TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU VỀ GIAO DIỆN WEB CHO MÔ HÌNH KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG (MOBILE PKI)

Electronic transactions – Web interface requirements for mobile signature service model (Mobile PKI)

DỰ THẢO THẨM ĐỊNH

HÀ NỘI – 2026

Nội dung **Trang**

Lời nói đầu

TCVN xxxxx:2026 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 những năm gần đây, việc tích hợp chữ ký số vào các ứng dụng và cổng dịch vụ trực tuyến đã trở thành xu hướng tất yếu trong tiến trình chuyển đổi số quốc gia. Đặc biệt, sự phát triển mạnh mẽ của mô hình ký số trên thiết bị di động (Mobile PKI) đã mở ra khả năng thực hiện ký số trực tiếp từ trình duyệt web trên các thiết bị di động - không đòi hỏi cài đặt plugin, phần mềm chuyên dụng hay thiết bị ngoại vi bổ sung. Mô hình này không chỉ nâng cao trải nghiệm người dùng mà còn góp phần mở rộng phạm vi ứng dụng chữ ký số trong các giao dịch hành chính công, thương mại điện tử và dịch vụ tài chính số.

Tuy nhiên, giao diện Web là điểm tiếp xúc trực tiếp giữa người dùng với toàn bộ hạ tầng Mobile PKI, do đó đây cũng là lớp dễ bị tổn thương nếu không được thiết kế và triển khai theo các yêu cầu kỹ thuật chặt chẽ. Những nguy cơ có thể trực tiếp xâm phạm tính xác thực, tính toàn vẹn và tính không thể phủ nhận của chữ ký số - các thuộc tính pháp lý cốt lõi mà pháp luật Việt Nam yêu cầu bảo đảm.

Bên cạnh yếu tố bảo mật, giao diện Web trong mô hình Mobile PKI còn phải đáp ứng đồng thời các yêu cầu về khả năng tương thích đa nền tảng, tính nhất quán trong quy trình xác nhận hành vi ký, khả năng hiển thị rõ ràng nội dung tài liệu cần ký, cũng như tính khả dụng đối với người dùng có trình độ công nghệ khác nhau. Những yêu cầu này hiện chưa được chuẩn hóa một cách thống nhất tại Việt Nam, dẫn đến sự không đồng đều về chất lượng triển khai giữa các nhà cung cấp dịch vụ và ứng dụng tích hợp chữ ký số.

Tiêu chuẩn này được xây dựng nhằm lấp đầy khoảng trống nêu trên, cung cấp một bộ yêu cầu kỹ thuật toàn diện và thống nhất về giao diện web áp dụng trong mô hình Mobile PKI. Đồng thời, tiêu chuẩn này được xây dựng bảo đảm phù hợp với khuôn khổ pháp lý về chữ ký điện tử và dịch vụ tin cậy của 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.

Giao dịch điện tử - Yêu cầu về giao diện Web cho mô hình ký số trên thiết bị di động (Mobile PKI)

Electronic transactions – Web interface requirements for mobile signature service model (Mobile PKI)

1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng đối với các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng; các đơn vị phát triển cổng dịch vụ công trực tuyến, ứng dụng thương mại điện tử và dịch vụ tài chính số có tích hợp chức năng ký số; các nhà phát triển thư viện và bộ công cụ hỗ trợ tích hợp Mobile PKI vào ứng dụng web; cũng như các cơ quan quản lý nhà nước trong lĩnh vực giao dịch điện tử, chữ ký số và an toàn thông tin mạng.

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

CHÚ THÍCH: ETSI TS 102 204 V1.1.4 (2003-08) được sử dụng làm nền tảng kỹ thuật để bảo đảm tính liên thông với các hệ thống MSSP/CA hiện đang triển khai theo mô hình này tại Việt Nam. Các yêu cầu cụ thể về mật mã, giao thức truyền tải và mô hình thiết bị trong tiêu chuẩn này được rà soát, cập nhật cho phù hợp với công nghệ hiện hành.

3 Thuật ngữ và chữ viết tắt

3.1 Thuật ngữ

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

Ứng dụng phụ thuộc (dependent application)

Là ứng dụng yêu cầu người dùng phải có ký số trên thiết bị di động để hoàn tất các thao tác giao dịch. Nếu không có ký số, ứng dụng có thể không hoạt động chính xác.

3.1.3

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]

3.1.4

Người dùng cuối (end-user)

Người dùng sở hữu thiết bị di động được liên kết với chữ ký trên thiết bị di động.

CHÚ THÍCH: Người dùng cuối là thuật ngữ kỹ thuật kế thừa từ khung MSS quốc tế (ETSI), chỉ vai trò của cá nhân sở hữu và sử dụng thiết bị di động trong giao thức ký số. Khi người dùng cuối thực hiện hành vi ký số, thuật ngữ pháp lý tương ứng theo Luật Giao dịch điện tử 2023 là chủ thể ký (3.1.3); trường hợp người dùng cuối là thuê bao đăng ký dịch vụ với nhà mạng di động, có thể được gọi là thuê bao theo pháp luật viễn thông. Tiêu chuẩn này sử dụng thống nhất thuật ngữ người dùng cuối ở mức độ kỹ thuật để bảo đảm nhất quán với các vai trò khác trong khung MSS (AP, RP, MSSP); việc áp dụng thuật ngữ pháp lý cụ thể (chủ thể ký, thuê bao) tùy thuộc vào ngữ cảnh pháp lý của từng giao dịch.

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

Quy trình ký số trên thiết bị di động (mobile signature process)

Trình tự logic của việc thu thập và sử dụng chữ ký số trên thiết di động.

3.1.7

Hồ sơ chữ ký số trên thiết bị di động (mobile signature profile)

Lưu trữ các thông tin mã hóa bảo mật, được liên kết trực tiếp với SIM điện thoại hoặc ứng dụng xác thực.

3.1.8

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.

3.1.9

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.

3.1.10

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.

3.1.11

Chuyển vùng giao dịch (transaction roaming)

Giao dịch mà người dùng cuối có thể sử dụng ứng dụng phụ thuộc từ AP phù hợp với mạng được truy cập

3.1.12

Dịch vụ giá trị gia tăng (value added service)

Những tiện ích bổ sung được cung cấp bởi MSSP ngoài ký số trên thiết bị di động

3.2 Chữ viết tắt

AP	Application Provider	Bên cung cấp ứng dụng
CA	Certification Authority	Tổ chức cung cấp dịch vụ chứng thực
CMS	Cryptographic Message Syntax	Cú pháp thông điệp mật mã
CRL	Certificate Revocation List	Danh sách chứng thư bị thu hồi
EESSI	European Electronic Signature Standardisation Initiative	Sáng kiến Tiêu chuẩn chữ ký điện tử Châu Âu
HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản
MNO	Mobile Network Operator	Nhà mạng di động
MSISDN	Mobile Station International Subscriber Directory Number	Số điện thoại di động của người dùng cuối
MSS	Mobile Signature Service	Dịch vụ 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
PIN	Personal Identification Number	Số nhận dạng cá nhân
RA	Registration Authority	Tổ chức đăng ký
RP	Relying Party	Bên tin tưởng
RPC	Remote Procedure Call	Gọi thủ tục từ xa
SMS	Short Message Service	Dịch vụ thông điệp ngắn
SOAP	Simple Object Access Protocol	Giao thức nhắn tin dựa trên XML
URI	Uniform Resource Identifier	Mã định danh tài nguyên thống nhất
WSDL	Web Service Description Language	Ngôn ngữ mô tả dịch vụ Web
XAdES	XML Advanced Electronic Signature	Chữ ký điện tử nâng cao XML
XML	extensible Markup Language	Ngôn ngữ đánh dấu có thể 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.

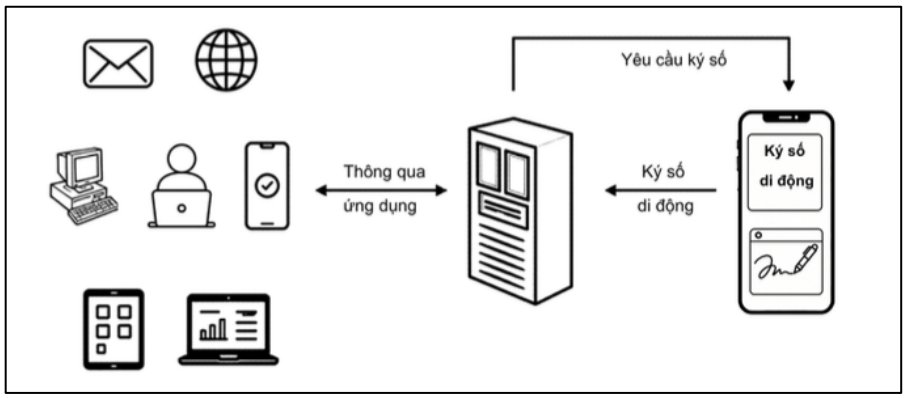
Giao dịch:

- 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.

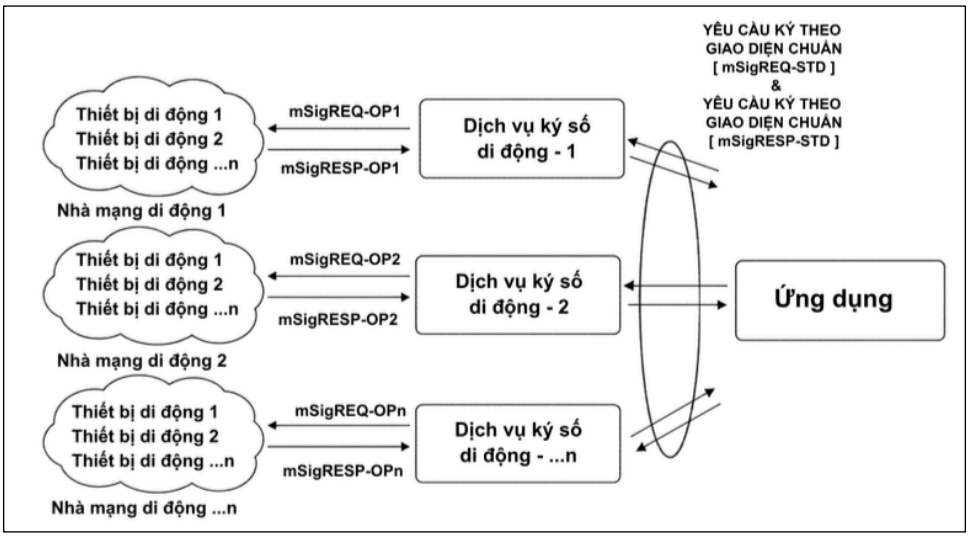
Khi xem xét việc sử dụng chữ ký trên thiết bị di động, chúng ta chỉ tập trung vào quy trình khởi tạo một chữ ký điện tử liên quan đến thông điệp được hiển thị cho người dùng cuối. Quy trình này loại trừ cụ thể việc kiểm soát ở cấp độ ứng dụng đối với thông điệp đã ký. Việc cung cấp một chữ ký trên thiết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

http://uri.etsi.org/TS102204/v1.1.2#

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/TS102204/v1.1.2#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:xenc="http://www.w3.org /2001/04/xmlenc#"
        xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:env=http://www.w3.org/2003/05/soap-envelopeelementFormDefault="qualified"
>
```

Điều này có nghĩa rằng tiền tố ‘ds’ được sử dụng trong toàn bộ tiêu chuẩn để biểu thị không gian tên của đặc tả W3C XML-Signature. Tiền tố ‘xs’ biểu thị không gian tên của đặc tả XML-Schema, tiền tố ‘xenc’ biểu thị không gian tên của khuyến nghị về XML Encryption và tiền tố ‘env’ biểu thị không gian tên của đặc tả SOAP 1.2. Tiền tố ‘mss’ được sử dụng để biểu thị không gian tên của MSS.

5 Chức năng của dịch vụ ký số trên thiết bị di động (MSS)

Mục đích của điều mục này là mô tả các chức năng cao cấp do MSSP cung cấp. Các chức năng này sẽ giúp xác định các phương pháp khác nhau mà dịch vụ Web ký số trên thiết bị di động cần phải triển khai.

5.1 Ký số trên thiết bị di động

MSSP phải hỗ trợ chức năng này, được sử dụng cho hai mục đích sau:

- Bất kỳ thực thể nào nhận chữ ký trên thiết bị di động từ người dùng cuối đối với nội dung văn bản có thể hiển thị. Văn bản ký được hiện thị trên thiết bị di động của người dùng cuối.
- Bất kỳ thực thể nào lấy chữ ký trên thiết bị di động từ người dùng cuối đối với dữ liệu đặc biệt và không thể hiển thị. Văn bản phải được hiện thị cho người dùng cuối để họ hiểu điều gì đang xảy ra.

MSSP có thể sử dụng các phương pháp triển khai kỹ thuật khác nhau trên mạng di động, trên nền tảng nhà cung cấp dịch vụ MSSP và trên thiết bị di động. Điều này dẫn đến 02 điểm sau:

- Hồ sơ chữ ký số trên thiết bị di động;
- Các chế độ truyền thông điệp dữ liệu trong dịch vụ ký số trên thiết bị di động.

5.1.1 Hồ sơ chữ ký số trên thiết bị di động

Nếu người dùng cuối không có cùng khả năng ký số, thì AP sẽ không nhận được cùng một chất lượng ký số trên thiết bị di động đồng nhất cho người dùng cuối cụ thể. MSSP có thể sử dụng các khả năng ký số trên thiết bị di động khác nhau của người dùng cuối, nhưng họ phải chỉ ra một loại chất lượng ký số nào đó cho AP, điều này gọi là hồ sơ chữ ký số trên thiết bị di động

Khi AP nhận hồ sơ chữ ký số trên thiết bị di động từ MSSP, nó phải có khả năng hỏi yêu cầu ký số trên thiết bị di động. Bản thân hồ sơ chữ ký số trên thiết bị di động không bao gồm thông điệp, thay vào đó là URI trỏ đến hồ sơ chữ ký số trên thiết bị di động.

Hồ sơ chữ ký số trên thiết bị di động được mô tả theo phương thức mà cả hai bên thống nhất; mỗi bên có thể tự định nghĩa URI riêng:

- Thông tin về giai đoạn đăng ký và cấp chứng thư như là: Gặp mặt trực tiếp hoặc từ xa; Cấp độ xác thực; Cấp giấy tờ tùy thân; Cấp khóa.
- Thông tin về hệ thống ký số trên thiết bị di động như là: Chính sách ký số; Mô tả về cơ chế kỹ thuật bảo vệ ký số trên thiết bị di động bao gồm thiết bị tạo ký số trên thiết bị di động, nền tảng ứng dụng tạo ký số trên thiết bị di động và MSSP.

5.1.2 Chế độ thông điệp ký số trên thiết bị di động

Đa số các trường hợp, MSSP phải gửi thông tin đến thiết bị di động của người dùng cuối để nhằm mục đích ít nhất là nhận được xác nhận từ người dùng cuối. Trong vài trường hợp, bước này có thể mất thời gian vì:

- Kết nối mạng kém tại vị trí người dùng cuối;
- Người dùng cuối chưa sẵn sàng xác nhận giao dịch;

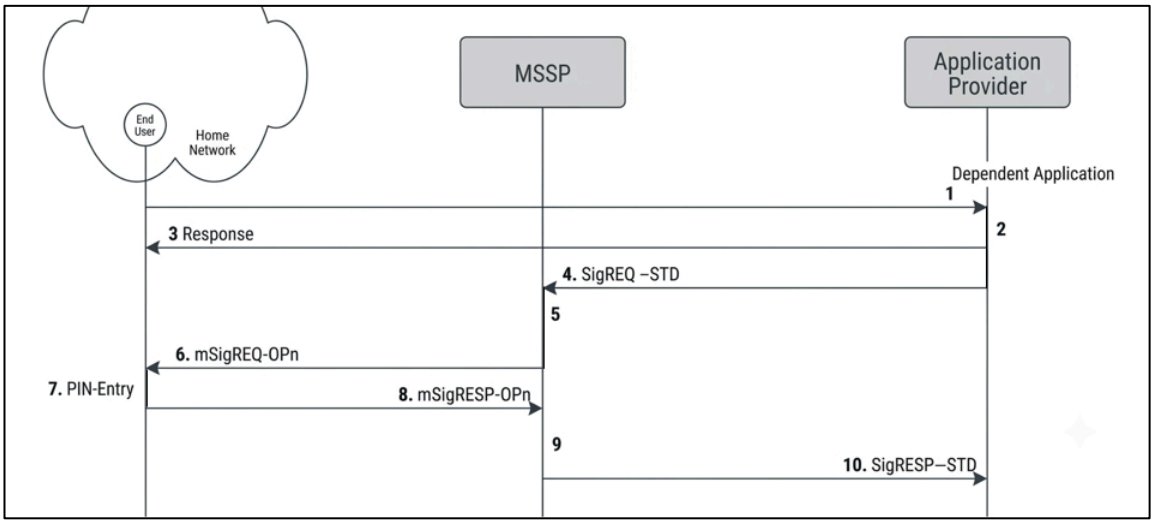
Vì những lý do này, MSSP có thể đang xử lý các giao dịch chưa hoàn tất ở chế độ “không đồng bộ”. Khi đó, RP sẽ bị treo. Việc nhận được ký số trên thiết bị di động trong một lần đối thoại yêu cầu - phản hồi duy nhất có thể không thuận tiện cho RP. Tại liệu này đề xuất rằng là MSSP PHẢI có khả năng sử dụng giao thức đa yêu cầu - phản hồi để xử lý hành vi không đồng bộ này.

Tiêu chuẩn này nghiên cứu cả chế độ đồng bộ và không đồng bộ vì RP không có những ràng buộc và nhu cầu. Có thể kịch bản chức năng khác nhau. Tuy nhiên, MSSP phải hỗ trợ tất cả chế độ.

Việc lựa chọn chế độ xử lý giao dịch thuộc về AP.

5.1.2.1 Chế độ đồng bộ

Chế độ này dựa trên hệ thống thông điệp một chiều. RP chỉ có thể liên hệ với MSSP. Trong trường hợp đó, chúng ta coi MSSP như là dịch vụ WEB cung cấp phương thức được gọi là "Phương pháp ký số trên thiết bị di động". Chỉ có một kết nối duy nhất cho việc kết hoạt phương thức này.



Hình 3. Phương pháp ký số trên thiết bị di động - Chế độ đồng bộ.

Các bước thực hiện được mô tả dưới đây:

1) Người dùng cuối - xác nhận yêu cầu giao dịch hoặc muốn truy cập vào dịch vụ;

2) AP - xử lý yêu cầu của người dùng cuối; khởi tạo dữ liệu;

3) AP - thông báo người dùng cuối thông qua kênh ứng dụng (vd: internet) rằng họ sắp gọi tới ứng dụng ký số trên thiết bị di động để xác nhận giao dịch;

4) AP - yêu cầu ký số tiêu chuẩn [SigREQ-STD] đến phương thức ký số trên thiết bị di động MSSP.

5) MSSP - xử lý [SigREQ-STD] từ AP; đánh giá tuyến đường thu nhận tín hiệu tốt nhất;

6) MSSP gửi yêu cầu ký số trên thiết bị di động đến người dùng cuối;

7) Người dùng cuối - thiết bị di động thể hiện văn bản cần được ký và ký số sau khi xác nhận;

8) Thiết bị di động trả về phản hồi ký số trên thiết bị di động cho MSSP;

9) MSSP xử lý phản hồi ký số;

10) MSSP truyền phản hồi phương thức ký số trên thiết bị di động [SigRESP-STD] trở lại AP có hoặc không có ký số.

Sau khi nhận được phản hồi ký số trên thiết bị di động, RP có thể gửi biên lai nhờ vào biên lai ký số trên thiết bị di động đã được mô tả trong Điều 5.5.

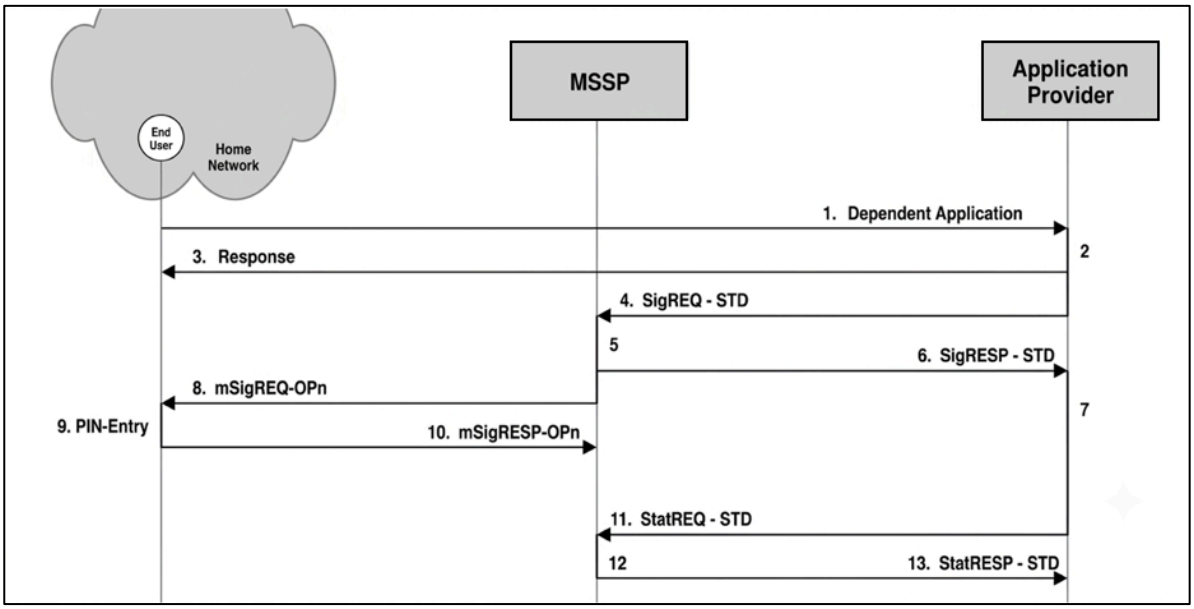
5.1.2.2 Chế độ máy khách không đồng bộ máy chủ

Trong trường hợp này, MSSP vẫn tiếp tục hoạt động trong hệ thống thông điệp một chiều; RP không thể liên lạc lại sau đó bởi MSSP. Vì vậy, MSSP sẽ chỉ xác nhận gọi đến "Phương thức ký số trên thiết bị di động" được mô tả ở trên và RP sẽ phải liên hệ với MSSP định kỳ để biết trạng thái của giao

dịch và có thể cả ký số. Bước cuối cùng là một phương pháp khác mà MSSP cung cấp, được gọi là "Phương thức truy vấn trạng thái ký số trên thiết bị di động".

Có ít nhất hai kết nối và RP là phía khởi tạo cả hai:

- Kết nối thứ nhất để kích hoạt phương pháp ký số trên thiết bị di động;
- Kết nối thứ hai để kích hoạt phương pháp trạng thái ký số trên thiết bị di động.



Hình 4. Phương pháp ký số trên thiết bị di động - Chế độ máy khách không đồng bộ máy chủ.

Các bước thực hiện được mô tả dưới đây:

1) Người dùng cuối - xác nhận yêu cầu giao dịch hoặc muốn truy cập và dịch vụ;

2) AP - xử lý yêu cầu của người dùng cuối; khởi tạo dữ liệu;

3) AP - thông báo người dùng cuối thông qua kênh ứng dụng rằng họ sắp gọi tới ứng dụng ký số trên thiết bị di động để xác nhận giao dịch;

4) AP - Yêu cầu ký số tiêu chuẩn [SigREQ-STD] đến phương thức ký số trên thiết bị di động MSSP.

5) MSSP - Xử lý [SigREQ-STD] từ AP; đánh giá tuyến đường thu nhận tín hiệu tốt nhất;

6) MSSP truyền phản hồi phương pháp ký số trên thiết bị di động [SigRESP-STD] trở lại AP với trạng thái cho thấy giao dịch đang xử lý;

7) AP theo dõi giao dịch;

8) MSSP - gửi yêu cầu ký số trên thiết bị di động đến người dùng cuối.

9) Người dùng cuối - thiết bị di động hiển thị văn bản cần ký và thực hiện ký số sau khi người dùng cuối xác nhận.

10) Thiết bị di động phản hồi ký số di động cho MSSP, đơn vị này sẽ xử lý phản hồi ký số.

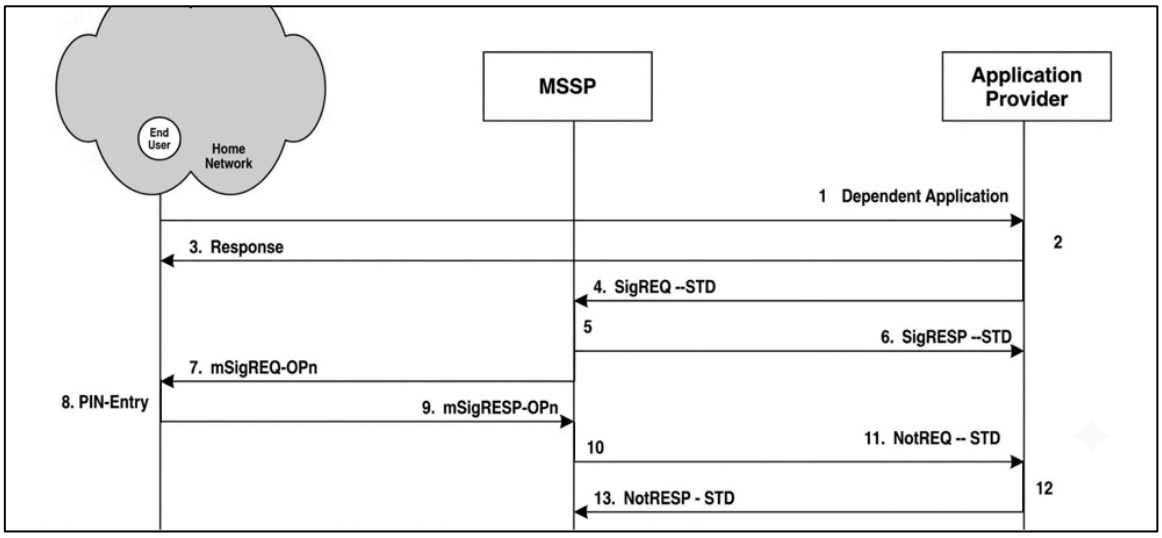
11) AP - Yêu cầu ký số tiêu chuẩn [SigREQ-STD] đến phương thức ký số trên thiết bị di động MSSP.

12-13) MSSP truyền phản hồi phương thức ký số trên thiết bị di động [SigRESP-STD] trở lại AP bao gồm trạng thái của giao dịch và có thể cả ký số trên thiết bị di động.

Sau khi nhận được phản hồi ký số trên thiết bị di động, RP có thể gửi biên lai nhờ vào biên lai ký số trên thiết bị di động đã được mô tả trong Điều 5.5.

5.1.2.3 Chế độ máy chủ không đồng bộ máy chủ

Trong trường hợp này, MSSP sẽ gửi thông báo ký số trên thiết bị di động cho RP khi ký số trên thiết bị di động sẵn sàng hoặc bị chấm dứt. Bên RP cần một "server" có khả năng để xử lý thông báo ký số trên thiết bị di động từ MSSP. Trong thực tế, bên RP sẽ cung cấp cho MSSP một "Phương pháp thông báo ký số trên thiết bị di động" mà MSSP có thể gọi. Có hai kết nối được thiết lập độc lập với nhau: kết nối đầu tiên gọi phương pháp ký số trên thiết bị di động (bởi AP) và kết nối thứ hai gọi phương pháp thông báo ký số trên thiết bị di động (bởi MSSP).



Hình 5. Phương pháp ký số trên thiết bị di động - Chế độ máy chủ không đồng bộ máy chủ.

Các bước thực hiện được mô tả dưới đây:

1) Người dùng cuối - xác nhận yêu cầu giao dịch hoặc muốn truy cập vào một dịch vụ;

2) AP - xử lý xác nhận của người dùng cuối; khởi tạo dữ liệu;

3) AP - thông báo người dùng cuối thông qua kênh ứng dụng rằng họ sắp gọi tới ứng dụng ký số trên thiết bị di động để xác nhận giao dịch;

4) AP - Yêu cầu ký số tiêu chuẩn [SigREQ-STD] đến phương thức ký số trên thiết bị di động MSSP.

5) MSSP - Xử lý [SigREQ-STD] từ AP; đánh giá tuyến đường thu nhận tín hiệu tốt nhất;

6) MSSP truyền phản hồi phương pháp ký số trên thiết bị di động [SigRESP-STD] trở lại AP với trạng thái cho thấy giao dịch đang xử lý;

7) MSSP - gửi yêu cầu mSign đến người dùng cuối;

8) Người dùng cuối - hiết bị di động hiển thị văn bản cần ký và thực hiện ký số sau khi người dùng cuối xác nhận..

9) Thiết bị di động trả về phản hồi ký số trên thiết bị di động cho MSSP;

10) MSSP xử lý phản hồi ký số;

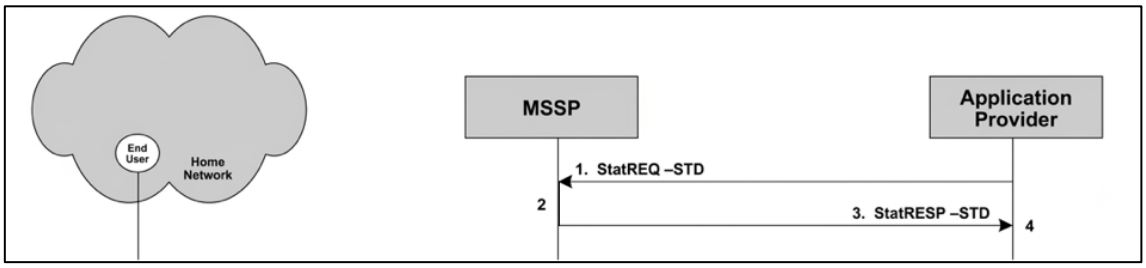
11) MSSP - gửi yêu cầu thông báo ký số trên thiết bị di động tiêu chuẩn [NotREQ-STD] đến phương pháp thông báo ký số trên thiết bị di động của AP.

12) AP xử lý thông báo của ký số;

13) AP chuyển phản hồi thông báo ký số trên thiết bị di động trở lại MSSP, có thể kèm theo biên lai cho người dùng cuối.

5.2 Truy vấn trạng thái ký số trên thiết bị di động

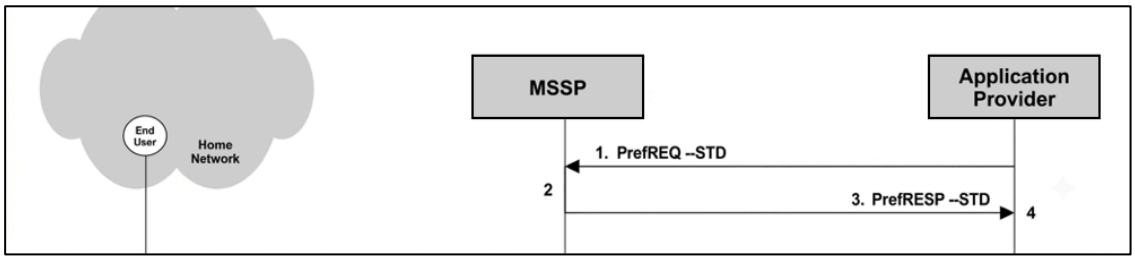
MSSP PHẢI hỗ trợ chức năng này, được AP sử dụng để lấy thông tin về giao dịch ký số trên thiết bị di động, dù đang trong quá trình xử lý hay đã hoàn tất. Điều này tương ứng với việc gọi "Phương thức truy vấn trạng thái ký số trên thiết bị di động".



Hình 6. Truy vấn trạng thái ký số trên thiết bị di động.

5.3 Truy vấn hồ sơ chữ ký số trên thiết bị di động

MSSP PHẢI hỗ trợ chức năng này, được AP sử dụng để lấy thông tin liên quan đến kiến trúc tổng thể tham gia vào quy trình ký số trên thiết bị di động. Thông thường, AP muốn lấy hồ sơ chữ ký số trên thiết bị di động trước khi yêu cầu ký số. Hồ sơ chữ ký số trên thiết bị di động sẽ được cung cấp dưới dạng URI. Chức năng này tương ứng với việc gọi "Phương thức truy vấn hồ sơ chữ ký số trên thiết bị di động".



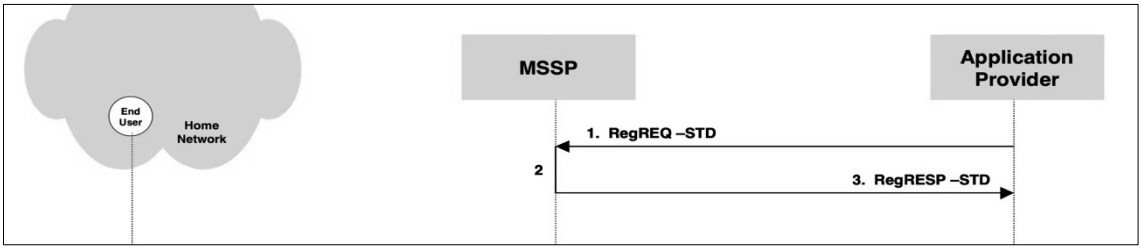
Hình 7. Truy vấn hồ sơ chữ ký số trên thiết bị di động.

5.4 Đăng ký ký số trên thiết bị di động

MSSP PHẢI hỗ trợ chức năng này. Bất kỳ AP nào đều sử dụng chức năng này để thông báo cho MSSP về người dùng cuối mới muốn đăng ký dịch vụ ký số trên thiết bị di động.

Một hành động tiếp theo của MSSP là tải xuống môt vài yếu tố bảo mật trong ứng dụng ký số trên thiết bị di động hoặc thậm chí kích hoạt chính ứng dụng ký số trên thiết bị di động. MSSP cũng có thể lấy thông tin từ thiết bị di động của người dùng cuối và phản hồi cho AP.

Chức năng này tương ứng với "Phương thức đăng ký ký số trên thiết bị di động".

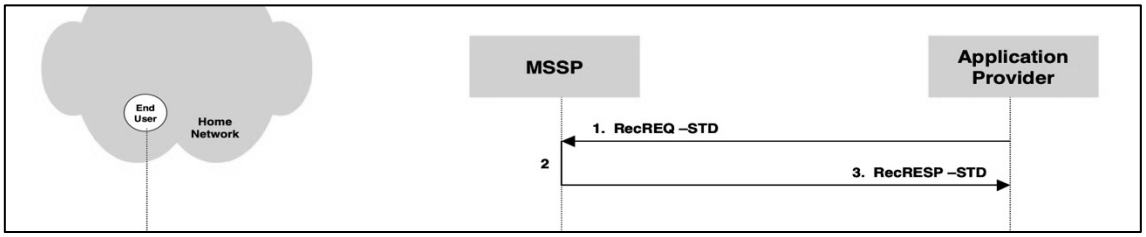


Hình 8. Đăng ký ký số trên thiết bị di động.

5.5 Biên lai ký số trên thiết bị di động

Phương pháp này là tùy chọn. AP sử dụng phương pháp này vào cuối giao dịch để cung cấp cho người dùng cuối kèm theo một biên lai nào đó thông báo cho người dùng cuối về quá trình giao dịch. Điều này tương ứng với việc kích hoạt "Phương thức biên lai ký số trên thiết bị di động".

Nội dung của biên lai sẽ khác nhau theo từng AP. Mỗi AP có các quy tắc riêng về việc xử lý biên lai. Tuy nhiên, giao diện này cho phép AP chèn văn bản/chữ ký số XML vào RecReq-STD.

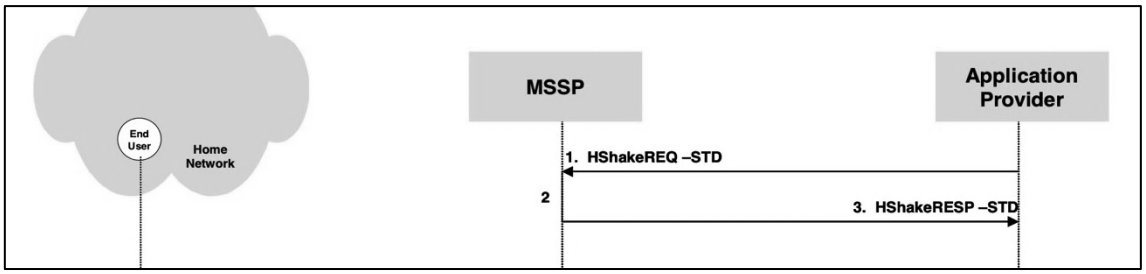


Hình 9. Biên nhận ký số trên thiết bị di động.

5.6 Bắt tay ký số trên thiết bị di động

MSSP PHẢI hỗ trợ chức năng này, nó được MSSP và AP sử dụng để thống nhất việc sử dụng chữ ký số XML trong quá trình giao tiếp. Điều 11 cung cấp mô tả và lý do sử dụng của chữ ký số XML trong các thông điệp được trao đổi giữa MSSP và AP. Chức năng này tương ứng với hai trường hợp thực tế:

- AP và MSSP không biết nhau, ví dụ trong trường hợp AP giao tiếp với MSSP gốc thông qua Mesh. Sau đó, cả hai bên đều muốn tìm hiểu khả năng của nhau.
- AP và MSSP có sự thỏa thuận thương mai trực tiếp và biết chính xác khả năng của nhau. Tuy nhiên, trong một vài trường hợp, AP hoặc MSSP muốn cải thiện bảo mật trong quá trình xử lý giao dịch bằng cách sử dụng chữ ký số XML, ví dụ khi có rủi ro về tài chính liên quan đến giao dịch.



Hình 10. Bắt tay ký số trên thiết bị di động.

6 Dịch vụ WEB ký số trên thiết bị di động

Dịch vụ ký số trên thiết bị di động được xác định là một dịch vụ WEB. Tất cả chức năng của MSSP được triển khai dựa trên mô hình trao đổi thông điệp yêu cầu - phản hồi đơn giản thông qua các phương pháp.

Các phương pháp được mô tả trong điều này một cách chính thức bằng ngôn ngữ mô tả dịch vụ WEB WSDL phiên bản 1.1, để tóm tắt thông tin được trình bày ở trên. Việc ràng buộc với giao thức mạng HTTP và SOAP 1.2.

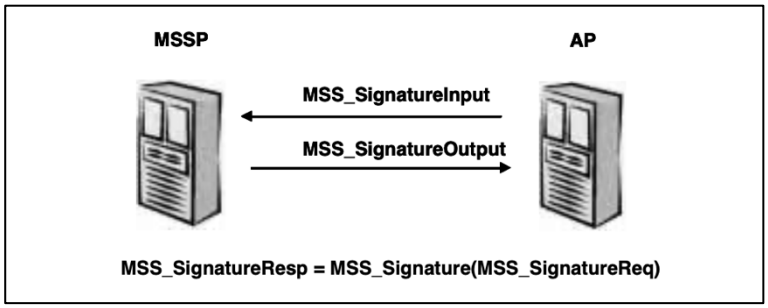
Các định nghĩa sau đây được áp dụng cho các định nghĩa lược đồ WSDL trong toàn bộ điều này:

```
<definitions
        xmlns="http://schemas.xmlsoap.org/wsdl/"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
        xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
        xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
        xmlns:tns="http://new.MSS_webservice.namespace"
        targetNamespace="http://new.MSS_webservice.namespace"
>
```

6.1 Phương thức ký số trên thiết bị di động

Thao tác WSDL có tên MSS_Signature bao gồm một WDSL thông điệp đầu vào và một thông điệp đầu ra. Thao tác này không có giá trị trả về. Thông điệp đầu vào WSDL đơn giản chỉ bao gồm một phần tử thuộc mss:MSS_SignatureReqType, trong khi thông điệp dữ liệu đầu ra WSDL bao gồm một phần tử thuộc

```
<message name="MSS_SignatureInput">
        <part name="MSS_SignatureReq" type="mss:MSS_SignatureReqType"/>
</message>
<message name="MSS_SignatureOutput">
        <part name="MSS_SignatureResp" type="mss:MSS_SignatureRespType"/>
</message>
<portType name="MSS_SignaturePortType">
        <operation name="MSS_Signature">
                <input message="tns:MSS_SignatureInput"/>
                <output message="tns:MSS_SignatureOutput"/>
        </operation>
</portType>
```



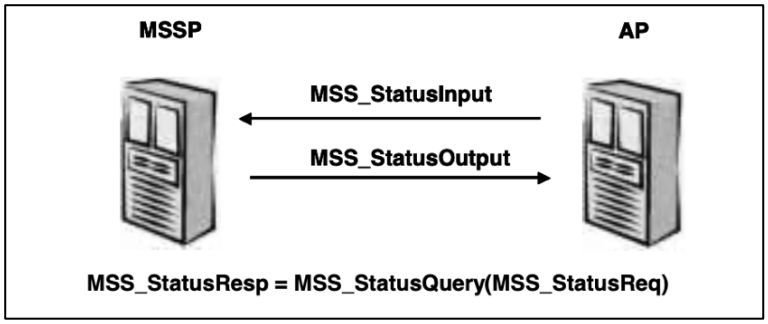
Hình 11. Phương thức ký số trên thiết bị di động - RPC Call.

Điều này có nghĩa là thông điệp MSS_SignatureReq đóng vai trò là tham số đầu vào của cuộc gọi thủ tục từ xa và thông điệp MSS_SignatureResp là tham số đầu ra tương ứng.

6.2 Phương thức truy vấn trạng thái ký số trên thiết bị di động

Thao tác MSS_Status có thể được mô tả chính xác theo cùng cách thao tác như MSS_Signature bằng cách sử dụng một phần tử thuộc mss:MSS_StatusReqType làm thành phần của thông điệp đầu vào và một phần tử thuộc kiểu mss:MSS_StatusRespType làm thành phần của thông điệp đầu ra.

```
<message name="MSS_StatusQueryInput">
        <part name="MSS_StatusReq" type="mss:MSS_StatusReqType"/>
</message>
        <message name="MSS_ StatusQueryOutput ">
        <part name="MSS_StatusResp" type="MSS_StatusRespType"/>
</message>

<portType name="MSS_StatusQueryType">
        <operation name="MSS_StatusQuery">
                <input message="tns:MSS_StatusQueryInput"/>
                <output message="tns:MSS_StatusQueryOutput"/>
        </operation>
</portType>
```

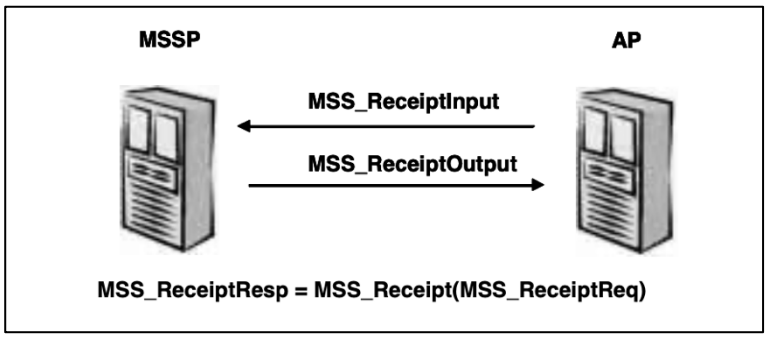


Hình 12. Truy vấn trạng thái ký số trên thiết bị di động - RPC Call.

6.3 Phương thức biên lai ký số trên thiết bị di động

Thao tác MSS_Receipt có thể được mô tả chính xác theo cùng cách thao tác như MSS_Signature bằng cách sử dụng một phần tử thuộc mss:MSS_ReceiptReqType làm thành phần của thông điệp đầu vào và một phần tử thuộc kiểu mss:MSS_ReceiptRespType làm thành phần của thông điệp đầu ra.

```
<message name="MSS_ ReceiptInput">
        <part name="MSS_ReceiptReq" type="MSS_ReceiptReqType"/>
</message>
<message name="MSS_ ReceiptOutput ">
        <part name="MSS_ReceiptResp" type="MSS_ReceiptRespType"/>
</message>

<portType name="MSS_ReceiptType">
        <operation name="MSS_Receipt">
                <input message="tns:MSS_ReceiptInput"/>
                <output message="tns:MSS_ReceiptOutput"/>
        </operation>
</portType>
```

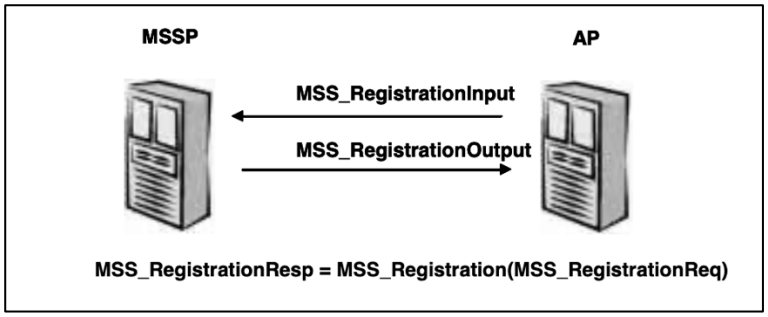


Hình 13. Mobile Signature Receipt - RPC Call.

6.4 Phương thức đăng ký ký số trên thiết bị di động

Thao tác MSS_Registration có thể được mô tả chính xác theo cùng cách thao tác như MSS_Signature bằng cách sử dụng một phần tử thuộc mss: MSS_RegistrationReqType làm thành phần của thông điệp đầu vào và một phần tử thuộc kiểu mss:MSS_RegistrationRespType làm thành phần của thông điệp đầu ra.

```
<message name="MSS_RegistrationInput">
        <part name="MSS_RegistrationReq" type="mss:MSS_RegistrationReqType"/>
</message>
        <message name="MSS_RegistrationOutput">
<part name="MSS_RegistrationResp" type="MSS_RegistrationRespType"/>
</message>

<portType name="MSS_RegistrationType">
        <operation name="MSS_Registration">
                <input message="tns:MSS_RegistrationInput"/>
                <output message="tns:MSS_RegistrationOutput"/>
        </operation>
</portType>
```



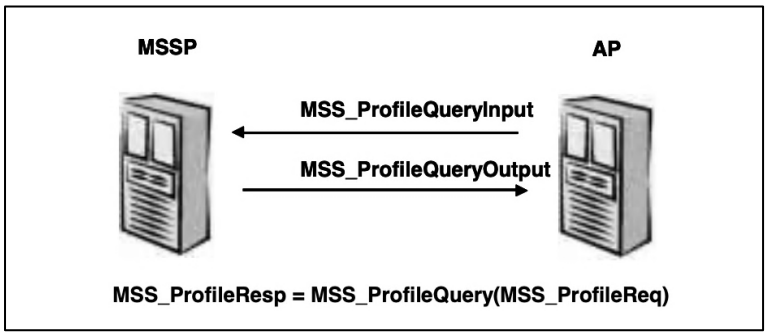
Hình 14. Đăng ký chữ ký trên thiết bị di động - RPC Call.

6.5 Phương thức truy vấn hồ sơ chữ ký số trên thiết bị di động

Thao tác MSS_Profile có thể được mô tả chính xác theo cùng cách thao tác như MSS_Signature bằng cách sử dụng một phần tử thuộc mss: MSS_ProfileReqType làm thành phần của thông điệp đầu vào và một phần tử thuộc kiểu mss:MSS_ProfileRespType làm thành phần của thông điệp đầu ra.

```
<message name="MSS_ProfileQueryInput">
        <part name="MSS_ProfileReq" type="mss:MSS_ProfileReqType"/>
</message>
        <message name="MSS_ ProfileQueryOutput ">
```

```
<part name="MSS_ProfileResp" type="MSS_ProfileRespType"/>
</message>

<portType name="MSS_ProfileQueryType">
        <operation name="MSS_ProfileQuery">
                <input message="tns:MSS_ProfileQueryInput"/>
                <output message="tns:MSS_ProfileQueryOutput"/>
        </operation>
</portType>
```

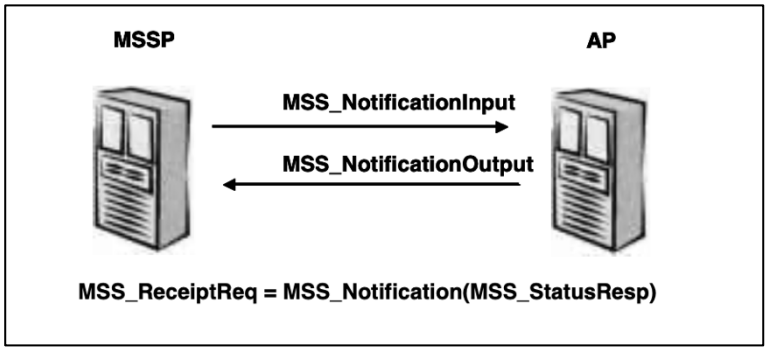


Hình 15. Truy vấn hồ sơ chữ ký số hồ sơ chữ ký số - RPC call.

6.6 Phương thức thông báo ký số trên thiết bị di động

Trong trường hợp thao tác MSS_Notification, thông điệp đầu vào của WSDL bao gồm một phần tử thuộc mss:MSS_StatusRespType, trong khi thông điệp đầu ra của WSDL bao gồm một phần tử thuộc kiểu mss:MSS_ReceiptReqType.

```
<message name="MSS_NotificationInput">
        <part name="MSS_StatusResp" type="mss:MSS_StatusRespType"/>
</message>
        <message name="MSS_NotificationOutput">
        <part name="MSS_ReceiptReq" type="mss:MSS_ReceiptReqType"/>
</message>

<portType name="MSS_NotificationPortType">
        <operation name="MSS_Notification">
                <input message="tns:MSS_NotificationInput"/>
                <output message="tns:MSS_NotificationOutput"/>
        </operation>
</portType>
```

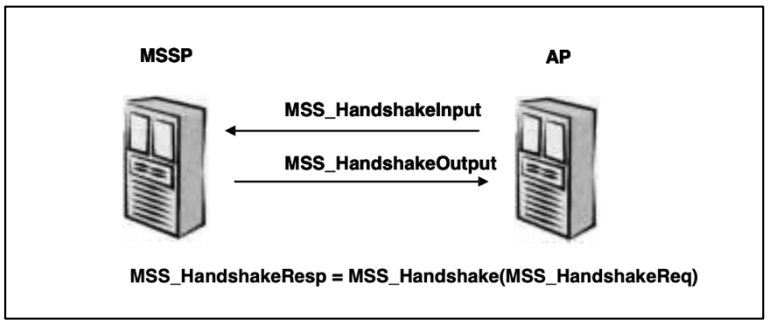


Hình 16. Mobile Signature notification - RPC Call.

6.7 Phương thức bắt tay ký số trên thiết bị di động

Thao tác MSS_Profile có thể được mô tả chính xác theo cùng cách thao tác như MSS_Signature bằng cách sử dụng một phần tử thuộc mss: MSS_HandshakeReqType làm thành phần của thông điệp đầu vào và một phần tử thuộc kiểu mss: MSS_HandshakeRespType làm thành phần của thông điệp đầu ra.

```
<message name="MSS_HandshakeInput">
        <part name="MSS_HandshakeReq" type="mss:MSS_HandshakeReqType"/>
</message>
        <message name="MSS_HandshakeOutput">
        <part name="MSS_HandshakeResp" type="mss:MSS_HandshakeRespType"/>
</message>

<portType name="MSS_HandshakePortType">
        <operation name="MSS_Handshake">
                <input message="tns:MSS_HandshakeInput"/>
                <output message="tns:MSS_HandshakeOutput"/>
        </operation>
</portType>
```



Hình 17. Bắt tay ký số trên thiết bị di động - RPC call.

7 Định dạng thông điệp

Trong phần này, các thông điệp trao đổi giữa AP và MSSP sẽ được trình bày. Các thông điệp này dựa trên các loại phụ trợ được mô tả trong phần 9.

7.1 Kiểu thông điệp trừu tượng

Kiểu trừu tượng này tập hợp tất cả các tham số sẽ được chứa một cách có hệ thống trong tất cả các thông điệp MSS. Các tham số sau đây chỉ liên quan đến giao thức.

Tên		Định dạng	Mô tả	Bắt buộc
MajorVersion		Integer	Phiên bản chính của giao diện, hiện tại là 1.	Có
MinorVersion		Integer	Phiên bản nhỏ hơn của giao diện, hiện tại là 1.	Có
AP_Info	_ID	anyURI	Mã định danh này được cấp cho AP trong quá trình đăng ký dịch vụ ký số trên thiết bị di động. Tất cả các AP, bao gồm cả MSSP, đều được xác định bằng mã định danh dựa trên URI.	Có
	AP_TransID	NCName	Mã số giao dịch được tạo bởi bộ công cụ AP cho một giao dịch mới. AP điền tham số này vào các yêu cầu của mình. Trong các thông điệp gửi từ MSSP, MSSP sử dụng tham số này để chỉ định cho AP biết giao dịch nào đã được xử lý	Có

	AP_PWD	String	Mật mã của AP, khi AP đăng ký với vai trò là bên dựa vào MSS, AP sẽ được cấp một mật mã. Mật mã này BẮT BUỘC được sử dụng để xác thực AP trong trường hợp kênh truyền chỉ áp dụng xác thực máy chủ một chiều qua TLS (xem 10.2.3). Trường hợp áp dụng xác thực TLS hai chiều (mutual TLS) bằng chứng thư số X.509v3 của AP, hoặc áp dụng cơ chế ký/xác thực thông điệp bằng mã xác thực thông điệp (MAC)/token dựa trên cặp khóa được cấp cho AP, MSSP CÓ THỂ chấp nhận không yêu cầu truyền AP_PWD dưới dạng bản rõ. Khuyến nghị các tổ chức triển khai mới ưu tiên áp dụng mutual TLS hoặc cơ chế MAC/token thay cho việc truyền mật khẩu dạng bản rõ.	Có điều kiện
	Instant	DateTime	AP BẮT BUỘC phải ghi rõ thời gian và ngày tháng khi thông điệp được khởi tạo.	Có
	AP_URL	anyURI	Trong trường hợp chế độ gửi thông điệp áp dụng cho thông điệp này là máy chủ không đồng bộ máy chủ, MSSP cần biết URL của phương thức thông báo của AP. AP sử dụng tham số này để chỉ định URL đó cho MSSP trong yêu cầu chữ ký số di động.	Không
MSSP_Info	MSSP_ID	MeshMemberType, xem 8.2.1	Tất cả các AP, bao gồm cả MSSP, đều được định danh thông qua các trình định danh dựa trên URI (URI-based identifier)	Có
	Instant	DateTime	MSSP PHẢI ghi rõ thời gian và ngày tháng khi thông đi hợp được khởi tạo. Tham số này không được đánh dấu là bắt buộc trong cột “Bắt buộc”, vì thành phần này chỉ được sử dụng trong các thông điệp phản hồi từ phía MSSP.	Không

Bảng 1. Các tham số kiểu thông điệp trừu tượng.

```
<xs:complexType name="MessageAbstractType" abstract="true">
<xs:sequence>
<xs:element name="AP_Info">
<xs:complexType>
<xs:attribute name="AP_ID" type="xs:anyURI" use="required"/>
<xs:attribute name="AP_TransID" type="xs:NCName" use="required"/>
<xs:attribute name="AP_PWD" type="xs:string" use="required"/>
<xs:attribute name="Instant" type="xs:dateTime" use="required"/>
<xs:attribute name="AP_URL" type="xs:anyURI" use="optional"/>
</xs:complexType>
</xs:element>
<xs:element name="MSSP_Info">
<xs:complexType>
<xs:sequence>
<xs:element name="MSSP_ID" type="mss:MeshMemberType"/>
</xs:sequence>
<xs:attribute name="Instant" type="xs:dateTime" use="optional"/>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="MajorVersion" type="xs:integer" use="required"/>
<xs:attribute name="MinorVersion" type="xs:integer" use="required"/>
</xs:complexType>
```

7.2 Yêu cầu ký số MSS [SigREQ - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUser	MobileUserType, xem 8.2.4	Bất kỳ trình định danh nào cho phép MSSP kết nối với thiết bị di động của người dùng cuối	Có

DataToBeSigned	DataType, xem 8.3.2	Dữ liệu mà RP yêu cầu người dùng cuối thực hiện ký số. Lưu ý rằng vì mục đích bảo mật, thành phần dữ liệu cần ký (DTBS) có thể bao gồm một phần tử XML đã được mã hóa.	Có
DataToBeDisplayed	DataType, xem 8.3.2	Sự hiện diện của tham số này cho biết dữ liệu cần ký là dữ liệu không hiển thị. Nội dung của các trường hiển thị sẽ được trình bày cho người dùng. Việc có cho phép tùy chọn này hay không có thể được quy định trong chính sách ký số.	Không
SignatureProfile	mssURIType, xem 8.2.3	RP yêu cầu sử dụng hồ sơ chữ ký số này trong quá trình xử lý giao dịch.	Không
AdditionalServices	List of AdditionalServiceType, xem 8.3.4	Danh mục các dịch vụ gia tăng dựa trên ký số di động, bao gồm: ● Kiểm tra hiệu lực ký số (Signature validation); ● Cấp dấu thời gian (Timestamping); ● Lưu trữ (Archiving); ● Các dịch vụ khác.	Không
MSS_Format	MssURI	RP yêu cầu một định dạng cho chữ ký số. Định dạng này có thể là: ● Chữ ký số XML (XML Signature); ● CMS (Cryptographic Message Syntax); ● PKCS#7; ● PKCS#10; ● Các định dạng khác	Không
KeyReference	KeyReferenceType, xem 8.3.3	Trong trường hợp MSSP không ngầm định biết trước khóa bí mật hoặc chứng thư số của người dùng cuối dùng để ký giao dịch, RP có quyền chỉ định các thông tin này	Không
SignatureProfileComparison	SignatureProfileComparisonType, xem 8.3.5	Trong tham số này, RP chỉ định cách thức MSSP phải xử lý đối với hồ sơ chữ ký số đã được đề cập ở trên	Không
ValidityDate	DateTime	Thời điểm hết hạn của giao dịch. Nếu đối số này không được chỉ định, một khoảng thời gian chờ (timeout) mặc định NÊN được sử dụng.	Không
TimeOut	positiveInteger	Thể hiện khoảng thời gian tính bằng giây mà MSSP phải chờ trước khi phản hồi cho AP. Nếu đối số này không được chỉ định, một khoảng thời gian chờ (timeout) mặc định NÊN được sử dụng	Không
MessagingMode	MessagingModeType, xem 8.3.1	Xác định chế độ gửi thông điệp, bao gồm: chế độ đồng bộ, chế độ máy khách không đồng bộ máy chủ hoặc chế độ máy chủ không đồng bộ máy chủ.	Có

Bảng 2. Các tham số yêu cầu ký số MSS.

```
<xs:element name="MSS_SignatureReq" type="mss:MSS_SignatureReqType"/>
<xs:complexType name="MSS_SignatureReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="DataToBeSigned" type="mss:DataType"/>
                <xs:element name="DataToBeDisplayed" type="mss:DataType" minOccurs="0"/>
                <xs:element name="SignatureProfile" type="mss:mssURIType" minOccurs="0"/>
                <xs:element name="AdditionalServices" minOccurs="0">
                    <xs:complexType>
```

```
                        <xs:sequence>
                            <xs:element name="Service" type="mss:AdditionalServiceType" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MSS_Format" type="mss:mssURIType" minOccurs="0"/>
                <xs:element name="KeyReference" type="mss:KeyReferenceType" minOccurs="0"/>
                <xs:element name="SignatureProfileComparison" type="mss:SignatureProfileComparisonType"
minOccurs="0"/>
            </xs:sequence>
            <xs:attribute name="ValidityDate" type="xs:dateTime" use="optional"/>
            <xs:attribute name="TimeOut" type="xs:positiveInteger" use="optional"/>
            <xs:attribute name="MessagingMode" type="mss:MessagingModeType" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

CHÚ THÍCH: Kiểu thông điệp SigREQ quy định tại Điều 7.2 áp dụng cho mỗi giao dịch ký số riêng lẻ. Đối với các đơn vị có nhu cầu xử lý đồng thời một khối lượng lớn chứng từ thu/chi (ví dụ: ngân hàng, tổ chức tài chính), tổ chức cung cấp dịch vụ CÓ THỂ triển khai bổ sung cơ chế ký theo lô (batch signing) bằng cách đóng gói nhiều yêu cầu SigREQ độc lập trong một phiên giao dịch nghiệp vụ ở tầng ứng dụng (AP), miễn là mỗi giao dịch ký thành phần vẫn tuân thủ đầy đủ cấu trúc thông điệp SigREQ/SigRESP quy định tại Điều 7. Đặc tả chi tiết cho giao thức và cấu trúc thông điệp hỗ trợ ký theo lô ở tầng giao diện Web (bao gồm cơ chế tối ưu số lượt round-trip) sẽ được nghiên cứu bổ sung trong lần soát xét tiếp theo của tiêu chuẩn.

7.3 Phản hồi ký số MSS [SigRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUser	MobileUserType, xem 8.2.4	Bất kỳ thông tin nhận dạng nào của người dùng cuối có liên quan đến giao dịch này.	Có
Status	StatusType, xem 8.4.2	Trạng thái hiện tại của giao dịch.	Có
SignatureProfile	mssURIType, xem 8.2.3	MSSP nên đưa ra một thông báo xác nhận về hồ sơ chữ ký số đã được sử dụng.	Không
MSS_Signature	SignatureType, xem 8.4.1	Chữ ký số di động được tạo lập trên thiết bị di động của người dùng cuối, cùng với các dữ liệu dịch vụ bổ trợ tùy chọn	Không
MSSP_TransID	NCName	Số hiệu giao dịch được tạo bởi MSSP cho giao dịch này	Có

Bảng 3. Các tham số phản hồi ký số MSS.

```
<xs:element name="MSS_SignatureResp" type="mss:MSS_SignatureRespType"/>
<xs:complexType name="MSS_SignatureRespType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="MSS_Signature" type="mss:SignatureType" minOccurs="0"/>
                <xs:element name="SignatureProfile" type="mss:mssURIType" minOccurs="0"/>
                <xs:element name="Status" type="mss:StatusType"/>
            </xs:sequence>
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

Yêu cầu chức năng:

Nếu yêu cầu hợp lệ VÀ được người nhận chấp nhận để xử lý VÀ không có thêm thông tin, người

nhận sau đó PHẢI đặt mã trạng thái 100 trong phản hồi trở lại cho người gửi:

- Nếu chế độ nhắn tin là đồng bộ VÀ MSSP nhận được Ký số trên thiết bị di động từ người dùng cuối, MSSP phải cho biết mã trạng thái 500.
- Nếu chứng của người ký bị thu hồi, MSSP PHẢI cho biết mã trạng thái 501.
- Nếu ký số hợp lệ, MSSP PHẢI cho biết mã trạng thái 502.
- Nếu ký số không hợp lệ, MSSP PHẢI cho biết mã trạng thái 503.

7.4 Yêu cầu trạng thái MSS [StatREQ - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MSSP_Transaction_ID	NCName	Trong tham số này, AP đề cập đến số giao dịch mà nó đang tìm kiếm thông tin.	Có

Bảng 4. Các tham số yêu cầu trạng thái MSS.

```
<xs:element name="MSS_StatusReq" type="mss:MSS_StatusReqType"/>
<xs:complexType name="MSS_StatusReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.5 Phản hồi trạng thái MSS [StatRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUser	MobileUserType, xem 8.2.4	Bất kỳ thông tin nhận dạng nào của người dùng cuối có liên quan đến giao dịch này.	Có
MSS_Signature	SignatureTyp, xem 8.4.1	Nếu có sẵn, tham số này chứa chữ ký số được tạo lập trên thiết bị di động của người dùng cuối	Không
Status	StatusType, xem 8.4.2	Trạng thái hiện tại của giao dịch.	Có

Bảng 5. Các tham số phản hồi trạng thái MSS.

```
<xs:element name="MSS_StatusResp" type="mss:MSS_StatusRespType"/>
<xs:complexType name="MSS_StatusRespType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="MSS_Signature" type="mss:SignatureType" minOccurs="0"/>
                <xs:element name="Status" type="mss:StatusType"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

Do phương thức truy vấn trạng thái có thể được AP gọi vào bất kỳ lúc nào, nên giá trị trạng thái có thể nhận tất cả các giá trị trong danh mục mã lỗi. Trong trường hợp phương thức này được gọi sau một yêu cầu ký số di động ở chế độ máy khách không đồng bộ máy chủ, AP thường sẽ nhận được các mã trạng thái thay vì các mã lỗi. Mã trạng thái điển hình cho phương thức này là mã 504, có nghĩa là AP sẽ

cần phải thực hiện gọi lại phương thức truy vấn trạng thái này một lần nữa.

7.6 Yêu cầu đăng ký MSS [RegREQ – STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUser	MobileUserType, xem 8.2.4	Ít nhất thì MSSP cần kích hoạt tính năng xác thực chữ ký trên thiết bị di động của người dùng cuối nếu tính năng đó chưa được kích hoạt.	Có
EncryptedData	xenc:EncryptedType	Nạp dữ liệu bảo mật vào ứng dụng ký số trên thiết bị di động của người dùng cuối.	Không
EncryptResponseBy	anyURI	Phần tử này xác định một khóa mã hóa/giải mã cụ thể đi kèm với một phương thức mã hóa. AP chỉ định phần tử này nhằm xác định khóa và phương thức sẽ được thiết bị di động sử dụng để mã hóa các thông tin bảo mật. AP sẽ nhận lại các thông tin đã được mã hóa này trong thông điệp RegRESP - STD.	Không
CertificateURI	anyURI	Được lưu trữ bởi MSSP và tải xuống ứng dụng ký số số di động.	Không
X509Certificate	base64Binary	Được lưu trữ bởi MSSP và tải xuống ứng dụng ký số trên thiết bị di động nếu có thể.	Không
Any	Any	Tham số này tạo điều kiện cho MSSP cung cấp cho AP một phương thức đăng ký tùy chỉnh. AP sẽ sử dụng tham số này để chỉ định các thông tin liên quan khác của người dùng cuối thu thập được từ giai đoạn đăng ký.	Không

Bảng 6. Các tham số yêu cầu đăng ký MSS.

```
<xs:element name="MSS_RegistrationReq" type="mss:MSS_RegistrationReqType"/>
<xs:complexType name="MSS_RegistrationReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="EncryptedData" type="xenc:EncryptedType" minOccurs="0"/>
                <xs:element name="EncryptResponseBy" type="xs:anyURI" minOccurs="0"/>
                <xs:element name="CertificateURI" type="xs:anyURI" minOccurs="0"/>
                <xs:element name="X509Certificate" type="xs:base64Binary" minOccurs="0"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.7 Phản hồi đăng ký MSS [RegRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
Status	StatusType, xem 8.4.2	Trạng thái hiện tại của giao dịch. Nếu quá trình đăng ký được thực hiện thành công, MSSP PHẢI chỉ định mã trạng thái 408.	Có
EncryptedData	xenc:EncryptedType	Truy xuất các thông tin bảo mật từ giai đoạn đăng ký trên thiết bị di động của người dùng cuối. Thông tin này có thể là mã PIN ký số hoặc khóa ký… Việc mã hóa phần tử này được yêu cầu thông qua phần tử EncryptReponseBy trong RegREQ – STD.	Không
CertificateURI	anyURI	Truy xuất thông tin công khai.	Không
X509Certificate	base64Binary	Truy xuất thông tin công khai.	Không
PublicKey	Base64Binary	Truy xuất thông tin công khai.	Không

Bảng 7. Các tham số phản hồi đăng ký MSS.

```
<xs:element name="MSS_RegistrationResp" type="mss:MSS_RegistrationRespType"/>
<xs:complexType name="MSS_RegistrationRespType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="Status" type="mss:StatusType"/>
                <xs:element name="EncryptedData" type="xenc:EncryptedType" minOccurs="0"/>
                <xs:element name="CertificateURI" type="xs:anyURI" minOccurs="0"/>
                <xs:element name="X509Certificate" type="xs:base64Binary" minOccurs="0"/>
                <xs:element name="PublicKey" type="xs:base64Binary" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.8 Yêu cầu hồ sơ MSS [ProfREQ - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUse	MobileUserType, xem 8.2.4	Trong trường hợp MSSP triển khai các kỹ thuật mật mã khác nhau cho các người dùng cuối, MSSP có thể phản hồi khác nhau tùy theo từng người dùng. AP sử dụng tham số này để chỉ định người dùng cuối mà hồ sơ ký số trên thiết bị di động của họ cần được truy xuất.	Không

Bảng 8. Các tham số yêu cầu hồ sơ MSS.

```
<xs:element name="MSS_ProfileReq" type="mss:MSS_ProfileReqType"/>
<xs:complexType name="MSS_ProfileReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.9 Phản hồi hồ sơ MSS [ProfRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileSignatureProfile	mssURIType, xem 8.2.3	Một hoặc nhiều hồ sơ ký số trên thiết bị di động được MSSP này hỗ trợ cho người dùng cuối đã được chỉ định trong yêu cầu truy xuất hồ sơ ký số trên thiết bị di động.	Không
Status	StatusType, xem 8.4.2	Trạng thái hiện tại của giao dịch.	Có

Bảng 9. Các tham số phản hồi hồ sơ MSS.

```
<xs:element name="MSS_ProfileReq" type="mss:MSS_ProfileReqType"/>
<xs:complexType name="MSS_ProfileReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

Yêu cầu chức năng:

Nếu người dùng cuối không được MSSP xác định và MSSP không thuộc mạng lưới dịch vụ chuyển vùng chữ ký số di động, thì MSSP PHẢI chỉ định mã trạng thái 105

7.10 Yêu cầu nhận MSS [RecREQ – STD]

Tên	Định dạng	Mô tả	Bắt buộc
MobileUser	MobileUserType, xem 8.2.4	Bất kỳ mã định danh nào cho phép MSSP liên hệ với thiết bị di động của người dùng cuối.	Có
Status	StatusType, xem 8.4.2	Trạng thái của giao dịch.	Không
MSSP_Trans_ID	NCName	Yêu cầu biên nhận PHẢI luôn được liên kết với một giao dịch ký trước đó. Về mặt này, tham số này PHẢI tương ứng với ID giao dịch mà MSSP đã xử lý.	Có
Message	DataType, xem 8.3.2	Một thông điệp mà RP muốn gửi tới người dùng cuối.	Không
SignedReceipt	XML Signature	AP có thể tùy chọn cung cấp cho người dùng cuối một biên nhận đã được ký số.	Không

Bảng 10. Các tham số yêu cầu nhận MSS.

```
<xs:element name="MSS_ReceiptReq" type="mss:MSS_ReceiptReqType"/>
<xs:complexType name="MSS_ReceiptReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="Status" type="mss:StatusType" minOccurs="0"/>
                <xs:element name="Message" type="mss:DataType" minOccurs="0"/>
                <xs:element name="SignedReceipt" type="ds:SignatureType" minOccurs="0"/>
            </xs:sequence>
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.11 Phản hồi nhận MSS [RecRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
Status	StatusType, xem 8.4.2	Trạng thái hiện tại của giao dịch.	Có

Bảng 11. Các tham số phản hồi nhận MSS.

```
<xs:element name="MSS_ReceiptResp" type="mss:MSS_ReceiptRespType"/>
<xs:complexType name="MSS_ReceiptRespType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="Status" type="mss:StatusType"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

7.12 Yêu cầu bắt tay MSS [HShakeREQ - STD]

Tên	Định dạng	Mô tả	Bắt buộc
SecureMethods	complexType	Thành phần này là danh mục các phương thức mà AP muốn được bảo mật.	Có
Certificates	complexType	Thông qua phần tử này, AP chỉ định một danh mục các chứng thư số mà mình có thể sử dụng để tạo chữ ký số XML. Nếu danh mục này trống, AP không hỗ trợ chữ ký số XML	Có
RootCAs	complexType	Thông qua thành phần này, AP chỉ định một danh mục các tổ chức chứng thực gốc (Root CA) được hỗ trợ mà mình có thể sử dụng cho mục đích xác thực chữ ký số XML. Nếu danh mục này trống, AP không bắt buộc sử dụng bất kỳ Root CA cụ thể nào	Có
SignatureAlgList	complexType	Tham số này chỉ định danh mục các thuật toán ký số được AP hỗ trợ. Mỗi thuật toán ký số được định danh bằng một URI, ví dụ: http://www.w3.org/2000/09/xmldsig#dsa-sha1	Có

Bảng 12. Các tham số yêu cầu bắt tay MSS.

```
<xs:element name="MSS_HandshakeReq" type="mss:MSS_HandshakeReqType"/>
<xs:complexType name="MSS_HandshakeReqType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="SecureMethods">
                    <xs:complexType>
                        <xs:attribute name="MSS_Signature" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Registration" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Notification" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_ProfileQuery" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Receipt" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Status" type="xs:boolean" use="required"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="Certificates">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Certificate" type="xs:base64Binary" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="RootCAs">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="DN" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="SignatureAlgList">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Algorithm" type="mss:mssURIType" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
```

```
</xs:complexType>
```

7.13 Phản hồi bắt tay MSS [HShakeRESP - STD]

Tên	Định dạng	Mô tả	Bắt buộc
MSSP_TransID	NCName	Số hiệu giao dịch được MSSP tạo ra cho quá trình bắt tay (handshake) này. Sau đó, AP sẽ sử dụng lại số hiệu giao dịch này trong lần gọi phương thức tiếp theo	Có
SecureMethods	complexType	Thành phần này là danh mục các phương thức mà MSSP yêu cầu phải được bảo mật.	Có
MatchingMSSPCertificates	complexType	Mục đích của thành phần này là chỉ định cho AP các chứng thư số của MSSP khớp với các tổ chức chứng thực gốc (Root CA) đã được AP nêu trong HShakeREQ - STD. Nếu danh mục này trống, MSSP không thể cung cấp chữ ký số XML cho AP.	Có
MatchingApCertificates	complexType	Mục đích của phần tử này là chỉ định cho AP các chứng thư số của AP mà MSSP có thể hiểu và tin cậy. Do đó, phần tử này là một tập hợp con của danh mục Chứng thư số đã được cung cấp trong HShakeREQ - STD. Nếu danh mục này trống, MSSP không thể sử dụng các chữ ký số XML do AP cung cấp.	Có
MatchingSigAlgList	complexType	Tham số này chỉ định danh mục các thuật toán ký số được AP và MSSP hỗ trợ. Sau đó, AP sẽ chọn sử dụng một trong các thuật toán đó. Mỗi thuật toán ký số được định danh bằng một URI, ví dụ: http://www.w3.org/2000/09/xmldsig#dsa-sha1.	Có

Bảng 13. Các tham số phản hồi bắt tay MSS.

```
<xs:element name="MSS_HandshakeResp" type="mss:MSS_HandshakeRespType"/>
<xs:complexType name="MSS_HandshakeRespType">
    <xs:complexContent>
        <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
                <xs:element name="SecureMethods">
                    <xs:complexType>
                        <xs:attribute name="MSS_Signature" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Registration" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Notification" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_ProfileQuery" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Receipt" type="xs:boolean" use="required"/>
                        <xs:attribute name="MSS_Status" type="xs:boolean" use="required"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MatchingMSSPCertificates">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Certificate" type="xs:base64Binary" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MatchingAPCertificates">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Certificate" type="xs:base64Binary" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MatchingSigAlgList">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Algorithm" type="mss:mssURIType" minOccurs="0" maxOccurs="unbounded"/>
```

```
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
        <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

8 Các kiểu dữ liệu bổ trợ (Auxiliary types)

Các kiểu thông điệp được quy định trong phần trước dựa trên các kiểu dữ liệu XML được cung cấp tại khoản này. Không gian tên XML (XML namespace) được sử dụng trong tiêu chuẩn này và các tiền tố (prefixes) dùng để biểu thị các không gian tên khác đã được định nghĩa trong phần giới thiệu.

8.1 Định danh URI (URI identifier)

Các mã định danh URI theo tiêu chuẩn RFC 2396 được sử dụng trong phạm vi tiêu này để định danh duy nhất cho:

- AP;
- MSSP;
- Các định dạng ký số;
- Các dịch vụ bổ trợ như: cấp dấu thời gian, xác thực chữ ký và lưu trữ chữ ký;
- Các hồ sơ chữ ký số;
- Không gian tên của lược đồ XML (XML-Schema).

Tất cả các AP, bao gồm cả MSSP, đều được xác định bằng mã định danh dựa trên URI. Do đó, mã định danh dựa trên URI phải là duy nhất. Vì vậy, KHUYẾN NGHỊ rằng mỗi AP nên sử dụng URL dựa trên tên miền riêng của mình cho mã định danh này.

Tuy nhiên, trong một số trường hợp, AP không phải tập trung vào máy chủ do một công ty lưu trữ, mà có thể là điện thoại di động hoặc PC của người dùng cuối. Trong những trường hợp đó, AP có URI dựa trên tên miền của MSSP hoặc tên miền của thực thể tiếp nhận cho các kịch bản chuyển vùng.

Để biểu thị một số định dạng ký số, các URI được quy định cụ thể tại phần kiểu ký số và để biểu thị một số dịch vụ bổ trợ được yêu cầu như cấp dấu thời gian, tham chiếu phần kiểu dịch vụ bổ trợ. AP NÊN chỉ định và công bố URI riêng cho dịch vụ của mình. KHUYẾN NGHỊ rằng URI này nên sử dụng URL dựa trên tên miền riêng của họ làm mã định danh.

Một số URI cho hồ sơ chữ ký số sẽ được công bố trong không gian tên của tiêu chuẩn này. Các bên tham gia dịch vụ chữ ký số trên thiết bị di động NÊN công bố thêm URI theo nhu cầu của họ.

8.2 Các kiểu dữ liệu bổ trợ chung

8.2.1 Thành viên mạng (MeshMemberType)

Kiểu dữ liệu này được dùng để biểu thị một thực thể. Việc này có thể thực hiện thông qua tên miền (DNS-Name), địa chỉ IP, một chuỗi ký tự định danh thực thể hoặc một URI.

```
<xs:complexType name="MeshMemberType">
    <xs:sequence> <xs:element name="DNSName" type="xs:string" minOccurs="0"/>
        <xs:element name="IPAddress" type="xs:string" minOccurs="0"/>
        <xs:element name="URI" type="xs:anyURI" minOccurs="0"/>
        <xs:element name="IdentifierString" type="xs:string" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

8.2.2 Thuật toán băm và giá trị băm (DigestAlgAndValueType)

Kiểu dữ liệu này đơn thuần là một cấu trúc chứa giá trị băm và tùy chọn chỉ định thuật toán đã sử dụng để tạo ra giá trị băm đó. Kiểu dữ liệu này chỉ được sử dụng kết hợp với kiểu mssURI. Đối với mục đích này, các kiểu DigestMethodType và DigestMethodValue của chữ ký số XML W3C sẽ được sử dụng.

```
<xs:complexType name="DigestAlgAndValueType">
    <xs:sequence>
        <xs:element name="DigestMethod" type="ds:DigestMethodType" minOccurs="0"/>
        <xs:element name="DigestValue" type="ds:DigestValueType"/>
    </xs:sequence>
</xs:complexType>
```

8.2.3 Định danh mssURI (mssURIType)

Kiểu dữ liệu này được dùng để chỉ định một URI và vì lý do an ninh, nó cũng cung cấp một giá trị băm liên quan riêng đến URI này. Phần tử này cung cấp khả năng bổ sung thêm các thông tin khác.

```
<xs:complexType name="mssURIType">
    <xs:sequence>
        <xs:element name="mssURI" type="xs:anyURI"/>
        <xs:element name="DigestAlgAndValue" type="mss:DigestAlgAndValueType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

8.2.4 Người dùng (MobileUserType)

Kiểu dữ liệu này dùng để xác định người dùng cuối. Theo đó, một mã định danh xác định người dùng cuối và bên cấp phát định danh tương ứng, số thuê bao di động (MSISDN) và MSSP gốc của người dùng cuối có thể được chỉ định theo bất kỳ sự kết hợp nào. Mục đích là để định danh duy nhất người dùng cuối.

8.3 Các kiểu dữ liệu bổ trợ của AP

Phần này mô tả các kiểu dữ liệu được AP sử dụng trong quá trình giao tiếp với MSSP.

8.3.1 Chế độ truyền tin (MessagingModeType)

Như đã mô tả ở trên, MSSP cung cấp cho các bên cung cấp ứng dụng các chế độ truyền tin khác nhau. Có ba chế độ truyền tin khả thi:

- Chế độ đồng bộ: Là chức năng yêu cầu - phản hồi cơ bản.
- Chế độ máy khách không đồng bộ máy chủ: Chức năng này thực hiện thông qua nhiều lần yêu cầu - phản hồi.
- Chế độ máy chủ không đồng bộ máy chủ: Đây là cơ chế truyền tin hai chiều, chế độ này yêu cầu năng lực đặc biệt từ phía máy khách, cụ thể là máy khách cũng phải hỗ trợ năng lực như

một máy chủ.

Quy định tuân thủ:

- MSSP phải hỗ trợ cả ba chế độ truyền tin nêu trên.
- Về cơ bản, AP sẽ chỉ định chế độ truyền tin cho MSSP.
- Phía máy khách của AP phải hỗ trợ ít nhất một trong ba chế độ này và nên hỗ trợ cả ba.

```
<xs:simpleType name="MessagingModeType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="synch"/>
        <xs:enumeration value="asynchClientServer"/>
        <xs:enumeration value="asynchServerServer"/>
    </xs:restriction>
</xs:simpleType>
```

8.3.2 Dữ liệu (DataType)

Kiểu dữ liệu này được dùng làm cấu trúc chứa các thông điệp cần ký hoặc hiển thị, được gửi từ AP hoặc RA tới người dùng cuối. Các thuộc tính tùy chọn sẽ chỉ định kiểu MIME và phương thức mã hóa thông điệp theo tiêu chuẩn RFC 2045 và RFC 2046.

```
<xs:complexType name="DataType">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="MimeType" type="xs:string" use="optional"/>
            <xs:attribute name="Encoding" type="xs:string" use="optional"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
```

8.3.3 Tham chiếu khóa (KeyReferenceType)

Kiểu dữ liệu này chỉ định khóa của người dùng cuối sẽ được sử dụng để tạo chữ ký số. Có thể tham chiếu một khóa bằng cách chỉ định:

CHÚ THÍCH: Trường hợp người dùng cuối sở hữu nhiều chứng thư chữ ký số và MSSP cần kiểm tra hiệu lực của chứng thư chữ ký số trước khi thực hiện ký (10.2.3, 8.4.2 - StatusType), RP/AP NÊN chỉ định KeyReference tương ứng với chứng thư chữ ký số đang có hiệu lực dùng để ký giao dịch, thông qua CertificateURL hoặc HashOfUsersPublicKey, nhằm tránh nhầm lẫn trong trường hợp thông tin chứng thư chữ ký số trên thiết bị của người dùng (ví dụ trên SIM) chưa đồng bộ kịp thời với hệ thống MSSP/CA (chứng thư chữ ký số đã hết hạn hoặc bị thu hồi nhưng chưa được cập nhật trên thiết bị do gián đoạn kết nối OTA). MSSP PHẢI kiểm tra trạng thái hiệu lực của chứng thư chữ ký số được tham chiếu tại thời điểm xử lý yêu cầu ký và trả về mã trạng thái tương ứng (xem Phụ lục B, mã 501 - REVOKED_CERTIFICATE) nếu chứng thư chữ ký số không còn hiệu lực.

- Một URI liên kết với chứng thư số;
- Tên phân biệt (Distinguished Name) của tổ chức cấp phát chứng thư;
- Giá trị băm của khóa;
- Giá trị băm khóa công khai của CA đã cấp phát chứng thư đó;
- Hoặc sử dụng bất kỳ phương thức nào khác.

```
<xs:complexType name="KeyReferenceType">
    <xs:sequence>
        <xs:element name="CertificateURL" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="CertificateIssuerDN" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
```

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

8.3.4 Dịch vụ bổ trợ (AdditionalServiceType)

Kiểu AdditionalServiceType được dùng để cho biết AP không chỉ yêu cầu ký số của người dùng cuối mà còn yêu cầu xác thực chữ ký này, cấp dấu thời gian, lưu trữ chữ ký hoặc các dịch vụ khác. Do đó, quy trình tương ứng sẽ được chỉ định bằng một URI. Thực thể chịu trách nhiệm thực hiện dịch vụ bổ trợ cũng có thể được chỉ định cụ thể.

```
<xs:complexType name="AdditionalServiceType">
    <xs:sequence>
        <xs:element name="Description" type="mss:mssURIType"/>
        <xs:element name="Entity" type="mss:MeshMemberType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

8.3.5 So khớp hồ sơ chữ ký số (SignatureProfileComparisonType)

Phần tử SignatureProfileComparison quy định hành vi của MSSP đối với các hồ sơ chữ ký số trên thiết bị di động được cung cấp trong yêu cầu ký số:

- exact (khớp chính xác): MSSP được yêu cầu phải khớp chính xác với ít nhất một trong các phần tử <SignatureProfile> được chỉ định.
- minimum (tối thiểu): MSSP được yêu cầu sử dụng một hồ sơ mà hệ thống đánh giá là tốt ít nhất bằng bất kỳ hồ sơ nào được chỉ định.
- better (tốt hơn): MSSP được yêu cầu sử dụng bất kỳ hồ sơ nào tốt hơn các hồ sơ đã cung cấp.

Nếu không được chỉ định, hệ thống mặc định là "exact".

```
<xs:simpleType name="SignatureProfileComparisonType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="exact"/>
        <xs:enumeration value="minimum"/>
        <xs:enumeration value="better"/>
    </xs:restriction>
</xs:simpleType>
```

8.4 Các kiểu dữ liệu bổ trợ của MSSP

Phần này mô tả các kiểu dữ liệu được MSSP sử dụng khi gửi thông điệp phản hồi cho AP.

8.4.1 Chữ ký (SignatureType)

Kiểu SignatureType đóng vai trò là cấu trúc chứa cho chữ ký số do người dùng cuối cung cấp. Chữ ký này có thể là:

- Chữ ký số XML (XML-Signature): Tuân thủ RFC 3275.
- Chữ ký mã hóa base64: Tuân thủ tiêu chuẩn PKCS#7.

- Chữ ký CMS (CMS-Signature): Tuân thủ RFC 2630.

Phần tử any cho phép sử dụng các định dạng chữ ký khác.

Kiểu dữ liệu này cũng đóng vai trò là cấu trúc cho chữ ký của người dùng cuối kết hợp với các thông tin bổ sung do MSSP hoặc một thực thể khác cung cấp.

```
<xs:complexType name="SignatureType">
    <xs:choice>
        <xs:element name="XMLSignature" type="ds:SignatureType"/>
        <xs:element name="Base64Signature" type="xs:base64Binary"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"/>
        <!-- this can also be an advanced XML Signature-->
    </xs:choice>
</xs:complexType>
```

8.4.2 Trạng thái (StatusType)

Kiểu StatusType biểu thị trạng thái của một thông điệp phản hồi. Cấu trúc này bao gồm:

- Một mã trạng thái bắt buộc thuộc kiểu StatusCodeType.
- Một thông điệp tùy chọn thuộc kiểu chuỗi ký tự.
- Một phần tử chi tiết trạng thái tùy chọn thuộc kiểu StatusDetailType.

```
<xs:complexType name="StatusType">
    <xs:sequence>
        <xs:element name="StatusCode" type="mss:StatusCodeType"/>
        <xs:element name="StatusMessage" type="xs:string" minOccurs="0"/>
        <xs:element name="StatusDetail" type="mss:StatusDetailType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
```

8.4.3 Mã trạng thái (StatusCodeType)

Kiểu StatusCodeType chứa trạng thái của thông điệp phản hồi tương ứng. Cấu trúc này cho phép sử dụng một hoặc nhiều mã trạng thái lồng nhau:

- Mã trạng thái cấp cao nhất: Bắt buộc phải là một trong các giá trị quy định tại Phụ lục A.
- Các mã trạng thái lồng nhau tiếp theo: Là tùy chọn và có thể được quy định cụ thể tùy theo từng phiên bản triển khai thực tế.

```
<xs:complexType name="StatusCodeType">
    <xs:sequence>
        <xs:element name="StatusCode" type="mss:StatusCodeType" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="Value" type="xs:integer" use="required"/>
</xs:complexType>
```

8.4.4 Chi tiết trạng thái (StatusDetailType)

Kiểu StatusDetailType có thể được sử dụng để cung cấp thêm thông tin chi tiết liên quan đến một số lỗi cụ thể phát sinh trong quá trình xử lý.

```
<xs:complexType name="StatusDetailType">
    <xs:sequence>
        <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

9 Ràng buộc giao thức truyền thông

Phần này định nghĩa việc ràng buộc giao thức cho dịch vụ ký số trên thiết bị di động trong các giao thức truyền thông. Việc chuyển đổi từ cơ chế trao đổi thông điệp yêu cầu - phản hồi của dịch vụ ký số di động sang các giao thức truyền thông tiêu chuẩn được gọi là ràng buộc giao thức.

Trong phạm vi tiêu chuẩn này, chỉ đề cập đến việc ràng buộc với giao thức SOAP, bởi vì dịch vụ Web ký số trên thiết bị di động PHẢI được triển khai trên nền tảng SOAP 1.2 chạy qua HTTP. Mục tiêu của việc quy định ràng buộc giao thức này là để đảm bảo tính liên thông giữa các hệ thống triển khai khác nhau.

CHÚ THÍCH: Ràng buộc SOAP 1.2/HTTP quy định tại Điều này là hồ sơ (profile) bắt buộc tối thiểu nhằm bảo đảm khả năng liên thông với các hệ thống MSSP/CA hiện đang vận hành theo mô hình ETSI TS 102 204. Các tổ chức cung cấp dịch vụ có thể triển khai bổ sung hồ sơ ràng buộc RESTful API/JSON tương đương về mặt ngữ nghĩa với các kiểu thông điệp MSS quy định tại Điều 7, kèm theo cơ chế ký/xác thực thông điệp bằng JSON Web Signature (JWS) hoặc JSON Web Token (JWT), miễn là vẫn duy trì hồ sơ SOAP 1.2 nêu trên để bảo đảm khả năng liên thông tối thiểu theo tiêu chuẩn này. Đặc tả chi tiết cho hồ sơ ràng buộc RESTful API (bao gồm cấu trúc thông điệp JSON và cơ chế ký JWS/JWT) sẽ được xem xét bổ sung trong lần soát xét tiếp theo của tiêu chuẩn.

SOAP là một giao thức dùng để trao đổi thông tin có cấu trúc trong môi trường phân tán và phi tập trung. Giao thức này dựa trên nền tảng XML và HTTP, bao gồm ba phần:

- Phong bì (Envelope): Bao bọc dữ liệu XML và chứa thông tin xử lý.
- Quy tắc mã hóa (Encoding rules): Dùng để khai báo các kiểu dữ liệu đặc thù của ứng dụng.
- Quy ước biểu diễn: Cho việc gọi thủ tục từ xa (RPC) và các phản hồi tương ứng. Giao thức này cũng cung cấp cơ chế ràng buộc các thông điệp SOAP với giao thức HTTP.

9.1 Quy tắc mã hóa

Các quy tắc mã hóa SOAP là tùy chọn. Những quy tắc này không được sử dụng trong ràng buộc SOAP của dịch vụ ký số di động. Thay vào đó, việc mã hóa sẽ sử dụng lược đồ XML của MSS.

9.2 Tiêu đề SOAP

Phong bì SOAP bao gồm hai phần: phần tiêu đề (Header - tùy chọn) và phần thân (Body - bắt buộc). Trong tiêu chuẩn này, chúng ta định nghĩa một khối tiêu đề MSS_MessageSignature tại khoản 10.3.

9.3 Thân SOAP

Các thành phần của bản tin trong các thao tác của dịch vụ ký số trên thiết bị di động được sắp xếp theo phong cách RPC. Cụ thể, mỗi phần là một tham số và xuất hiện bên trong một phần tử bao bọc (wrapper element) nằm trong phần thân (Body).

- Tên của phần tử bao bọc này trùng với tên của thao tác (operation).
- Mỗi tham số phương thức được trình bày bởi một bộ truy cập (accessor) của phần tử bao bọc này. Tên của tham số phương thức và bộ truy cập là trùng nhau.
- Thứ tự sắp xếp là rất quan trọng: các phần phải xuất hiện theo đúng thứ tự của các tham số trong lời gọi hàm.

9.4 SOAP trên giao thức HTTP

Việc ràng buộc dịch vụ ký số di động PHẢI được triển khai bằng SOAP 1.2 trên nền tảng HTTP. SOAP 1.2 qua HTTP yêu cầu phải có một mục nhập SOAPAction trong tiêu đề HTTP. Giao thức bảo mật TLS cũng được sử dụng để bảo mật kênh truyền.

9.5 Mô tả WSDL

Trong điều khoản này, việc ràng buộc giao thức của MSS được tóm tắt một cách chính thức bằng WSDL đã được giới thiệu trong phần trước.

Trong ví dụ WSDL bên dưới, phần tử soap:binding có hai thuộc tính. Giá trị "rpc" của thuộc tính style cho biết rằng thao tác được sử dụng như một cuộc gọi thủ tục từ xa với những hàm ý được mô tả trong phần SOAP Body. Giá trị của thuộc tính transport biểu thị rằng SOAP qua HTTP được sử dụng.

Nếu SOAP qua HTTP được sử dụng, cần có một mục SOAPAction trong tiêu đề HTTP. Do đó, phần tử soap:operation yêu cầu một thuộc tính bắt buộc soapAction nhận một URI làm giá trị, giá trị này phụ thuộc vào cách triển khai. Thuộc tính style một lần nữa cho biết rằng dữ liệu chứa trong phần thân SOAP phải được sắp xếp như một cuộc gọi thủ tục từ xa SOAP.

Giá trị “literal” của thuộc tính use của phần tử soap:body cho biết rằng mỗi phần WSDL tham chiếu đến một định nghĩa lược đồ, cụ thể là MSS XML-Schema. Loại được tham chiếu bởi phần trở thành lược đồ của phần tử bao quanh.

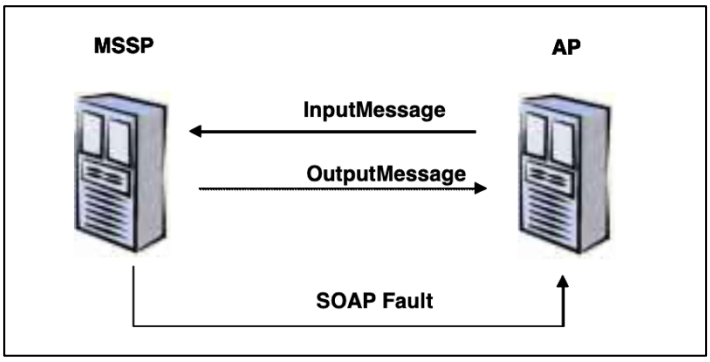
Thành phần dịch vụ kết hợp một nhóm các cổng có liên quan.

```
<?xml version="1.0" encoding="utf-8"?>
<definitions    xmlns="http://schemas.xmlsoap.org/wsdl/
                    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                    xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
                    xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
                    xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
                    xmlns:tns="http://new.webservice.namespace"
                    targetNamespace="http://new.webservice.namespace">

    <import namespace="http://uri.etsi.org/2003/v1.1.2#" location="MSS.xsd"/>
            <message name="MSS_SignatureInput">
                <part name="MSS_SignatureReq" type="mss:MSS_SignatureReqType"/>
            </message>
            <message name="MSS_SignatureOutput">
                <part name="MSS_SignatureResp" type="mss:MSS_SignatureRespType"/>
            </message>

    <portType name="MSS_SignaturePortType">
            <operation name="MSS_Signature">
                <input message="tns:MSS_SignatureInput"/>
                <output message="tns:MSS_SignatureOutput"/>
            </operation>
        </portType>

    <binding name="MSS_SignatureBinding" type="tns:MSS_SignaturePortType">
            <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
            <operation name="MSS_Signature">
```

```
            <soap:operation soapAction="uri" style="rpc"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
        </operation>
    </binding>

    <service name="MSS_SignatureService">
        <port name="MSS_SignaturePort" binding="tns:MSS_SignatureBinding">
            <soap:address location="http://www.Example-MSSP.com"/>
        </port>
    </service>
</definitions>
```

9.6 Xử lý lỗi

Đặc tả SOAP 1.2 đã chuẩn hóa thông điệp lỗi SOAP chung để truyền tải thông tin lỗi. Khi có lỗi xảy ra sau khi nhận thông điệp đầu vào của một phương thức SOAP, bên nhận sẽ gửi lại một thông điệp lỗi SOAP thay vì thông điệp đầu ra tương ứng.



Hình 18: Xử lý lỗi

Thông điệp lỗi SOAP là một thông điệp SOAP điển hình. Phần thân chứa một phần tử XML Fault, phần tử này bao gồm các thành phần sau:

- Code: Có giá trị thuộc một trong năm mã chuẩn của SOAP và chứa các mã con đặc thù của ứng dụng.
- Reason: Cung cấp giải thích về lỗi bằng ngôn ngữ tự nhiên để con người có thể đọc hiểu.
- Node: Cung cấp thông tin về nút SOAP nào trên đường truyền thông điệp đã gây ra lỗi.
- Role: Xác định vai trò của nút đang vận hành tại thời điểm xảy ra lỗi.
- Detail: Dùng để truyền tải các lỗi đặc thù của ứng dụng.

Các mã chuẩn của SOAP bao gồm:

- VersionMismatch: Sai lệch phiên bản.
- MustUnderstand: Không hiểu thành phần bắt buộc.
- DataEncodingUnknown: Không xác định được kiểu mã hóa dữ liệu.
- Sender: Lỗi do bên gửi.
- Receiver: Lỗi do bên nhận.

Dịch vụ Web ký số di động quy định các mã lỗi con, chi tiết tại Phụ lục B:

- Các mã từ 101 đến 108 là mã con thuộc nhóm Sender.
- Các mã còn lại thuộc nhóm Receiver.

Ví dụ 1:

```
<env:Envelope    xmlns:env="http://www.w3.org/2003/05/soap-envelope"
                        xmlns:m="http://www.example.org/timeouts"
                        xmlns:xml="http://www.w3.org/XML/1998/namespace">
    <env:Body>
        <env:Fault>
            <env:Code>
                <env:Value>env:Receiver</env:Value>
                <env:Subcode>
                    <env:Value>208</env:Value>
                </env:Subcode>
            </env:Code>
            <env:Reason>
                <env:Text xml:lang="en">EXPIRED_TRANSACTION</env:Text>
            </env:Reason>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

Ví dụ 2:

```
<env:Envelope    xmlns:env="http://www.w3.org/2003/05/soap-envelope"
                        xmlns:m="http://www.example.org/timeouts"
                        xmlns:xml="http://www.w3.org/XML/1998/namespace">
    <env:Body>
        <env:Fault>
            <env:Code>
                <env:Value>env:Sender</env:Value>
                <env:Subcode>
                    <env:Value>101</env:Value>
                </env:Subcode>
            </env:Code>
            <env:Reason>
                <env:Text xml:lang="en">WRONG_PARAM</env:Text>
            </env:Reason>
        </env:Fault>
    </env:Body>
</env:Envelope>
```

10 Dịch vụ Web: Các cân nhắc về bảo mật và quyền riêng tư

Một dịch vụ web được triển khai trên nền tảng SOAP qua HTTP có thể được coi là một giao thức Internet và các cân nhắc bảo mật trong chương này chỉ giới hạn trong phạm vi của giao thức đó.

10.1 Quá trình bắt tay (Handshake)

Các cân nhắc về bảo mật giúp hiểu rõ về các biện pháp đối phó tiềm năng cần được triển khai dựa trên một mô hình mối đe dọa. Tuy nhiên, mục tiêu của tiêu chuẩn này là đảm bảo tính liên thông giữa các phiên bản triển khai khác nhau của giao thức. Do đó, chúng ta phải xác định các cơ chế bảo mật bắt buộc.

Cần hiểu rằng các cơ chế bắt buộc có thể là bắt buộc phải triển khai hoặc bắt buộc phải sử dụng. Việc người dùng cuối có thực sự sử dụng các cơ chế này hay không không phải là yêu cầu bắt buộc

tuyệt đối.

Nếu các bên xác định rằng họ đang triển khai giao thức trên một mạng lưới "an toàn", họ có thể chọn tắt các cơ chế bảo mật mà họ tin rằng đem lại giá trị thấp so với chi phí về hiệu năng hệ thống.

Ngược lại, một số cơ chế bảo mật cơ bản phải được sử dụng một cách hệ thống và do đó sẽ được nêu rõ là bắt buộc phải sử dụng.

Vì vậy, các bên tham gia vào quá trình xử lý giao dịch Ký số di động sẽ tự thương lượng việc sử dụng các cơ chế này, có tính đến các yếu tố không chỉ thuần túy về bảo mật. Đây chính là mục đích của phương thức bắt tay đã được quy định ở các phần trên, và các cân nhắc bảo mật dưới đây nhằm giải thích nội dung của phương thức này.

10.2 Bảo mật và quyền riêng tư (Security and Privacy)

10.2.1 Mục đích

Tính bảo mật, tính toàn vẹn và tính chống chối bỏ là các phương thức để bảo vệ dịch vụ web chống lại:

- Việc sử dụng trái phép.
- Việc sử dụng không phù hợp.
- Tấn công từ chối dịch vụ (DoS).

Một số vấn đề về quyền riêng tư và bảo mật cũng có thể được đặt ra bởi AP hoặc chủ thể ký. Trong trường hợp đó, mục tiêu là thiết lập bảo mật đầu cuối giữa người ký và AP, nhằm bảo vệ dữ liệu khỏi sự nghe lén từ phía hệ thống MSSP.

Để đạt được bảo mật đầu cuối, AP cần mã hóa dữ liệu cần ký bằng khóa bí mật của người ký hoặc bằng khóa công khai của chủ thể ký. Ở chiều ngược lại, chủ thể ký nên mã hóa ký số trên thiết bị di động hoặc loại bỏ các dữ liệu dạng văn bản rõ.

Tuy nhiên, cần lưu ý rằng các thỏa thuận thương mại được giả định là sẽ điều chỉnh mối quan hệ giữa AP, MSSP và chủ thể ký. Đó là lý do tại sao tiêu chuẩn này chỉ tập trung vào tính bảo mật cho người ký và AP. Chúng tôi giả định rằng MSSP cũng quan tâm đến tính toàn vẹn của dữ liệu nhận được từ AP, vì chất lượng dịch vụ phụ thuộc vào điều đó. Dù trong trường hợp nào, cũng cần có một mối quan hệ tin cậy với các quy định về quyền riêng tư giữa Người ký, MSSP và AP.

10.2.2 Mô hình đe dọa đơn giản hóa cho dịch vụ Web ký số trên thiết bị di động

Giả định rằng các hệ thống đầu cuối tham gia vào việc trao đổi giao thức không bị xâm nhập. Ngược lại, giả định rằng kẻ tấn công có quyền kiểm soát gần như hoàn toàn đối với kênh truyền thông mà các hệ thống đầu cuối sử dụng để kết nối.

Các cuộc tấn công điển hình xảy ra trên các giao thức Internet bao gồm: Vi phạm tính bảo mật, nghe lén mật khẩu, tấn công mã hóa ngoại tuyến, tấn công phát lại, chèn bản tin, xóa bản tin, sửa đổi bản tin và tấn công xen giữa.

10.2.3 Khung bảo mật (Security framework)

Khung bảo mật là tập hợp các biện pháp đối phó liên quan đến các cuộc tấn công mô tả ở trên:

- TLS RFC 2246: Ngăn chặn vi phạm tính bảo mật, chèn bản tin, sửa đổi bản tin, nghe lén mật khẩu và tấn công xen giữa.
  - Xác thực máy chủ: MSSP sở hữu Chứng thư số X509v3.
  - Xác thực lẫn nhau: Cả MSSP và AP đều sở hữu Chứng thư số X509v3.
- Chữ ký số: Các chữ ký số XML được mô tả chi tiết tại khoản 10.3. Nói một cách rộng rãi, chúng cung cấp bảo mật mức đối tượng xuyên suốt mạng lưới định tuyến, nhằm cung cấp tính chống chối bỏ giữa MSSP và AP.
- Trình định danh AP và MSSP: Cho phép các bên nhận diện lẫn nhau.
- Mật khẩu AP: Cung cấp cơ chế xác thực AP trong trường hợp chỉ sử dụng xác thực máy chủ qua TLS.
- Cơ chế số tức thời và số hiệu giao dịch: Ngăn chặn tấn công phát lại.

10.3 Chữ ký số XML (XML Signatures)

Để đưa chữ ký số XML trở thành một cơ chế bảo mật trong giao thức của chúng ta, chúng tôi kế thừa mô hình mở rộng của SOAP 1.2. Việc này được thực hiện bằng cách đặt một chữ ký số XML vào trong một khối tiêu đề thuộc phần tiêu đề của phong bì SOAP.

Về mặt kỹ thuật, khối tiêu đề sau đây sẽ được thêm vào bản tin SOAP:

Phần tử MSS_MessageSignature có một phần tử con là một chữ ký số XML, cùng với hai thuộc tính bổ sung:

- Thuộc tính vai trò: Được dùng để chỉ định nút SOAP mà khối tiêu đề MSS_MessageSignature hướng tới.
- Thuộc tính mustUnderstand: Được dùng để chỉ định việc xử lý khối tiêu đề MSS_MessageSignature là bắt buộc hay tùy chọn.

Chữ ký số XML này chính là chữ ký số của phần thân SOAP.

Khi một hệ thống MSSP hoặc AP tiêu chuẩn nhận được một bản tin SOAP có chứa khối tiêu đề MSS_MessageSignature và vai trò của bên nhận khớp với thuộc tính role, thì bên nhận PHẢI thực hiện kiểm tra tính hợp lệ của ký số theo mô hình xử lý của chữ ký số XML.

Quy trình tạo mục nhập MSS_MessageSignature:

- Chuẩn bị phong bì SOAP mục tiêu với phần thân và các tiêu đề cần thiết.
- Tạo một khuôn mẫu cho phần tử <ds:Signature>. Khuôn mẫu này giả định chứa nội dung trống cho các phần tử <ds:DigestValue> và <ds:SignatureValue>.
- Tạo một mục nhập tiêu đề mới MSS_MessageSignature và thêm khuôn mẫu trên vào mục này.
- Thêm mục nhập tiêu đề MSS_MessageSignature vào phần iêu đề SOAP.
- Thêm các thuộc tính SOAP “role” và “mustUnderstand” vào mục nhập.

- Tính toán giá trị cho các phần tử <ds:DigestValue> và <ds:SignatureValue> dựa trên nội dung của phần thân SOAP.

Lưu ý về tính chống chối bỏ: Chúng ta sử dụng chữ ký số XML trong các bản tin SOAP nhằm đạt được tính chống chối bỏ giữa MSSP và AP. Tuy nhiên, cách dễ dàng nhất để bên ký phủ nhận bản tin là tuyên bố rằng khóa bí mật của họ đã bị lộ và kẻ tấn công đã ký bản tin đang bị tranh chấp. Để chống lại kiểu tấn công này, RP cần chứng minh được rằng khóa của bên ký chưa bị lộ tại thời điểm ký. Việc này đòi hỏi một hạ tầng đáng kể, bao gồm lưu trữ thông tin thu hồi chứng thư và các máy chủ cấp dấu thời gian để xác lập thời điểm bản tin được ký. Các nội dung này nằm ngoài phạm vi của tiêu chuẩn này.

Do đó, việc quy định thêm một khối tiêu đề bổ sung trong Tiêu đề SOAP chỉ là một bước tiến hướng tới tính chống chối bỏ, và không được coi là bước cuối cùng để hoàn thiện cơ chế này.

10.4 Ký số trên thiết bị di động

Giao diện Web được đặc tả trong tiêu chuẩn này có thể truyền tải nhiều loại chữ ký số khác nhau. Việc sử dụng chữ ký số không phù hợp hoặc trái phép là một mối đe dọa an ninh đối với người ký.

10.5 Các giao thức bảo mật

Như đã mô tả trước đó, giao thức TLS được sử dụng trong tiêu chuẩn này để cung cấp bảo mật kênh truyền. Trên thực tế, giao diện dịch vụ Web cho mô hình ký số trên thiết bị di động được đặc tả chạy trên nền tảng SOAP qua HTTP và trên lớp TLS. TLS cung cấp một kênh truyền được mã hóa và xác thực chạy trên nền TCP.

Thông thường, phía máy chủ luôn được xác thực bằng một chứng thư số. Các máy khách cũng có thể sở hữu chứng thư số để thực hiện xác thực lẫn nhau. Các cấp độ TLS khác nhau này được sử dụng tùy theo nhu cầu của AP và MSSP.

Ngoài ra, TLS sử dụng các thuật toán mật mã khác nhau cho việc ký số và mã hóa. Theo đó, giữa máy khách và máy chủ sẽ có một quá trình thương lượng về các thuật toán này để sử dụng cho bảo mật kênh truyền. Quá trình này được gọi là chọn tập hợp thuật toán mã hóa. Do đó, hệ thống có nguy cơ bị tấn công leo thang. Để ngăn chặn loại tấn công này, hệ thống PHẢI sử dụng tối thiểu TLS 1.2, khuyến nghị sử dụng TLS 1.3, và PHẢI vô hiệu hóa các phiên bản TLS/SSL cũ (SSL 3.0, TLS 1.0, TLS 1.1). Tiêu chuẩn này bắt buộc một danh sách các tập hợp thuật toán mã hóa có thể sử dụng, ưu tiên các bộ thuật toán hỗ trợ tính bảo mật chuyển tiếp tuyệt đối (Perfect Forward Secrecy - PFS):

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (TLS 1.2, hỗ trợ PFS)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2, hỗ trợ PFS)
- TLS_AES_128_GCM_SHA256 (TLS 1.3, khuyến nghị)
- TLS_AES_256_GCM_SHA384 (TLS 1.3, khuyến nghị)

CHÚ THÍCH: Các bộ thuật toán mã hóa TLS_RSA_WITH_3DES_EDE_CBC_SHA và TLS_RSA_WITH_AES_128_CBC_SHA (trao đổi khóa RSA tĩnh, không hỗ trợ PFS, sử dụng thuật toán 3DES đã bị khuyến cáo loại bỏ trên toàn cầu) không được phép sử dụng do không đáp ứng yêu cầu về an toàn thông tin hiện hành, đồng thời có nguy cơ ảnh hưởng đến giá trị pháp lý của chữ ký số theo quy định tại Luật Giao dịch điện tử 2023.

PHỤ LỤC A: SOAP FAULT Subcodes

Giá trị	Thông điệp	Mô tả
101	WRONG_PARAM	Lỗi trong các tham số của yêu cầu
102	MISSING_PARAM	Một tham số trong yêu cầu bị thiếu
103	WRONG_DATA_LENGTH	Dữ liệu cần ký (DTBS) quá lớn.
104	UNAUTHORIZED_ACCESS	AP không xác định hoặc mật khẩu sai hoặc AP yêu cầu một dịch vụ bổ sung mà nó chưa đăng ký
105	UNKNOWN_CLIENT	Người dùng cuối mà AP kết nối đến không được MSSP biết đến
106	HANDSHAKE_REQUIRED	MSSP muốn đàm phán trước với AP về việc sử dụng chữ ký XML trong các thông điệp
107	INAPPROPRIATE_DATA	MSSP không thể xử lý Loại MIME hoặc kiểu mã hóa đã cho của DTBS hoặc
108	INCOMPATIBLE_INTERFACE	Các tham số phiên bản phụ và/hoặc phiên bản chính không phù hợp với người nhận thông điệp
109	UNSUPPORTED_PROFILE	AP đã chỉ định Hồ sơ Chữ ký Di động mà MSSP không hỗ trợ
208	EXPIRED_TRANSACTION	Đã đến ngày hết hạn giao dịch hoặc đã hết thời gian chờ
209	OTA_ERROR	MSSP không thể liên hệ với thiết bị di động của người dùng cuối
401	USER_CANCEL	Khách hàng đã hủy giao dịch
402	PIN_NR_BLOCKED	Lỗi trong quá trình Chữ ký Di động trên thiết bị di động
403	CARD_BLOCKED	
404	NO_KEY_FOUND	
405	NO_URL_FOUND	
406	PB_SIGNATURE_PROCESS	
407	REGISTRATION_NOK	
422	NO_CERT_FOUND	Không tìm thấy chứng chỉ nào cho msisdn này
423	CRL_PB	Lỗi trong quá trình xác minh Chứng chỉ. Nền tảng không thể xác định liệu chứng chỉ có được kích hoạt hay không
424	CRL_EXPIRED	
425	ERROR_CERTIFICATE	
900	INTERNAL_ERROR ETSI	Lỗi không xác định

Bảng 14. SOAP FAULT Subcodes.

PHỤ LỤC B: MSS Status Codes

Giá trị	Thông điệp	Mô tả
100	REQUEST_OK	Yêu cầu đã được bên nhận (MSSP hoặc AP) chấp nhận.
400	USER_SIGN	Người dùng cuối đã nhận được yêu cầu chữ ký trên thiết bị di động của mình.
408	REGISTRATION_OK	
500	SIGNATURE	Chữ ký trên thiết bị di động đã được tạo thành công và sẵn sàng sử dụng
501	REVOKED_ CERTIFICATE	Chữ ký trên thiết bị di động đã được tạo thành công. Tuy nhiên, chứng thư của chủ thể ký đã bị thu hồi
502	VALID_SIGNATURE	Chữ ký trên thiết bị di động đã được tạo thành công và chữ ký hợp lệ
503	INVALID_SIGNATURE	Chữ ký XML đã được tạo thành công nhưng chữ ký không hợp lệ
504	OUSTANDING_TRANSACTION	
600	OK with PUSH confirmation	Thông điệp đã được nhận và đang được xử lý. Cần gửi xác nhận cho người dùng cuối (thông điệp văn bản SMS)
601	OK without PUSH confirmation	Thông điệp đã được nhận và đang được xử lý. Không có xác nhận cho người dùng cuối
602	NOK with PUSH Information	Có sự cố khi nhận thông điệp. Cần gửi thông tin cho người dùng cuối
603	NOK without PUSH information	Có sự cố khi nhận thông điệp. Không có thông tin nào được gửi đến

Bảng 15. MSS Status Codes.

CHÚ THÍCH: Các giá trị mã trạng thái (Status Code) tại Phụ lục này là mã con đặc thù của ứng dụng, được truyền tải bên trong phần tử StatusCode/StatusDetail của thông điệp SOAP Body (xem 8.4.3, 8.4.4) hoặc trong phần tử Fault Subcode của thông điệp lỗi SOAP (xem 9.6, Phụ lục A). Các giá trị này hoàn toàn độc lập với mã trạng thái HTTP (HTTP Status Code) và không được sử dụng thay thế cho mã trạng thái HTTP ở tầng vận chuyển; do đó việc trùng giá trị số (ví dụ: 500) với mã trạng thái HTTP không gây nhầm lẫn về mặt kỹ thuật khi phân tích đúng ngữ cảnh của thông điệp. Tổ chức cung cấp dịch vụ CÓ THỂ bổ sung các mã trạng thái, mã lỗi riêng ngoài danh mục tại Phụ lục A và Phụ lục B để phục vụ nhu cầu vận hành nội bộ, với điều kiện bảo đảm đầy đủ các mã trạng thái bắt buộc quy định tại tiêu chuẩn này nhằm bảo đảm khả năng liên thông và phục vụ kiểm thử tuân thủ.

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

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