộc sử dụng thuật toán băm thuộc họ SHA-2 (SHA-256, SHA-384, SHA-512) hoặc SHA-3.
- Nghiêm cấm sử dụng thuật toán SHA-1 và MD5 do không còn bảo đảm an toàn.

A.2 Thuật toán khóa công khai

- RSA: độ dài khóa tối thiểu 2048 bit; khuyến nghị sử dụng độ dài khóa từ 3072 bit trở lên đối với các hồ sơ triển khai mới.
- Đường cong Elliptic (ECC): sử dụng thuật toán ECDSA hoặc EdDSA trên các đường cong tiêu chuẩn NIST P-256 hoặc P-384.

Thư mục tài liệu tham khảo

[1] Luật Giao dịch điện tử 2023: Quy định về giá trị pháp lý và phân loại chữ ký điện tử;

[2] Nghị định 23/2025/NĐ-CP: Quy định chi tiết về chữ ký điện tử và dịch vụ tin cậy.

[3] ETSI TR 102 203 V1.1.1 (2003-05) Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements

[4] ETSI TS 102 204 V1.1.4 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface

[5] ETSI TS 102 207 V1.1.3 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services

[6] ISO/IEC 27001:2022: “Information security, cybersecurity and privacy protection – Information security management systems – Requirements”.