Mobile Connect SIM Applet LoA 4 Extensios Specifications

Version 1.0.1

06 December 2022

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

Mobile Connect is a portfolio of mobile-based secure identity services delivered by mobile operators, that can be integrated into third-party Service Provider's applications to provide authentication, authorisation, and permissioned access to a User's attributes.

One of the key aspects of the Mobile Connect architecture is its support for "Pluggable Authenticators" such that a range of authenticators can be easily employed to meet different Operator/SP/user needs whilst also ensuring that Mobile Connect is future-proof and can accommodate new authentication mechanisms as they come along (e.g., providing support for advanced biometric authenticators or the inclusion of passive behavioural authentication methods).

IDY.10 Tech Mobile Connect SIM Applet Authenticator Specification [1] defines the requirements for the deployment of a SIM-Applet authenticator within Mobile Connect. The specification outlined three supportable authentication modes to provide levels of assurance: LoA2, LoA3 and LoA4 as described in Table 1. The specification only detailed B.1 and B.2 modes.

Level of Assurance	Description	Authentication mechanisms
1	N/A	N/A
2	Single-factor authentication ("something I have")	B.1 Click OK
3	Two-Factor authentication ("something I have" plus "something I know")	B.2 Enter Personal Code
4	Multi-factor plus PKI	B.3 Multifactor + Mobile Signature (certificates)

Table 1: Authentication modes

- B.1 uses the possession of device/card as the factor used for authentication by requesting user consent through a simple button press on the mobile device: e.g., 'click OK', 'Press 1' etc.; the challenge to the device/card is returned back with a signed response authenticating the possession of the device/card.
- B.2 is similar to B.1 but with the addition of a Personal Code challenge to the user (Personal Code entered by the user is verified on the applet).
- B.3 Mobile Signature would be used specifically for those use cases where secure, non-repudiated identity assertion is required for verticals such as banking and Government. This level of service would require robust identity proofing and the deployment of a certificate chain. Mobile Signature can also be used for other non-repudiation purposes, e.g. transaction authorisation or electronic document signature.
- Note that the adoption of B.3 does not change the User Experience (UX) which will depend on whether B.3 is used in conjunction with B.1 or B.2. However, if B.1 "Click OK" is used in conjunction with B.3, the overall level of assurance will be classed as LoA3 and not as LoA4.

This document defines the functional requirements for a certificate based SIM Applet authenticator including a Card Authentication Application provisioned to the user's SIM/UICC and supporting PKI to achieve a level of assurance of LoA4

This document may also use the terms ‘applet’ and ‘SIM Applet’ to designate the Card Authentication Application.

Future versions of this document will detail the OTA protocol commands and messages that Card Authentication Application and MSSP should support, in order to be compliant with this specification. Defining OTA protocol and commands assures interoperability between MSSPs and applets.

1.1 Audience

The target audience for this document are the Mobile Operator and SIM vendors service/technical departments who are considering implementing / deploying / upgrading the SIM applet module.

Readers of this document are expected to have familiarity with and a good understanding of the SIM Applet low level concepts, how SIM Applet messaging works and a good understanding of the Mobile Connect.

1.2 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.3 Definitions

Term	Description
Card manufacturer	Supplier of the SIM/UICC and resident software (e.g. firmware and operating system).
Device	Equipment, into which a SIM/UICC is inserted, that provides communication functions.
Mobile Network Operator	An entity providing access capability and communication services to its Customers through a mobile network infrastructure.
OTA Platform	An operator platform for remote management of SIM/UICCs.

1.4 Abbreviations

Term	Description
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRM	Customer Relationship Management
CSR	Certificate Signing Request
ECC	Elliptic Curve Cryptography
FIFO	First In First Out
GUI	Graphical User Interface
ID GW	Identity Gateway

Term	Description
IMEI	International Mobile Equipment Identity
INT	Interface
LoA	Level of Assurance
MSSP	Mobile Signature Service Provider
NFC	Near Field Communication
NMR	Network Measurement Results
OTA	Over-the-Air
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PoP	Proof of Possession
RA	Registration Authority
RAM	Remote Application Management
RMF	Remote File Management
RSA	A public-key cryptographic algorithm named after its inventors Rivest, Shamir and Adleman
SMS-PP MO	Short Message Service Point to Point Mobile Originated
SMS-PP MT	Short Message Service Point to Point Mobile Terminated
SOAP	Simple Object Access Protocol
SP	Service Provider
UI	User Interface
UICC	Universal Integrated Circuit Card
VA	Validation Authority

1.5 References

Ref	Doc Number	Title
[1]	IDY.10	Tech Mobile Connect SIM Applet Authenticator Specification
[2]	ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)
[3]	3GPP TS 23.040	Technical Specification Group Core Network and Terminals; Technical realisation of the Short Message Service (SMS)
[4]	3GPP TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
[5]	GSM 03.40	Digital cellular telecommunications system (Phase 2+); Technical realisation of the Short Message Service (SMS) Point-to-Point (PP) (GSM 03.40)
[6]	IDY.04	Mobile Connect Technical Architecture and Core Requirements
[7]	ETSI TR 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

2 Mobile Signature Service in Mobile Connect Architecture

With reference to IDY.10 Tech Mobile Connect SIM Applet Authenticator Specification [1], chapter 4, the following certificate life cycle management elements need to be added in order to complete the architecture for the B.3 Mobile Signature mode, (See Figure 1):

- Certification Authority (CA) platform (responsible for certificate issuance).
- Registration Authority (RA) platform (responsible for user registration and certificate signing request management).
- Validation Authority (VA) platform (responsible for providing information on whether signatures and certificates are valid or not).

The system contains at least four new interfaces (INT): INT9, INT10, INT11, INT12 and INT3c - as new branch of the Mobile Signature Service Provider (MSSP) interface. Implementations of interfaces INT9 and INT11 are business dependent decisions and the applet does not set any related requirements.

The RA and VA platforms are interfaced with MSSP. The definition of interfaces between VA and MSSP and between operator System and RA (optional) is out of scope in this document. However, the use of standard interfaces is recommended.

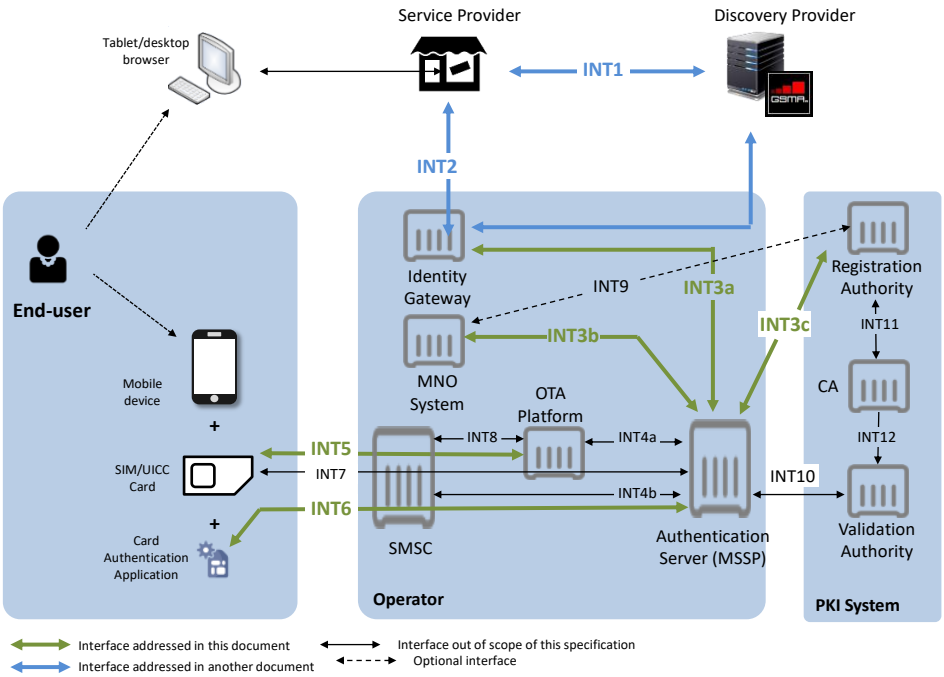

Figure 1: Complete Mobile Connect system architecture

3 Card Authentication Application: General Requirements

3.1 Hosting Device Requirements

The Card Authentication Application shall work across all mobile devices featuring a display and input capabilities (basic, feature and smartphones, tablets with SIM/UICC).

The device shall support:

- Short Message Service Point to Point Mobile Terminated (SMS-PP MT) and Short Message Service Point to Point Mobile Originated (SMS-PP MO) as defined in ETSI TS 102 223 [2] and in 3GPP TS 23.040 [3] (or either GSM 03.40 [5] for device with SIM cards)
- As a minimum, the following set of commands as defined in ETSI TS 102 223 [2] and 3GPP TS 31.111 [4]:

    - `PROVIDE LOCAL INFORMATION`: location information, International Mobile Equipment Identity (IMEI), Network Measurement Results (NMR), date and time, access technology) (optional)
    - Access to `TERMINAL PROFILE`
    - `SEND SHORT MESSAGE`
    - `ENVELOPE (SMS-PP DOWNLOAD)`
    - `DISPLAY TEXT`
    - `GET INKEY`
    - `GET INPUT`
    - `MORE TIME`
    - `PLAY TONE` (optional)

NOTE: The behaviour of some proactive commands used in this specification may be different depending on the device. This means that the end user experience may vary depending on device (e.g. timer management, wake-up from standby mode or play tone).

3.2 Applet General Requirements

The Card Authentication Application shall work on Universal Integrated Circuit Card (UICC) with SIM application (2G) or/and (U)SIM application (3G/4G), or SIM card (2G already defined in section 5 of the SIM Applet Authenticator Specification [1]).

However, in order to fulfil Public Key Infrastructure (PKI) requirements, the Card Authentication Application shall be used on UICC platforms equipped with hardware-based cryptographic accelerators supporting RSA or Elliptic Curve Cryptography (ECC). Please refer to Annex A for recommended key length.

The applet shall support:

- RSA or ECC cryptographic algorithms
- SHA-256 and SHA-384 and SHA-512 hash algorithm
- at least the Public Key Cryptography Standard (PKCS) #1 RSA Cryptography Standard v1.5 with padding scheme
- and optionally IETF RFC 5652 Cryptographic Message Syntax (CMS) based on PKCS#7
- on-board key generation

The MSSP shall know cryptographic mechanisms available on the applet in terms of encryption, hashing and padding functionalities.

It shall be possible to load, install and configure the Card Authentication Application by Over-the-Air (OTA).

The applet shall have its own life-cycle and can be managed independently of other card applets.

Options for applet deployment and card architecture for this specification shall be the same as detailed in the SIM Applet Authenticator Specification [1], section 6.3.

There are a number of ways in which the card could be used for providing the authentication capability:

- An applet as a standalone application and providing a simple-text based user interface.
- An applet as a SIM browser plug-in. The applet delegates the Graphical User Interface (GUI) management to the SIM browser (e.g. a S@T browser or a WIB browser).
- An applet as a standalone application, but delegating the GUI management to a native application on the device.

This document will only focus on the first option and is in scope for this authenticator applet, describing one possible way of implementing the applet and the protocol.

In order to ensure high completion rates using an OTA download deployment, the code (OTA package) of the Card Authentication Application size shall be as small as reasonably possible but still ensuring interoperability across Java Card platforms.

To ensure interoperability of a Java Card applet the implementation shall not use any SIM platform-proprietary library.

Depending on the targeted market segment, the operator is free to choose the most appropriate deployment mode (card issuance or OTA loading) for a given user.

3.3 Authentication, Signature Keys and Certificate Management

The applet shall support multiple key pairs (at least 2).Eeach key pair shall be assigned to a specific key usage (authentication or non-repudiation).

NOTE: Non-repudiation scenarios are not in the scope of the current release of this document.

For security reasons, private keys shall never be exported outside the applet.

Also, cryptographic operation using private key shall be performed only if the personal code is successfully verified.

The applet shall support on-board key pair generation (mandatory).

The activation of the applet and the registration of the public key should use a minimum number of commands and related SMS messages between the applet and the server (e.g. activation and registration command sent in one SMS and the returned SMS messages optimised to contain the public key and other data for registration and certificate issuance).

Optionally, during the enrolment/registration procedure the user certificate may be also stored in the applet, depending on applet capabilities. The MSSP shall know if the applet needs a user certificate.

In order to improve RSA crypto processor computing performances, the use of private keys in CRT format is recommended.

3.4 Personal Code Requirements

The user owns and chooses the personal code. The personal code value shall not be defined or initialised remotely, i.e. by a server or other external entity.

The personal code value is defined during the Certificate Issuance by means of the personal code creation process. The applet may support the use of a specific personal code, different from the authentication personal code, when the private key has a non-repudiation key usage (i.e. a Signature Key). The MSSP shall initialise or manage these personal codes properly.

Note: Non-repudiation scenarios are not in the scope of the current release of this CPAS document.

The personal code is locally stored within the Card Authentication Application and not shared with the server, the operator or any other party. In particular, it shall not be OTA-readable by the operator with Remote Application Management (RAM) or Remote File Management (RFM) functions. It shall not be readable from any other applet interfaces and shall not be accessible from any other application in the SIM Card.

It shall not be possible to alter the length of the personal code remotely after the first configuration as this can weaken the security. It may be possible to configure the personal code length just once during personalisation phase and this step shall always occur after the applet installation and before the first personal code setup done by the user.

The length of the personal code should be at minimum 4, either digits or alphanumeric characters. However, the CA may define another minimum length according to its policies. The user shall be informed about the required personal code format during the personal code creation and the personal code reset/change journeys.

3.5 User Journey

This section provides an overview of the different user flows for the Card Authentication Application mechanism and complements the user flows for the wider Mobile Connect proposition [6].

The Card Authentication Application shall support the customer journey as it is defined and described within the SIM Applet Authenticator Specification [1], section 3 (“User Journey on Device”), with the following exceptions.

3.5.1 First Registration Steps (Personal Code Setup and Certificate Enrolment) and Journey Examples

During the first registration of a new user to Mobile Connect service, the following steps shall be performed:

- User identity and user MSISDN shall be verified.
- Card Authentication applet shall be initialised, generating key pair(s).
- The user shall choose a personal code(s) required to use the private keys.
- Public-private key pairs in user's Card Authentication applet shall be registered and associated with user identity (a digital certificate shall be created for each key pair).

The user identification can be performed either with a face-to-face recognition or using other techniques. For example: online procedure through operator self-service portal or dedicated Mobile Connect portal, in cooperation with a partner such as a bank which can authenticate its customers by means of strong authentication and perform the first authentication or user identification step in the process.

In the last part of this section, several examples of the first registration journey in Mobile Connect are presented. However, the user identification flows proposed here may be modified or arranged depending on the regulations in force in the operator's country (e.g. allowing or not face-to-face recognition performed by a third party or the usage of self-service portals).

Also, depending on the registration process the RA/CA may generate a Proof of Possession (PoP) code (e.g. 8 digits, including checksum as last digit) which must be delivered to the user - via SMS, e-mail, printout or displayed in the registration User Interface (UI). The PoP code should generally be sent to the user and then verified using two different channels for security reasons - it may be sent to user by SMS, e-mail or printout and then managed or verified by RA/CA as part of the public key registration request message returned by the applet.

The Mobile Connect system knows if the applet already has the appropriate PKI key pair for registration (i.e. keys have been pre-generated during personalisation).

Two types of keys may be used in the Mobile Connect system: authentication and non-repudiation. Both keys may share the same personal code or they may use different personal codes with different lengths (e.g. authentication personal code length is 5 digits, non-repudiation personal code is 6 digits).

NOTE: Further details about non-repudiation scenarios will be described in a future release of this or other CPAS documents.

A first example of First Registration Journey is described here, considering that user registration can take place face-to-face at the operator shop and the operator acts as the Registration Authority (RA).

At the operator shop, the shop assistant will first identify the user (the user presents some form of identity document and the shop assistant checks the authenticity of the document) by agreed means (visual inspection and/or using some special equipment). The shop assistant verifies the identity of the user against the presented document.

Next, the shop assistant will start the registration process from the registration UI, which could be provided by the subscription management or CRM system used at the operator shops. The shop assistant clicks on a link that instructs the connected Mobile Connect system to start the user enrolment and the key registration process after verifying that the

Card Authentication applet is present on target SIM card. If the Card Authentication applet is not yet installed on the user's SIM card, the Mobile Connect System starts the applet provisioning process.

The Mobile Connect system sends a specific registration command to the Card Authentication applet to start the enrolment process in the applet and, if necessary, activates the applet first.

If the PoP Code is used during the enrolment process and, for example, it is managed and checked by the Card Authentication applet (see Figure 2):

- The applet displays a text to request the user to enter the PoP code (if included in the request).
- The applet validates the PoP code checksum, if the checksum validation has been requested.
- If the checksum fails, the applet asks the user to enter the PoP Code again. After a configurable number of false attempts, the applet shall display an error message indicating that the Mobile Connect service has not been properly activated and will return the error code to the Mobile Connect system.

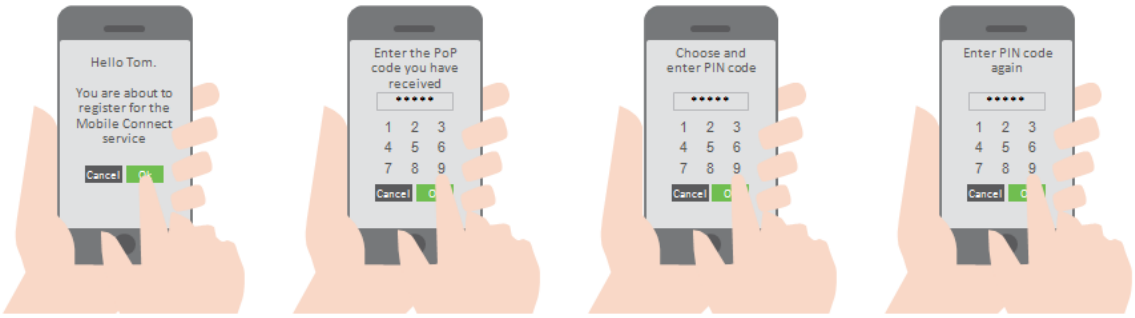

Figure 2: First registration: indicative flow

The registration command sent to the applet by the Mobile Connect system may also include both the command to generate the appropriate key pair (e.g. if a key pair is not present yet in the Card authentication applet or a key renewal is needed) and the command to choose the personal code (otherwise, Personal Code Creation Journey as in the SIM Applet Authenticator Specification [1] may occur). For security reasons, the key pairs (pre-generated or just-generated) present in the Card Authentication applet before the creation of the personal code shall be unusable until the user has successfully chosen his personal code.

The personal code creation shall be conducted only via the user's mobile phone. Therefore, the personal code remains private and only known to the user. The following steps may be taken in order to perform this:

- The applet displays a text to request the user to select and enter his or her personal code.
- The user enters the personal code (or clicks on the "Cancel" button).
- The applet displays a text to request the user to enter his or her personal code a second time.

- The user enters the personal code (or clicks on the “Cancel” button).
- If both personal codes match, the applet stores the new personal code value locally.
- If the personal codes do not match, the applet displays an error message on the screen of the mobile phone. If the maximum number of attempts is not reached, the applet shall restart the sequence; else the applet shall display a final error message indicating that the Mobile Connect service has not been properly activated.

Enrolment Procedure (i.e. key registration and digital certificate creation) follows these steps:

- The applet may generate a new key pair (e.g. if it does not already exist in the applet or if the certificate related to the existing one is expired – it may be going to expire or it may have been revoked, therefore a new key pair generation is required). Generally, if key generation is performed by a stand-alone command, it will send back the just-generated public key to the Mobile Connect system. The public key will be used by the RA platform to create the Certificate Signing Request (CSR).
- The applet will start the public key registration process, asking the user to enter the personal code to sign the public key (or CSR-derived data) with the corresponding private key. The applet will send the signed response to the Mobile Connect system (the signed response may contain also other data).
- The Mobile Connect system will receive the signed public key and other data. If the PoP code has not been validated yet using a separate flow, the PoP code validation is performed. The Registration Authority system sends the public key with other user-related data (or signed CSR) to the Certification Authority, requesting a certificate.
- The CA creates and issues the certificate and returns the status to the RA, which informs the Mobile Connect system of the successful certificate creation.
- The Mobile Connect system updates the user registration status and informs him about successful activation, e.g. sending the user an SMS.

If user clicks on the “Cancel” button at any of the steps, the applet shall display error message indicating that the Mobile Connect service has not been properly activated and will return the error code to the Mobile Connect system.

When user requires registration of an additional key pair (e.g. to be used in non-repudiation scenarios) the Enrolment Procedure must be repeated.

As suggested before, another example may be done using online service for user enrolment. In this case the user logs in to the portal/online service and clicks on a link that instructs the connected Mobile Connect system to send a specific command to the Card Authentication applet to start user enrolment and key registration process. The user will receive a PoP Code via e.g. SMS or email. The next steps will be the same as in the above-mentioned scenario. After a successful enrolment the user will receive an SMS informing of successful activation. The same confirmation can be shown on the portal/online service as well.

Other enrolment methods could rely on an SMS sent from the user's mobile phone to start the process, the use of self-service kiosk and an eID card as proof of identity, an online service combined with a strong authentication (e.g. smart card/token or eID card).

3.5.2 The "Click OK" Journey

Using "Click OK" is not allowed as it does not comply with LoA4 requirements.

The reason is that the user must be authenticated locally (e.g. by means of personal code verification) before allowing the applet to create authentication response (i.e. signing input data with user's private key).

3.5.3 The "Personal Code" Journey

If the service provider needs a high level of assurance (LoA4),they may require their users to authenticate, authorise or consent to a transaction by entering their personal code in order to create a digital signature with the Card Authentication Application. In this scenario, the Card Authentication Application will pop up a display text and will require a personal code entry. This pop-up display is triggered by the reception of a message that can only be sent by the Authentication Server (MSSP). The entry value is checked locally against the stored personal code value in the Card Authentication Application (see section 5.2).

The authentication platform should have the option to select a 'one-step' or 'two-step' user journey to meet local or operator requirements:

One-step user journey: The display message pop-up and the personal code input field are displayed in the same pop-up message.

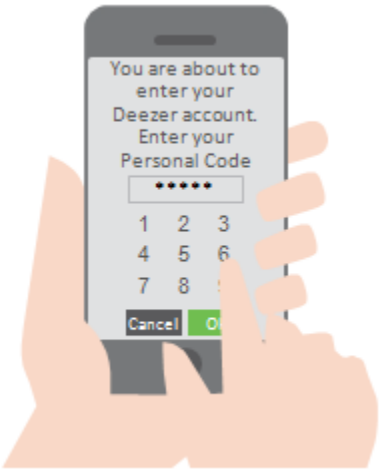

Figure 3: One-step user journey

Two-step user journey: the display message pop-up must first be acknowledged by the user. It is then followed by the personal code input field pop-up.

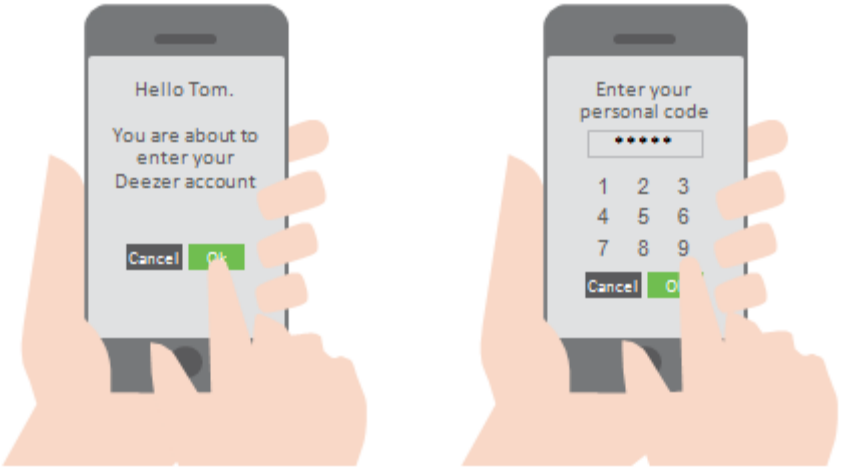

Figure 4: Two-step user journey

The Card Authentication Application shall implement a retry mechanism and optionally a time out management (recommended). In case of an erroneous personal code entry, several retry pop-ups (configurable) may be displayed before the applet returns a failed result to both the user and the MSSP. The user is then unable to use the Card Authentication applet until he performs unblocking of the personal code (see section 3.5.4). If a new authentication request arrives and the previous one is still being processed, a First In First Out (FIFO) model should be used for the requests. This will be handled by the MSSP and the Identity Gateway (ID GW).

In case of non-repudiation key usage (further details about these scenarios will be described in a future release of this or other documents), a transaction identifier (or similar code, such as a user-defined text string) shall be shown to the user on both the browser or the application on the device where the user had requested the signature and the Card Authentication applet display-message popup in order to give user the possibility to check what he's going to sign, according to "what you see is what you sign" rule.

3.5.4 Wrong Personal Code Journey/Unblock

After a configurable amount of consecutive wrong personal codes, the personal code is blocked and cannot be validated anymore.

The Mobile Connect system is notified of the situation in the response message sent from the applet. The Mobile Connect system will send an SMS informing of the situation and indicating how the user can unblock his personal code.

There are several possible solutions to unblock the personal code.

For example, the user navigates on the dedicated Mobile Connect portal and clicks on a 'Personal code Unblock' link or button (or any equivalent user experience). This service is available without requiring any user authentication. The Mobile Connect system sends an e-mail to a private e-mail address (provided during the registration process) containing an URL link allowing to trigger the unblock sequence.

The user logs on his private e-mail account and clicks on the link that instructs the Mobile Connect system to send a specific command to unblock the personal code on the user's mobile equipment - this command is generated and sent by the MSSP.

To enforce security, especially when the user's private e-mail account is configured on the user's smartphone, a mechanism like challenge/response may be used in order to authenticate the user before starting the Unblock Personal Code procedure.

Another solution could go through a Customer Care service of the home operator. The Customer Care agent, after having authenticated the user, may trigger the sending by the MSSP of the same specific command to unblock the personal code on the user's mobile equipment (what happens in details before the call of the MSSP is out of scope of this document). This is the preferred solution as it represents a more homogeneous option for the PKI services, where this flow shall verify the identity of the user.

It may also be possible to provide the user with an unblocking code. The Card Authentication applet would include an unblocking mechanism selectable from the applet menu and allowing the user to enter the unblocking code to reset the PIN after which the user has to create a new personal code. The unblocking code would be delivered together with the card or it could be requested from Customer Care service after proper identification and authentication of the user.

3.5.5 Change/Reset Personal Code Journey

The user navigates on the dedicated Mobile Connect portal and authenticates using the Mobile Connect service. The user clicks on a 'Personal Code Change' link or button (or any equivalent user experience). The Mobile Connect system sends a specific command triggering the personal code change on the user's mobile equipment (this command is generated and sent by the MSSP) after which the user has to create a new personal code.

As for the previous case, another possibility would be going through the Customer Care service.

In addition, the Card Authentication applet could include a mechanism to change the personal code selectable from the applet menu and allowing the user to create a new personal code. The user would be requested to enter the old personal code, enter the new personal code and re-enter it in order to store the value in the applet.

3.5.6 User Cancels the Authentication Request

In case the user cancels the authentication request on the pop-up message at the applet, the applet shall send the corresponding error code to the MSSP and close down. The MSSP shall send the error code to the ID GW. The service provider (SP) gets the authorisation error and may display an appropriate error message.

NOTE: The system shall never consider any action by the user, of any form, performed after the personal code entry as a cancelation by the user. User cancelation shall only be considered before the personal code entry.

3.5.7 Change Smart Card Within the Same Operator/New Card Issuance

At any time the user may subscribe to other operator services (e.g. Near Field Communication, NFC) requesting the issuance of a new card. The user will be requested to re-enrol to the Mobile Connect service as in 3.5.1.

3.5.8 Operator Change

At any time the user may change operator. In that case, a new card will be issued to the user. The user will be requested to re-register for Mobile Connect through their new operator. Note that the user may retain their existing MSISDN.

3.5.9 Unsubscribe from Mobile Connect

At any time, the user may unsubscribe from Mobile Connect service. The user navigates on the dedicated Mobile Connect portal and authenticates using the Mobile Connect service. The user clicks on an 'Unsubscribe' link or button (or any equivalent user experience). The Mobile Connect system sends a command requesting a signed confirmation using the Mobile Connect service. According to the service and CA policies, the Mobile Connect system could either:

- Simply unsubscribe the user at the MSSP level and send a request to the CA to revoke the user certificates.
- Or unsubscribe the user at MSSP level and send a command to deactivate and/or delete the key pairs and/or delete the Card Authentication applet (this command is generated and sent by the MSSP). It then sends request to the CA to revoke the user certificates.

As for the previous case, another possibility could be that the user goes through a Customer Care service.

3.5.10 Revoking the Certificates

At any time the user may request a certificate revocation due to several reasons (e.g. the mobile device is lost or has been stolen, the user thinks the personal code could have been compromised and he cannot or does not want to reset the Personal Code). The user navigates on the dedicated Mobile Connect portal and authenticates using the Mobile Connect service (or other agreed means if he no longer has the mobile device). The user clicks on a 'Revoke' link or button (or any equivalent user experience). According to service and CA policies, the Mobile Connect system could either:

- Send a request to the CA to revoke the user certificates, after confirmation from the CA change status of the user's keys and certificates in the MSSP as revoked.
- Or send a request to the CA to revoke the user certificates, after confirmation from the CA change status of user's keys and certificates in the MSSP as revoked.Send a command to deactivate and/or delete the key pairs and/or delete the Card Authentication applet (this command is generated and sent by the MSSP) if the device can be reached. Another possibility is to generate a new key pair overwriting the revoked one.

The user should go through a Customer Care service to start the process. The user will be requested to re-enrol to the Mobile Connect service.

3.5.11 Suspending and Reactivating the Service

At any time the user may request the service and certificate suspension due to several reasons (e.g. not planning to use the Mobile Connect service for a longer period of time and thus wanting to unsubscribe from the service temporarily). The user navigates on the dedicated Mobile Connect portal and authenticates using the Mobile Connect service. Then, the user clicks on a 'Suspend' link or button (or any equivalent user experience). The Mobile Connect system will then send request to the CA to suspend the user certificates.

According to service and CA policies, the Mobile Connect system could either:

- Set the user status to *suspended* and send a request to the CA to suspend the user certificates.
- Or set the user status to *suspended* and send a request to the CA to suspend the user certificates. After this, it would send a command to deactivate the Card Authentication applet (this command is generated and sent by the MSSP).

In order to re-activate the service and the certificates, the user navigates on the dedicated Mobile Connect portal and authenticates using some agreed means (e.g. see authentication mechanisms proposed in section 3.5.43.5.4) and clicks on a 'Re-activate' link or button (or any equivalent user experience).

As for the previous case, another possibility would be going through the Customer Care service for both actions.

3.5.12 Expired Certificate

Certificates have a certain validity period defined in the CA policies (e.g. two or five years). The validity or expiration date is included in the certificate data during the certificate creation process. When the digital signature is verified at the MSSP, the certificate is verified also. If the certificate has expired, the user cannot create a valid authentication response. Therefore, the user must re-enrol for Mobile Connect service in order to have valid certificates. Re-enrolment follows the same process as in section 3.5.1 First Registration 3.5.1 (Personal Code Setup and Certificate Enrolment).

3.5.13 Service Lifetime Extension

Before the expiration of the certificate, the operator may invite the user to extend the Mobile Connect service lifetime thanks to a certificate renewal. The user may be authenticated, through, for example, the Mobile Connect LoA4 Card Authentication Application itself.

This step shall be performed following the same flows in section 3.5.1 for the Enrolment Procedure but the registered key pair should be different from the one associated with the expiring certificate.

3.6 Multilanguage Support

The applet shall support multiple languages. At least, same predefined string reported in the SIM Applet Authenticator Specification [1] shall be used.

4 Card Authentication Application: Functional Requirements

The Mobile Signature Service Card Authentication Application shall implement the following basic functionalities supporting the use of PKI and certificates for user authentication and digital signature through an OTA interface (conforming to LoA4).

- Applet general information and personalisation
    - (During installation) Set a personal code length and a maximum number of retries, a number of key pairs slots, optionally algorithm key length (e.g. 2048bit for RSA).
    - Update applet data (e.g. text strings) and language selection.
    - Applet enabling/disabling (optional).
- Personal code management:
    - Reset personal code (authentication or signature when multiple PCs are used)
    - Unblock personal Code (authentication or signature when multiple PCs are used)
- Authentication and digital signature function: sign transaction (sign hash, and optionally sign text)
- Authentication/Signature Data management
    - Generate key pair (mapped on `SetAuthenticationHandlerData`)
    - Register public key (particular case of `SignTransaction`)
    - Get public key (mapped on e.g. `GetAuthenticationHandlerData`)
    - Import certificate (optional)
    - Delete key pair
    - Delete certificate (optional)

5 Detailed Procedures

The flows described in this section focus on the interactions between the ID GW, operator, MSSP, CA, RA, VA and Card Authentication applet (SIM applet), as well as hiding the other Mobile Connect aspects and components, such as the interactions between the service provider and the ID GW (over Open ID Connect). Refer to Mobile Connect Technical Architecture and Core Requirements [6] for further details on the Mobile Connect Architecture and APIs. Operator in these diagrams refers to a non-specified entity provided by the operator in order to execute management operations, which is open to choose by developers.

Any failure returned to the ID GW or operator by the MSSP in these sequences is an applicative error and not a Simple Object Access Protocol (SOAP) error or fault. SOAP faults are not illustrated.

Commands sent from MSSP to Card Authentication applet can be regrouped in a same SMS (provided that they fit a single SMS). Nevertheless for purpose of clarity, the following sequences illustrate one command per SMS.

5.1 First Registration (Personal Code Setup and Certificate Enrolment)

This section describes the steps that the Mobile Connect system shall perform to register a new user. These steps include personal code setup and user certificate enrolment.

Two flows are shown in order to cover all possible key generation procedures:

- The use of pre-generated key pairs (recommended when key generation is time-consuming).
- Key pair generation directly performed during the key registration command.

Both sequences are triggered by the RA on a request from the user.

NOTE: To simplify Figure 5 and Figure 6, the Int4a/b and INT5 interfaces allowing communication between MSSP and Card Authentication Application are not shown.

Pre-conditions:

- The user belongs to the operator.
- The user is not registered in the MSSP (this is the first registration).
- The user has already been authenticated by the operator (by another mechanism).
- The user wishes to register in the Mobile Connect service.

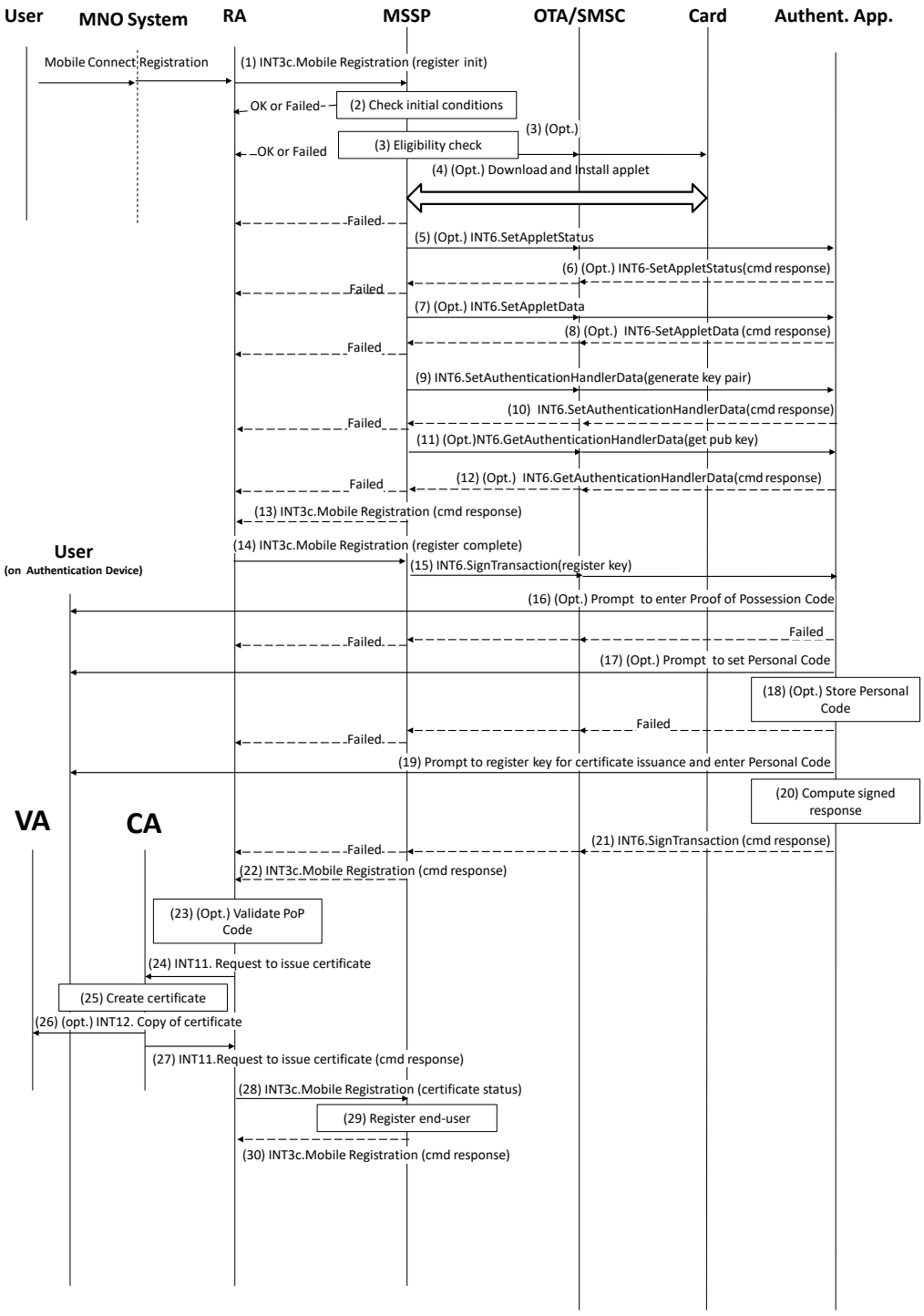

Figure 5: Sequence flow describing first registration: use of pre-generated key pair

Figure 5 describes the flow that Mobile Connect System shall follow when a pre-generated key pair is used.

1. RA calls the `INT3c-MobileRegistration` function, in `register_init` mode, with its relevant input data- at least the user identifiers (can be many, but at least MSISDN is mandatory), the requested signature profile.
2. The MSSP shall check that the user can be registered. The check shall include at least the following steps:

   - The request is well formed (all data present).
   - The user can be registered for the requested signature profile (e.g.the applet supports the type of key and certificate, the key index, there is enough memory for the key or the personal code is not blocked).

   If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.

3. If the registration request is acceptable, the MSSP shall check the eligibility of the user. The MSSP shall verify the user's mobile equipment status:

   - Is the Card Authentication applet already loaded and installed on the card? This check may be performed using simply the card content representation of the OTA Platform (if available), or by interrogating OTA the card. If yes (i.e. the card authentication applet is already loaded and installed on the card) the MSSP shall go to the step (5).
   - If a suitable (unregistered) PKI key pair already exists on the applet or if it needs to be generated.

4. Optionally, the MSSP may trigger the loading and installation of the applet. This step is performed using the OTA platform functions and is out of scope of this specification. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end.
5. Optionally the MSSP may send the `INT6-ChangeappletStatus` function to the applet to activate the applet if the applet exists but it has not been activated yet.
6. The applet shall then return the response of the `INT6-ChangeappletStatus` function to the MSSP. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end.
7. Optionally the MSSP may send the `INT6-SetappletData` function to modify the applet configuration if the applet exists and has been activated.
8. The applet shall return the response of the `INT6-SetappletData` function to the MSSP. In case of error during this step, the MSSP may return a response indicating the failure, and the procedure may end.
9. If no unregistered key pair is already present in card authentication applet, `INT6-SetAuthenticationHandlerData` is sent to the applet that shall perform key pair generation.
10. The applet sends back to the MSSP platform the public key. When the applet supports multiple slots to contain different key pairs, steps from 9 to 12 may be repeated for each key slot in order to complete pre-generation of all key pairs.
11. Optionally, if the MSSP platform has not received the public key complete of all its parts, it may use `INT6.GetAuthenticationHandlerData` asking for public key.

12. The MSSP sends back the `INT3c.MobileRegistration` response to RA, sending back public key pre-generated on the user SIM card. MSSP shall send back public key of first not-yet-registered key pair created with requested key usage.
13. The RA shall send `INT3c.MobileRegistration`, in `register_complete` mode, to MSSP to start key registration and enrolment. This request shall include at least user identifiers (there can be many, but at least the MSISDN is mandatory), the requested signature profile and key usage information. The MSSP shall register first not-yet-registered key pair created with requested key usage.
14. MSSP shall complete key registration sending `INT6.SignTransaction(register key)`"
15. Optionally, the applet may request the user to enter a Proof of Possession code at this stage if he was given the code at the start of the registration process and it has not been previously verified using other mechanism. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
16. Optionally, if the MSSP platform has never sent `INT6.ManagePersonalCode` to the applet before, the applet shall request the user to choose his personal code and re-enter it in order to store the value in the applet. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end. If the personal code for desired key usage already exists, the applet shall not request the user to choose a new personal code at this stage.
17. The applet shall store the personal code value in the applet.
18. Then the applet shall ask the user to enter his personal code in order for the applet to compute a signed response to the `INT6-SignTransaction(register key)` function. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
19. The signed response to the `INT6-SignTransaction` function is computed over the public key part of the PKI key pair and other data which can be used for certificate request for the CA. The private key part of the key pair is used to sign the response containing, for example, a CSR or PKCS#10 derived construct. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
20. The applet shall send the signed response to the `INT6-SignTransaction` function.
21. The MSSP sends the RA the response to the `INT3c-MobileRegistration` function with relevant output data, for example, a signed CSR or PKCS#10 derived construct. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end.
22. If the PoP code is used, the RA will validate the code before continuing with the process.
23. The RA will send a certificate issuance request with the necessary data to the CA (through INT11).
24. The CA shall create the certificate for user and publish it in its data repository and can optionally make available a copy of the certificate to the VA (through INT12).
25. The CA shall return the status of the certificate creation to RA (through INT11). Optionally it can also return the certificate
26. The RA will call the `INT3c-MobileRegistration` function, in `certificate_status` mode, to inform the MSSP of certificate creation and the user and the key are now registered. Optionally, the certificate may be sent to MSSP server.

27. The MSSP shall update its local database to reflect the newly registered user, the key pair (optionally certificate) and the applet status.
28. The MSSP shall return the response of the `INT3c-MobileRegistration` function indicating that the user has been registered.

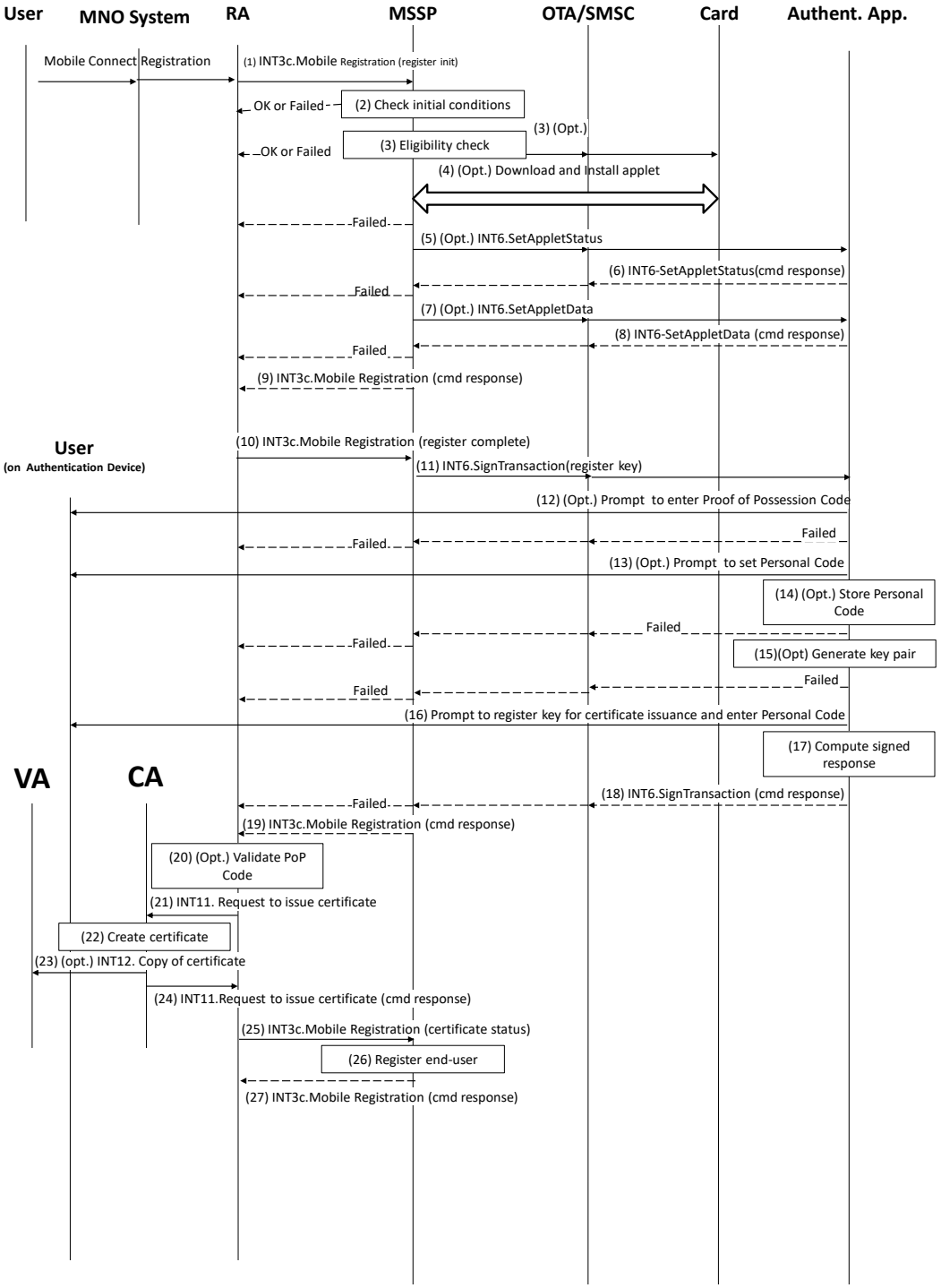

Figure 6: Sequence flow describing first registration: key pair generated during registration step

1. RA calls the `INT3c-MobileRegistration` function, in `register_init` mode, with its relevant input data: at least user identifiers (there can be many, but at least the MSISDN is mandatory), the requested signature profile.
2. The MSSP shall check that the user can be registered. The check shall include at least the following steps:

   - The request is well formed (all data present).
   - The user can be registered for the requested signature profile (e.g. the applet supports the type of key and certificate, the key index, there is enough memory for the key, the personal code is not blocked.).

   If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.

3. If the registration request is acceptable, the MSSP shall check the eligibility of the user. The MSSP shall verify the user's mobile equipment status:

   - Is the Card Authentication applet already loaded and installed on the card? This check may be performed using simply the card content representation of the OTA platform (if available), or by interrogating OTA the card. If yes (i.e. the Card Authentication applet already loaded and installed on the card) the MSSP shall go to step (5).
   - If a suitable (unregistered) PKI key pair already exists on the applet or if it needs to be generated.

4. Optionally, the MSSP may trigger the loading and installation of the applet. This step is performed using the OTA platform functions and is out of scope of this specification. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end. Key generation may be performed when user is not aware of it taking place.

   If the Card Authentication applet cannot be loaded and installed, the MSSP shall return a response indicating the failure, and the procedure shall end.

5. Optionally the MSSP may send the `INT6-ChangeappletStatus` function to the applet to activate the applet if the applet exists but it has not been activated yet.
6. The applet shall then return the response of the `INT6-ChangeappletStatus` function to the MSSP. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end.
7. Optionally the MSSP may send the `INT6-SetappletData` function to modify the applet configuration if the applet exists and has been activated.
8. The applet shall return the response of the `INT6-SetappletData` function to the MSSP. In case of error during this step, the MSSP may return a response indicating the failure, and the procedure may end.
9. MSSP sends back `INT3c-MobileRegistration` response to RA.

10. RA shall send `INT3c-MobileRegistration`, in `register_complete` mode, to MSSP to start key registration and enrolment; request shall include at least user identifiers (can be many, but at least MSISDN is mandatory), the requested signature profile and key usage information.
11. MSSP shall complete key registration sending `INT6-SignTransaction(register key`.
12. Optionally the applet may request the user to enter a Proof of Possession code at this stage if he was given the code at the start of the registration process and it has not been previously verified using other mechanism. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
13. Optionally, if MSSP Platform has never sent `INT6-ManagePersonalCode` to the applet before, the applet shall request the user to choose his personal code and re-enter it in order to store the value in the applet. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end. If the Personal code for the key type already exists the applet shall not request the user to choose a new personal code at this stage.
14. The applet shall store the personal code value in the applet.
15. The applet shall then generate the PKI key pair of the requested type.

    Optionally if the PKI key pair already exists then a new key pair is not generated.

16. The applet shall then ask the user to enter his personal code in order for the applet to compute a signed response to the `INT6-SignTransaction(register key)` function. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
17. The signed response to the `INT6-SignTransaction` function is computed over the public key part of the PKI key pair and other data which can be used for certificate request for the CA. The private key part of the key pair is used to sign the response containing e.g. a CSR or PKCS#10 derived construct. In case of error during this step, the applet shall return a response indicating the failure, and the procedure shall end.
18. The applet shall send the signed response to the `INT6-SignTransaction` function.
19. The MSSP sends the RA the response to the `INT3c-MobileRegistration` function with relevant output data e.g. a signed CSR or PKCS#10 construct. In case of error during this step, the MSSP shall return a response indicating the failure, and the procedure shall end.
20. If the PoP code is used, the RA will validate the code before continuing with the process.
21. The RA will send a certificate issuance request with the necessary data to the CA (through INT11).
22. The CA shall create the certificate for user and publish it in its data repository and can optionally make available a copy of the certificate to the VA (through INT12).
23. The CA shall return the status of the certificate creation to RA (through INT11). Optionally it can also return the certificate
24. The RA will call the `INT3c-MobileRegistration` function, in `certificate_status` mode, to inform the MSSP of certificate creation and the user and the key are now registered. Optionally, the certificate may be sent to MSSP Server
25. The MSSP shall update its local database to reflect the newly registered user, the key pair (optionally certificate) and the applet status.

26. The MSSP shall return the response of the `INT3c-MobileRegistration` function indicating that the user has been registered.

NOTE: In both flows, if at one point there is an error or if the user aborts the process, then the applet should be reset to initial status. An Authentication Handler aborted setting should be deleted, with associated applicative keys and if no other Authentication Handlers are present, then the applet data parameters should also be deleted including the personal code.

The key pairs should not be available for use outside the enrolment and first registration procedure until the entire procedure itself is completed successfully (e.g. a generated key pair can be used to sign its own CSR but cannot be used to sign any other authentication data from any interface or SP until the entire enrolment procedure is completed successfully).

5.2 The Personal Code Journey (Authentication or Signing Request)

The following figure describes the call flow for the case where the user, navigating a service provider's service, clicks on a Mobile Connect button (or something equivalent depending on the service provider's service implementation) and triggers the authentication/signing using the mobile phone of the user. This sequence is triggered by the user.

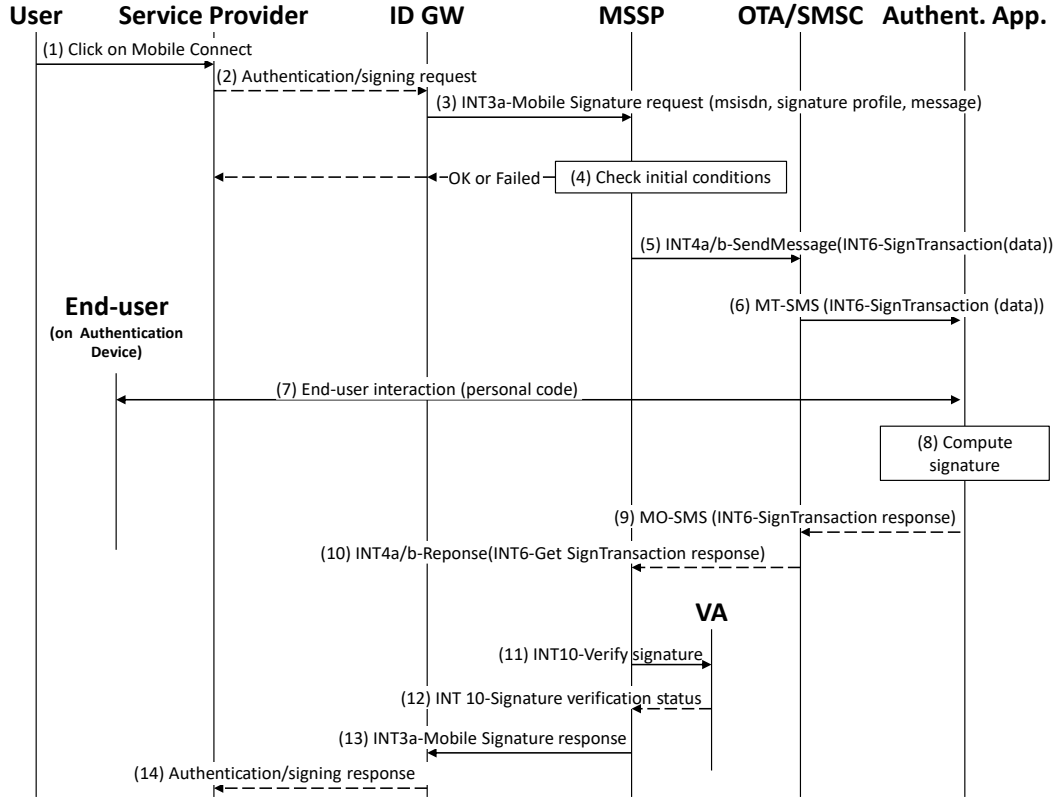

Figure 7: Sequence flow for the authentication journey

NOTE: This flow is an indicative flow in the applet / MSSP authentication context, and hides the other Mobile Connect aspects and components, for example, the ID GW.

1. The user navigating a service provider's service clicks on a Mobile Connect button.

2. By a process that is out of scope of this document, the ID GW receives the authentication/signing request.
3. The ID GW calls the `INT3a-MobileSignature` function with its relevant input data - at least the end-user identifier (e.g. the MSISDN, signature profile, data/hash to be signed or message).
4. The MSSP verifies that the ID GW request is acceptable. The check shall include at least the following steps:

   - the request is well formed (all data is present).
   - the user is already registered for the requested signature profile.
   - the user is activated.
   - a valid certificate exists for the user and the key type.

   If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.

5. The MSSP shall send a secure message targeting the SIM applet and containing the `INT6-Sign transaction` command with its relevant input data. Depending on the SIM/UICC architecture, the MSSP may either manage the secure message part or delegate it to the operator OTA.
6. The SIM applet handles the user experience as described in user journey in section 3.5.3.
7. The SIM applet generates signature data.
8. The SIM applet returns the MO-SMS containing the execution data of the `INT6-Sign Transaction` command to the MSSP.
9. The MSSP receives the authentication data returned by the SIM applet. Depending on the SIM/UICC architecture, the MSSP may have to additionally handle the secure transport layer. Then, the MSSP sends the authentication data to the Validation Authority for signature verification and receives the status, for example, the signature OK and certificate valid.
10. The MSSP returns the response of the "`NT3a-MobileSignature` function indicating if the user has been authenticated or not, or depending on the request it may also return the signed data/hash.
11. The ID GW returns the authentication/signing response to the service provider by a process which is out of scope of this document.

    This procedure illustrates the 'Asynchronous Server-Server Mode' defined in the SIM Applet Authenticator Specification [1], section 9.1.2.1.

5.3 Wrong Personal Code Journey/Unblock Personal Code

The following figure describes the call flow corresponding to the personal code unblock procedure. This sequence is triggered by the operator on a request from the user.

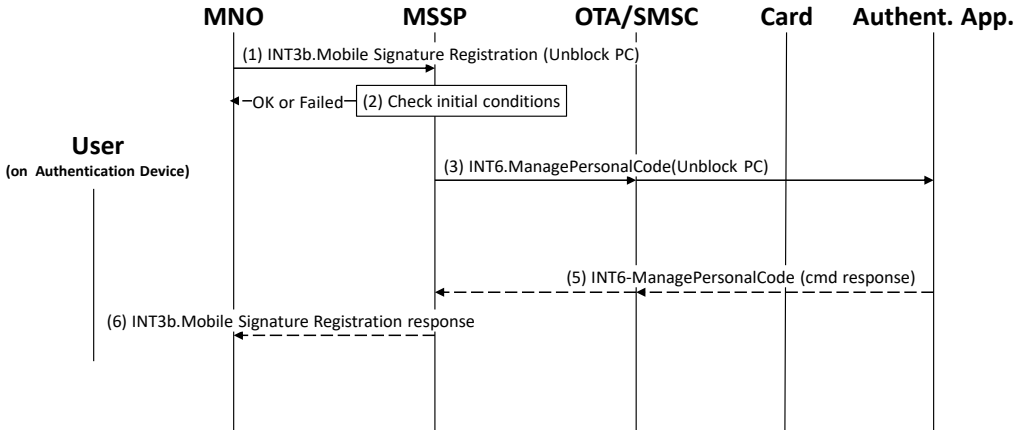

Figure 8: Sequence flow describing the personal code unblocking

NOTE: To simplify the figure, the Int4a/b and INT5 allowing communication between MSSP and Card Authentication Application are not illustrated.

Pre-conditions:

- The user is already registered in the MSSP.
- The user is registered for the LoA4 authentication mode.
- The user has been authenticated by the operator by a mean out of scope of this document.

1. The operator calls the `INT3b-MobileSignatureRegistration` function in the "Unblock PC" mode, with its relevant input data.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode and that user is activated for Mobile Connect. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.
3. The MSSP shall send the INT6-ManagePersonalCode function to the applet to unblock the personal code stored on the applet. The applet can display a message to the user via DISPLAY TEXT.
4. The applet shall return the response of the `INT6-ManagePersonalCode` function to the MSSP.
5. The MSSP shall return the response of the `INT3b-MobileSignatureRegistration` function to the operator.

Alternatively, the applet provides the means to unblock the personal code locally, i.e. select. The user would be requested to enter unblocking code, then enter the new personal code and re-enter it in order to store the value in the applet.

5.4 Change/Reset Personal Code Journey

The following figure describes the call flow corresponding to the User Personal Code reset. This sequence is triggered by the operator on a request from the user.

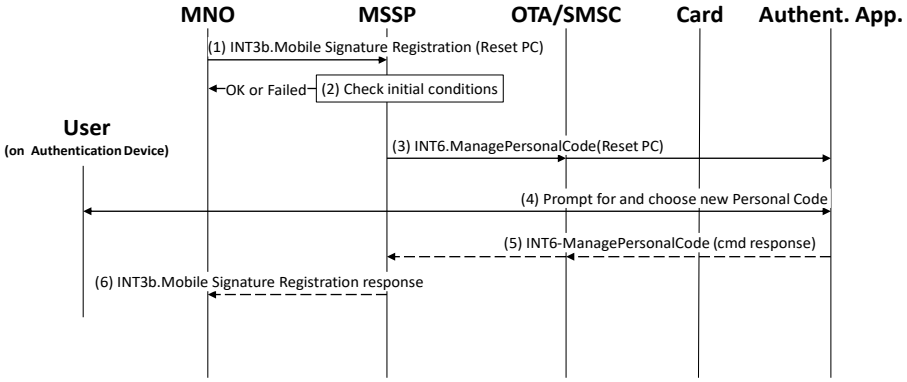

Figure 9: Sequence flow for change/reset personal code journey

NOTE: To simplify the figure, the Int4a/b and INT5 allowing communication between MSSP and the Card Authentication application are not illustrated.

Pre-conditions:

- The user is already registered in the MSSP.
- The user is registered for the LoA4 authentication mode.
- The user has been authenticated by the operator by a mean out of scope of this document.

1. The operator calls the `INT3b-MobileSignatureRegistration` function in the "Reset PC" mode, with its relevant input data.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode and that the user is activated for Mobile Connect. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.
3. The MSSP shall send the `INT6-ManagePersonalCode` function to the applet to reset the personal code stored on the applet.
4. The applet shall request the user to enter his new personal code according to the user journey described in section 3.5.5. In analogy with the SIM Applet Authenticator Specification [1], the applet shall also unblock the personal code (resetting retry counter to its maximum value).
5. The applet shall return the response of the `INT6-ManagePersonalCode` function to the MSSP.
6. The MSSP shall return the response of the `INT3b-MobileSignatureRegistration` function to the operator.

Alternatively, the applet provides the means to change the personal code locally, i.e. selectable from the applet menu and allowing the user to create a new personal code. The user would be requested to enter the old personal code, then enter the new personal code and re-enter it in order to store the value in the applet.

5.5 Change Smart Card within the Same Operator/New Card Issuance

The procedure is the same as for the first registration because the sser will get a new card and therefore needs to go through the complete registration process including setting the personal code. This sequence is triggered by the operator on a request from the user.

Pre-conditions:

- The user is already registered in the MSSP for the LoA4 authentication mode.
- The user's new card is already provisioned within the OTA Platform and associated with the same (or new MSISDN).
- The user's new card is able to host the Card Authentication Application.
- The user has been authenticated by the operator by a mean out of scope of this document.

It is assumed that the user keeps his MSISDN when the card is changed.

5.6 Operator Change

The procedure is the same as for the first registration because the user will get a new card and therefore needs to go through the complete registration process including setting the personal code. This sequence is triggered by the operator on a request from the user.

Pre-conditions:

- The user belongs to the operator.
- The user has not been registered for the LoA 4 authentication mode in the new MSSP.
- The user's new card is already provisioned within the OTA Platform and associated with the same (or new MSISDN).
- The user's new card is able to host the Card Authentication Application.

The user might keep his MSISDN when the card is changed depending on if number portability service is available.

5.7 Unsubscribe Mobile Connect

This sequence is triggered by the RA or the operator either on a request from the user or for some other valid reason (e.g. the user is no longer a customer of the operator). Unsubscribing from the service will result in certificate revocation also.

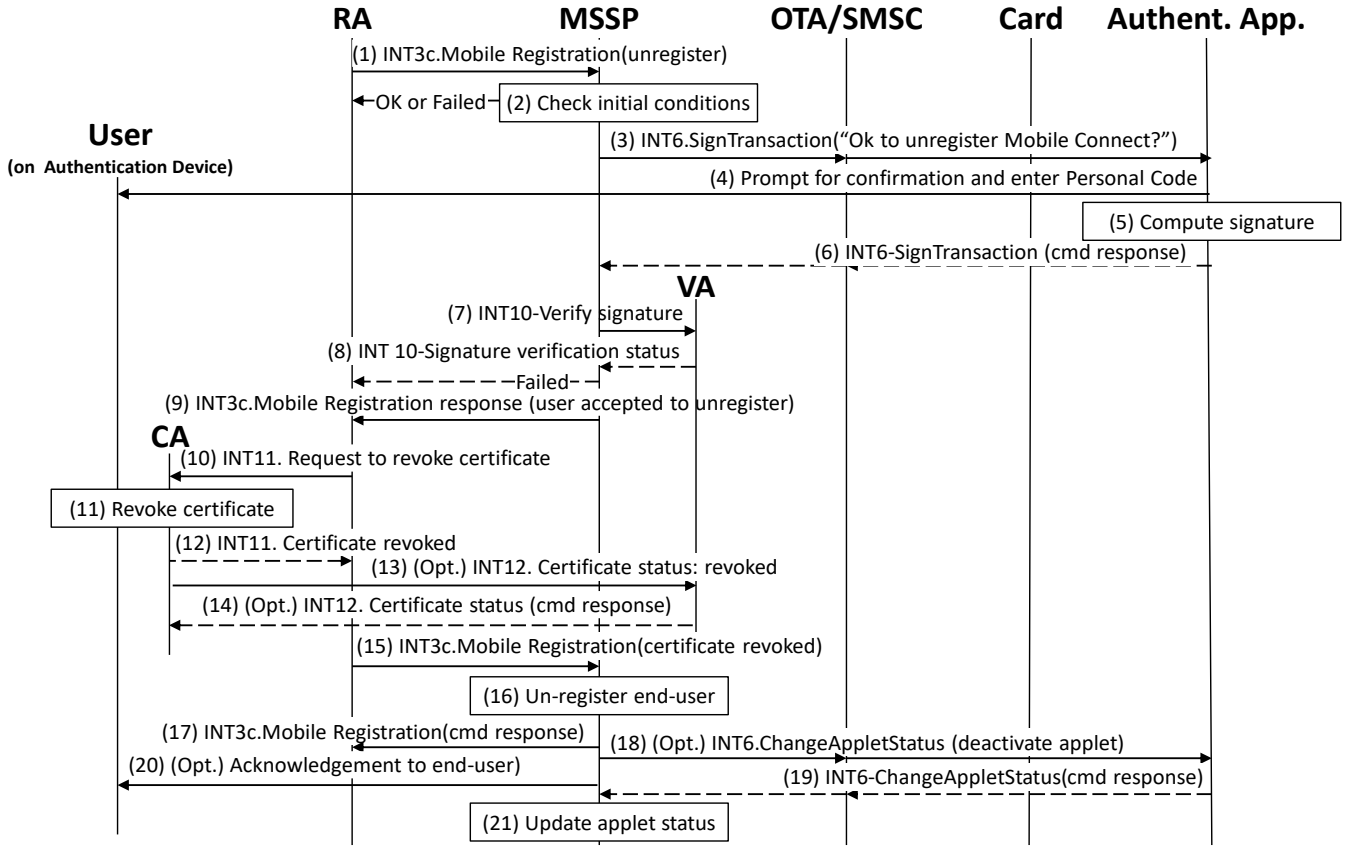

Figure 10: Sequence flow describing the unsubscribing of the user

NOTE: To simplify the figure, the Int4a/b and INT5 allowing communication between MSSP and Card Authentication Application are not illustrated.

Pre-conditions:

- The user is still registered in the MSSP
- The user's applet is still in activated state, the card is provisioned within the OTA Platform and associated with MSISDN belonging to user.
- The user has been authenticated by the operator by a mean out of scope of this document.

The request for the user to respond with a signature can be optional and the process can skip steps 3-9.

If the user has several certificates associated with the MSSP/CA, the steps 10-17 have to be repeated for each certificate.

1. The RA calls the `INT3c-MobileSignatureRegistration` function in the "Unregister" mode, with its relevant input data.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode, that user is activated for Mobile Connect, that the applet is still active and that the personal code has not been blocked. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.

3. The MSSP shall send a secure message targeting the SIM applet and containing the `INT6-Sign transaction` command with its relevant input data asking permission from the user to unsubscribe from the service. Depending on the SIM/UICC architecture, the MSSP may either manage the secure message part or delegate it to the operator OTA.
4. The SIM applet shall request the user to enter his personal code according to the user journey described in section 3.5.5 to sign the request to unsubscribe.
5. The SIM applet shall compute the signed response to the request.
6. The SIM applet returns the MO-SMS containing the execution data of the `INT6-Sign Transaction` command to the MSSP.
7. The MSSP receives the signed data returned by the SIM applet. Depending on the SIM/UICC architecture, the MSSP may have to additionally handle the secure transport layer. Then, the MSSP sends the authentication data to the Validation Authority for signature verification and receives the status, for example, the signature OK and certificate valid.
8. The MSSP returns the response of the `INT3c-MobileSignatureRegistration` function indicating whether the user has accepted to unregister from the service or not, or depending on the request it may also return the signed data/hash.
9. The RA will send a request to the CA to revoke the user certificate (through INT11).
10. The CA revokes the certificate and returns the status information to the RA.
11. Optionally the CA will send the certificate status information also to the VA (through INT12).
12. The RA will call `INT3c-MobileSignatureRegistration` function to notify the MSSP the user certificate has been revoked.
13. The MSSP shall update its local database with the status information: the user un-registered, certificate has been revoked.
14. The MSSP returns to the RA the response of the `INT3c-MobileSignatureRegistration` function.
15. Optionally the MSSP may deactivate the SIM applet.
16. The user may receive acknowledgment of successful unregistration.
17. The MSSP updates the applet status in the local data base.

5.8 Revoking the Certificates

This sequence is triggered by the RA or operator either on a request from the user or for some other valid reason (e.g. the user is no longer a customer of the operator or the user has lost the mobile device containing the card with the authentication applet).

Pre-conditions:

- The user is still registered in the MSSP.
- The user’s certificates are still valid (have not expired or have not been revoked).
- User has been authenticated by the operator by a mean out of scope of this document.

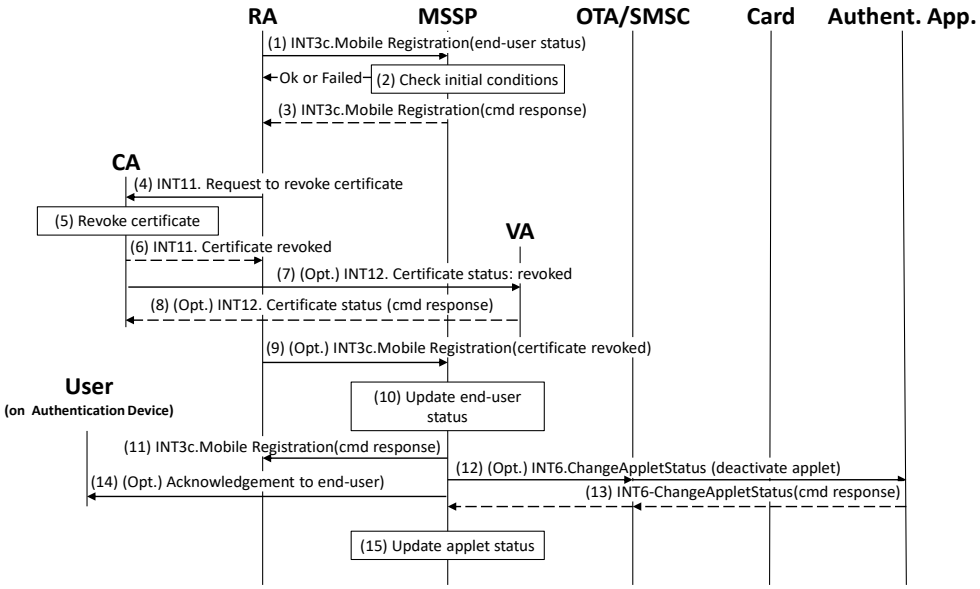

Figure 11: Sequence flow describing user certificate revocation

If the user has several certificates associated with the MSSP/CA, the steps 4-8 have to be repeated for each certificate.

1. The RA calls the `INT3c-MobileSignatureRegistration` function to verify the initial pre-conditions.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode, that user is activated for Mobile Connect, that the applet is still active and that the certificates are still valid. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.
3. The MSSP returns the response of the `INT3c-MobileSignatureRegistration` function indicating the status of the pre-conditions.
4. The RA will send a request to the CA to revoke the user certificate (through INT11).
5. The CA revokes the certificate and returns the status information to the RA.
6. Optionally the CA will send the certificate status information also to the VA (through INT12).
7. The RA will call `INT3c-MobileSignatureRegistration` function to notify the MSSP the user certificate has been revoked.
8. The MSSP shall update its local database with the status information: user certificate has been revoked.
9. The MSSP returns to the RA the response of the `INT3c-MobileSignatureRegistration` function.
10. Optionally the MSSP may deactivate the SIM applet.
11. The user may receive acknowledgment of certificate revocation.
12. The MSSP updates the applet status in the local data base.

5.9 Suspending the Service

This sequence is triggered by the RA or operator either on a request from the user or for some other valid reason (e.g. the user does not want to use the service for some period of time).

Pre-conditions:

- The user is still registered in the MSSP.
- The user's certificates are still valid (have not expired and/or revoked).
- The user has been authenticated by the operator by a mean out of scope of this document.

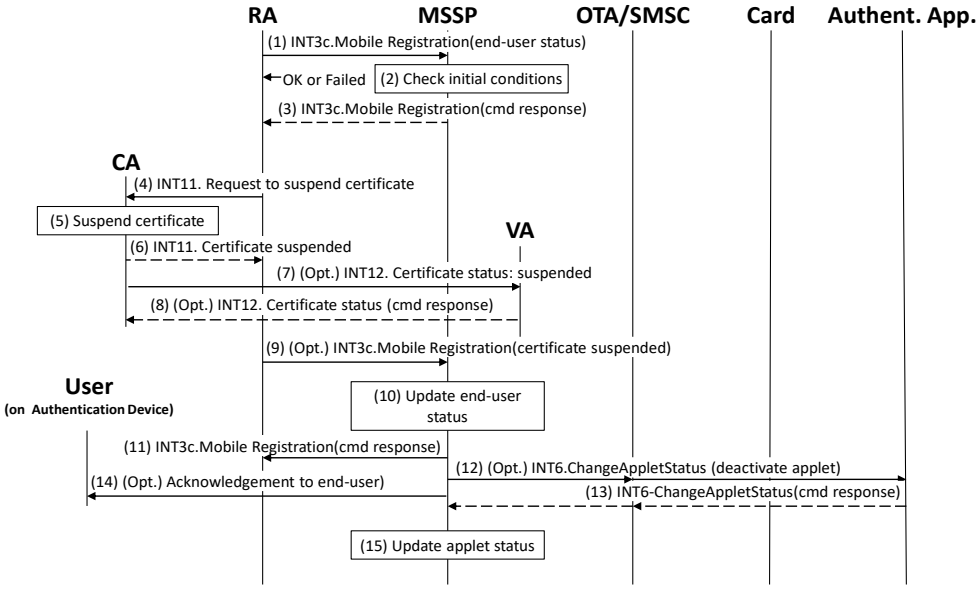

Figure 12: Sequence flow describing service and certificate suspension

If the user has several certificates associated with the MSSP/CA, the steps 4-8 have to be repeated for each certificate.

1. The RA calls the `INT3c-MobileSignatureRegistration` function to verify the initial pre-conditions.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode, that user is activated for Mobile Connect, that the applet is still active and that the certificates are still valid. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.
3. The MSSP returns the response of the `INT3c-MobileSignatureRegistration` function indicating the status of the pre-conditions.
4. The RA will send a request to the CA to suspend the user certificate (through INT11).
5. The CA suspends the certificate and returns the status information to the RA.
6. Optionally, the CA will send the certificate status information also to the VA (through INT12).
7. The RA will call `INT3c-MobileSignatureRegistration` function to notify the MSSP the user certificate has been suspended.
8. The MSSP shall update its local database with the status information: user certificate has been suspended.
9. The MSSP returns to the RA the response of the `INT3c-MobileSignatureRegistration` function.
10. Optionally the MSSP may deactivate the SIM applet.

11. The user may receive acknowledgment of certificate suspension.
12. The MSSP updates the applet status in the local data base.

5.10 Reactivating the Service/Certificate

User may have stopped using the Mobile Connect service (but has not unsubscribed) and therefore the certificates have been suspended preventing the use of the service. The status of the certificate(s) has to be changed to active/re-activated.

The following figure describes the flow to re-activate user certificate. If the user has several certificates associated with the MSSP/CA the steps have to be repeated for each certificate.

Pre-conditions:

- The user is still registered in the MSSP.
- The user's certificates are still valid (have not expired).
- The user has been authenticated by the operator by a mean out of scope of this document.

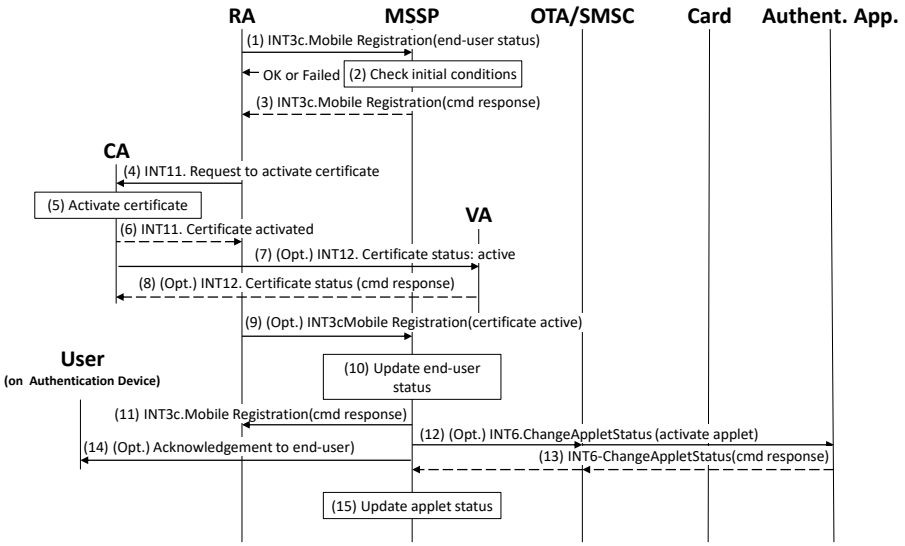

Figure 13: Sequence flow describing service and certificate reactivation

If the user has several certificates associated with the MSSP/CA, the steps 4-8 have to be repeated for each certificate.

1. The RA calls the `INT3c-MobileSignatureRegistration` function to verify the initial pre-conditions.
2. The MSSP shall verify that the user is registered for the LoA4 authentication mode, that user is activated for Mobile Connect, that the applet is either active or deactivated and that the certificates are still valid. If any of the conditions to be verified are not satisfied, the MSSP shall return a response indicating the failure, and the procedure shall end.
3. The MSSP returns the response of the `INT3c-MobileSignatureRegistration` function indicating the status of the pre-conditions.
4. The RA will send a request to the CA to re-activate the user certificate (through INT11).

5. The CA re-activates the certificate and returns the status information to the RA.
6. Optionally the CA will send the certificate status information also to the VA (through INT12).
7. The RA will call `INT3c-MobileSignatureRegistration` function to notify the MSSP the user certificate has been re-activated.
8. The MSSP shall update its local database with the status information: user certificate has been re-activated.
9. The MSSP returns to the RA the response of the `INT3c-MobileSignatureRegistration` function.
10. Optionally the MSSP may activate the SIM applet if it has been deactivated previously.
11. The user may receive acknowledgment of certificate re-activation.
12. The MSSP updates the applet status in the local data base.

5.11 Expired Certificate

The certificate validity period is normally 1-5 years depending on the CA policies. After the certificate expires, the user needs to have valid certificate(s) in order to continue using the Mobile Connect service. The procedure to get valid certificates is the same as for first registration because the user needs to go through the complete registration process including setting the personal code. Also, depending on CA policies and local regulation, generation of new key pair may be a mandatory step during certificate renewal process.

Pre-conditions:

- The user is already registered in the MSSP.
- The user's applet is still in activated state, the card is provisioned within the OTA Platform and associated with the same MSISDN.
- The user's new card is able to host the Card Authentication Application.

5.12 Service Lifetime Extension

This sequence is triggered by the RA or the operator on a request from the user (e.g. after receiving a remainder from operator about an imminent certificate expiration).

A new key pair, different from the one associated with expiring certificate, shall be registered in order to guarantee to the user the service availability (same flows described in section 5.1 may be used).

Pre-conditions:

- The user is still registered in the MSSP.
- The user's certificates are still valid (have not expired or have not been revoked yet), but are going to expire.
- The user may have been authenticated by the operator using Mobile Connect and still valid Loa4 certificate.

Annex A Recommendations for algorithms and key sizes

A.1 NIST Recommendations

Cryptoperiod (usable) up to year 2030
Recommended algorithms and key lengths
- RSA: at least 2048 bit key
- ECC: at least 224 bit key
- hash algorithms: SHA-224, 256, 384 or 512

Table 2: NIST recommendations

A.2 ETSI Recommendations

Signature suite	1 years	3 years	6 years	10 years
RSA with SHA-256	1 536 bit key length	2 048 bit key length	2 048 bit key length	not recommended
RSA improved probabilistic signature scheme with SHA-1	1 536 bit key length	Not recommended		
RSA improved probabilistic signature scheme with SHA-224	1 536 bit key length	2 048 bit key length	2 048 bit key length	not recommended
RSA improved probabilistic signature scheme with SHA-256	1 536 bit key length	2 048 bit key length	2 048 bit key length	3 072 bit key length
ECDSA with SHA-224	224 bit key length	224 bit key length	not recommended	
ECDSA with SHA-256	256 bit key length	256 bit key length	256 bit key length	256 bit key length

Table 3: ETSI recommendations

Recommended signature suites for a resistance during X years according to ETSI TR 119 312, November 2014 [7].

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	14/11/2014	First version	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
0.2	24/11/2014	Added Sections: • Abbreviations • Definitions of terms • References • Mobile Signature Service in Mobile Connect Architecture • User journeys Requirements re-arranged in separate sections	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
0.3	01/12/2014	• Editorial fixes on section numbering • Added: system architecture diagram and interfaces definitions aligned with the SIM Applet Authenticator Specification [1] • Removed: click-OK/LoA 2 scenarios (focusing on LoA 4); SHA1 (not collision free); mandatory on-card certificate storage Fixed: mandatory cryptographic algorithms (RSA or ECC)	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
0.4	11/12/2014	Commented, revised the architecture in Figure 1, added the algorithm and key recommendations as Annex B	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
0.5	19/02/2015	User journeys defined, added ETSI recommendations for algorithms and key sizes	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia

0.6	18/03/2015	Added: descriptions and flows for the detailed procedures in section 5.	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
0.7	20/03/2015	Modified Figure 1; revised sections 3.5.1, 5.1; minor editorial changes	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
1.0.0 RC	31/03/2015	Modified Figure 6; added Figure 7 and split First registration flow in two flows for clarity; modified description in 5.1; minor editorial changes	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
1.0.0 RC	21/04/2015	Updated after biweekly call on 17/04/2015.	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
1.0.0 RC	30/04/2015	Use of PoP code clarified. Final version for a release candidate	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
1.0.0 RC	13/05/2015	• Added: section 3.5.13, describing service renewal before certificate expiration; • Modified: sections 5.3 and 5.4 in analogy with the SIM Applet Authenticator Specification [1] user experience • Proposed as final version for a release candidate	CPAS 13 workstream	Jouni Heinonen/Valimo, Laura Colazza/Telecom Italia
1.0.1 RC		• Minor editorial changes and updated references as part of the transition to BAU		Nick Spencer
1.0.1	06/12/2022	Version for publication	TG	Yolanda Sanz/GSMA

B.2 Other Information

Type	Description
Document Owner	IDG
Editor / Company	Yolanda Sanz / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You MAY notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.