# First Summary
## Toward the Realization of Electronic Certificates for Smartphones

December 25, 2020

# Basic policies for installing smartphones with Individual Number Card functionality

## Basic Policies

1. Accessibility to various procedures and services from just one smartphone
2. Easy online smartphone installation
3. Easy-to-use UX unique to smartphones
4. High security for safe and reliable services
5. Compatibility with global standards

# 1. Accessibility to various procedures and services from just one smartphone

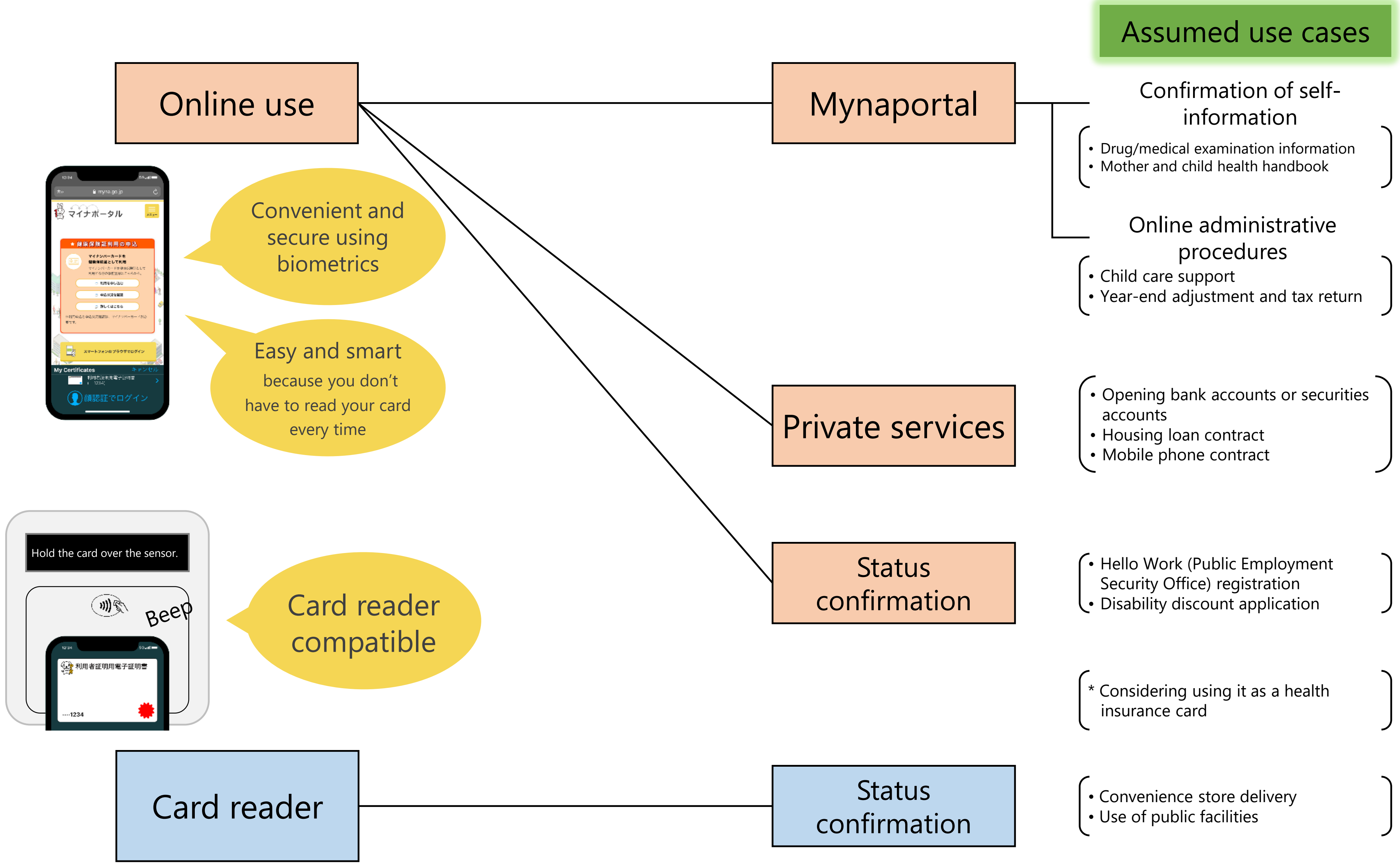
## Basic Policy 1

- The Individual Number Card has the functionality of the Public Certification Service for Individuals, or the Japanese Public Key Infrastructure (JPKI), which enables advanced and high-security identity verification online by preventing spoofing and tampering.
  By installing this functionality on smartphones, it becomes possible to have the convenience of accessibility to various procedures by using smartphones in place of Individual Number Cards.
- At the same time, this functionality will support actions toward the expanded use of the Individual Number Card and the needs of its private-sector use (e.g., the functional expansion of the Mynaportal and the digitalization of various national qualifications).

## Specific Policies

- □ Both types of electronic certificates (signature certification and user identification) of the JPKI can be installed on a smartphone. Thus, it is easy to use a smartphone for various online applications as well as personal authentication on the Mynaportal.
- □ In addition to online use, compatibility with card readers using NFC will be verified for a variety of services including certificate issuing services at convenience stores.
- □ Studies will be done, and action assignments and countermeasures identified, to promote the utilization of electronic certificates issued by private businesses (private IDs) linked to the JPKI.
- □ Installing other functions that the Individual Number Card has (such as the card surface information input assistance function) will be considered after addressing various issues, such as interoperability with related international standards.

# Future use cases (Including those under consideration)



Assumed use cases

Online use

- Convenient and secure using biometrics
- Easy and smart because you don’t have to read your card every time

Mynaportal

Confirmation of self-information
- Drug/medical examination information
- Mother and child health handbook

Online administrative procedures
- Child care support
- Year-end adjustment and tax return

Private services
- Opening bank accounts or securities accounts
- Housing loan contract
- Mobile phone contract

Status confirmation
- Hello Work (Public Employment Security Office) registration
- Disability discount application

* Considering using it as a health insurance card

Card reader

- Card reader compatible

Status confirmation
- Convenience store delivery
- Use of public facilities

# 2. Easy online smartphone installation

## Basic Policy 2

- It is currently necessary to go to the office of a local government to get a JPKI electronic certificate for the Individual Number Card issued or reissued.
  However, provided one has a Individual Number Card, with electronic certificates installed on a smartphone it is possible to easily receive certificates online rather than in person.
- Unlike certificates associated with an Individual Number Card, there is a need to consider the lifecycle of smartphones, such as when they are replaced or transferred or sold, in terms of any certificates installed therein.
  The certificates can be easily and safely installed online even if someone upgrades their smartphone.

## Specific Policies

- □ It will be possible to obtain electronic certificates for smartphones online, assuming that the Individual Number Card has been issued by face-to-face verification at a local government office, via a smartphone by scanning the Individual Number Card and sending an application signed with a electronic signature certificate. Each type of smartphone electronic certificate will be limited to one per person.
- □ If a smartphone is lost or locked, then new electronic certificates can be quickly installed on a new phone. Therefore, similar to new issuance, reissuance can be done online using the electronic signature certificate.
- □ When replacing a smartphone, in principle, the user must apply for the certificates to be revoked. However, it is not mandatory to do this using the old handset, all needed procedures can be completed using the new device. Compared with existing similar apps, it will be a simple UX.
- □ Users can also revoke the electronic certificates on their smartphone via the same device, and without their card.
- □ The PIN/password for smartphone electronic certificates can also be set online.

# 3. Easy-to-use UX unique to smartphones

## Basic Policy 3

- ■ Smartphone electronic certificates will be implemented by making the most of the strength of installing them on a smartphone instead of the Individual Number Card. Easy-to-use and understandable UX will be realized by making the best use of the existing smartphone and associated features and capabilities, while listening to the voices of users.
- ■ When using Individual Number Card electronic certificates there is a need for problematic PIN/password-based authentication. As such, it is necessary to consider introducing a PIN/password-independent authentication mechanism that utilizes the biometric authentication of smartphones while ensuring sufficient security.

## Specific Policies

- □ An understandable operation flow, with few screen transitions or complicated operations, for users will be achieved at the demonstration stage in cooperation with the private section through user tests, and listening to the opinions of users.
- □ The objective is to have a stress-free UX, minus any screen transitions between apps, and to utilize APIs installed in smartphones so that only legitimate apps can access electronic certificates.
- □ It has become common to use biometric authentication devices installed in smartphones. With this in mind, measures are to be considered to utilize biometric authentication while prioritizing the security that is required for the JPKI.

  At the same time, with consideration for the current authentication level of biometric authentication, its application for user authentication functionality will be studied.

  Further, and with reference to the concept and mechanism of FIDO authentication, which has become widespread as an approach that uses biometric authentication for online authentication on smartphones, related issues such as the requirements for biometric authentication function, ideal methods of third-party evaluation, the concept of an authentication level, the demarcation point of responsibility in cases of emergencies, and the provision of sufficient guidance for users, will be identified and examined. Thus, the overarching aim is to balance a user-friendly UX and high security.

# 4. High security for safe and reliable services

## Basic Policy 4

- ■ The electronic certificates of smartphones are important, with electronic signature certificates having estimated effectivity, and user authentication electronic certificates enabling access to the Mynaportal. Therefore, as with Individual Number Cards, it is essential to ensure the same high level of security.
- ■ Furthermore, there are concerns that electronic certificates and private keys remaining in the chip of a smartphone is replaced or transferred may be used by unauthorized people if they end up in the hands of a third party. Therefore, the electronic certificates and private keys of the old handset have to be properly revoked and deleted.

## Specific Policies

- □ Smartphone electronic certificates will be issued based on identity verification using the electronic signature certificate in the Individual Number Card, which is only eligible for people who have obtained this same card through strict identity verification at the office of a local government.

  Smartphone electronic certificates are distinguishable from those of the card and are managed by being linked to the card's certificates. When the card's electronic certificates revoke, then so will those linked to a smartphone.
- □ The private key associated with each of the smartphone electronic certificates is generated in a tamper-proof secure chip (later referred to as GP-SE) inside the smartphone and is safely stored in the applet in the chip. Communication between the server and the chip in the smartphone is secured by the secure channel protocol (SCP03) that complies with international standards.
- □ Unauthorized people may use any electronic certificates or private keys that remain in a lost smartphone. To prevent this, the following measures will be examined in terms of technology and operation.
  - ● If a smartphone is lost then a call center can handle temporary revocations of any associated electronic certificates.
  - ● Revocation is possible with just a smartphone, and without having to go to a government office. When changing handsets it will be possible to apply for the revocation of electronic certificates in the old handset from the new one.
  - ● The electronic certificates and private keys in the old handset will be remotely deleted after revocation.
  - ● Assuming that the data will not be deleted properly, the electronic certificates and private keys can be deleted by a factory reset.
  - ● Cooperation with MNOs and secondhand sellers will be required to confirm the deletion of the electronic certificates and make it known that they should be deleted before a handset is resold.
  - ● Technical measures are needed to prevent electronic signatures using a private key associated with revoked smartphone electronic certificates.

# 5. Compatibility with global standards

## Basic Policy 5

- If a method that is not internationally supported is adopted for the installation of smartphone electronic certificates, then the phone models that support these certificates will be limited and there is a risk that they may not be widely used. Therefore, when considering a specific method, it is necessary to comply with global standards and fully consider the possibility of an actual rollout of smartphone electronic certificates.
- Furthermore, it is necessary to constantly carry out reviews from the viewpoint of improving user convenience and in light of international trends relating to digital IDs and electronic signatures.

## Specific Policies

□ Ensure sufficient reliability of the JPKI while referring to the level of identity verification and personal authentication in the Digital Identity Guidelines (SP 800-63-3) issued by the NIST.

□ The GlobalPlatform-supported secure element (GP-SE) will be utilized as a storage medium for the electronic certificates and the private keys. The GP-SE is a general-purpose chip that complies with international standards and it is expected to be widely installed on handsets sold by MNOs as well as SIM-free handsets.

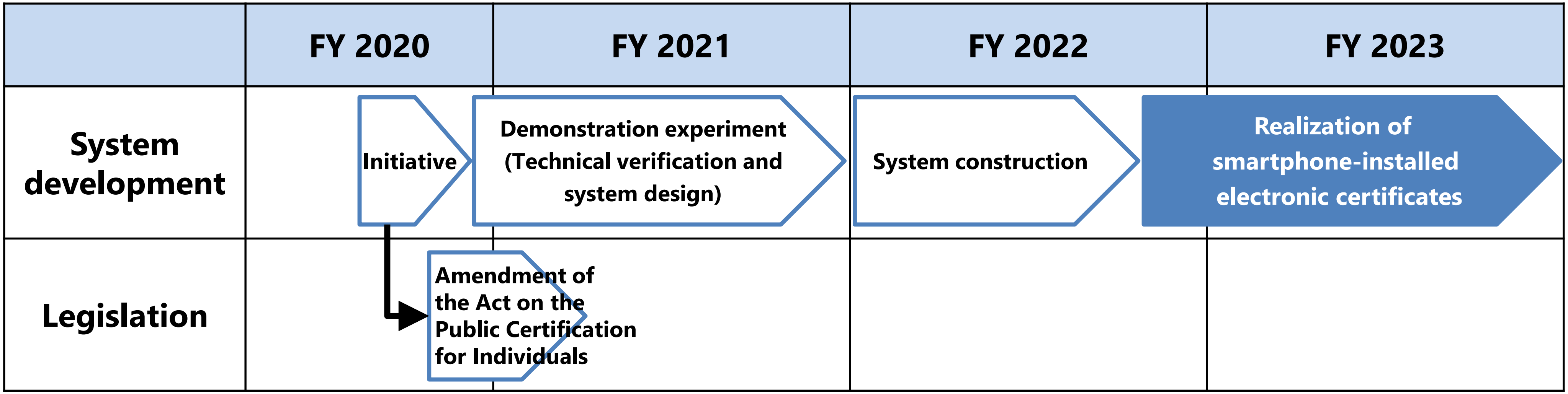
□ Consistency with international standards will be ensured in regard to the technical requirements for storage media, such as ISO/IEC 15408 (the CC Certification), the eIDAS Regulation for qualified electronic signature creation devices (QSCD), and FIPS 140-2.

□ Close attention will be paid to ensuring compatibility with de facto standards in the global smartphone ecosystem, such as the Android Compatibility Definition Documents (CDD).

□ Considering the international trends related to digital IDs, the installation status of the GP-SE, the spread of private IDs linked to the JPKI, etc., the necessity for a method that does not require the GP-SE will be studied with reference to remote electronic signatures and the Estonian Smart-ID.

# Schedule for realization

- ➢ **The objective is to install smartphone electronic certificates on Android devices by the end of FY 2022 (2023 Q1).**
- ➢ **A bill is in the planning stages for submission to the next ordinary session of the Diet to amend the Act on the Public Certification for Individuals in order** to develop the necessary systems.
- ➢ **The early realization of certificates on iPhones is an objective as well.**

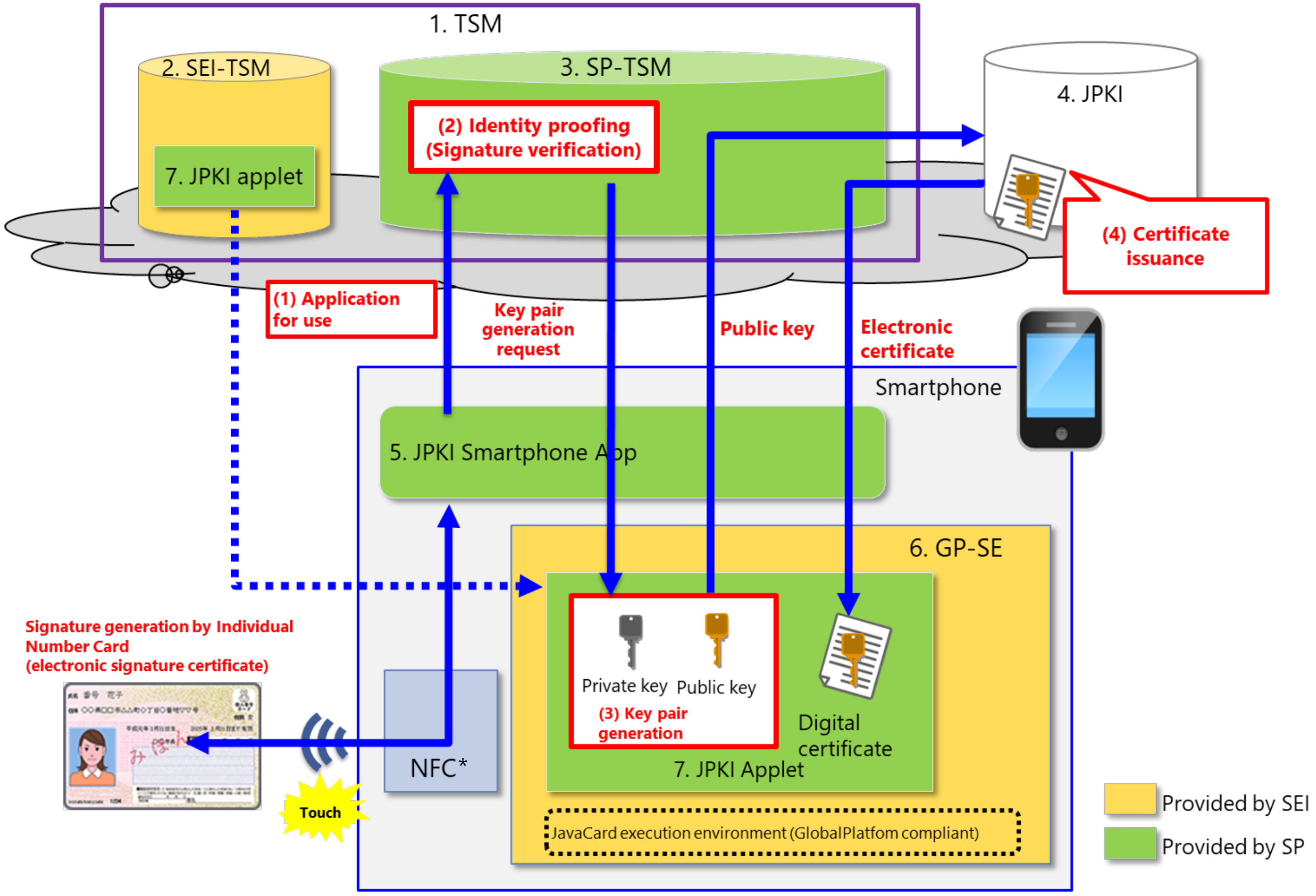


| | FY 2020 | FY 2021 | FY 2022 | FY 2023 |
|---|---|---|---|---|
| System development | Initiative | Demonstration experiment (Technical verification and system design) | System construction | Realization of smartphone-installed electronic certificates |
| Legislation | Amendment of the Act on the Public Certification for Individuals | | | |

# References

# System configuration for installing electronic certificate on a smartphone

## System configuration for mounting a electronic certificate on a smartphone and glossary



* Type B is used.

Remarks: In the above figure, it is assumed that users download the JPKI smartphone app is downloaded from Google Play.

### Server

1. TSM: Trusted Service Manager
   - Consisting of the SEI-TSM and SP-TSM. Securely distributes data to the secure element (SE) on a smartphone.

2. SEI-TSM
   - A TSM operated by a secure element issuer (SEI).
   - Responsible for keeping applets of service providers (SPs) and storing applets in the SE.

3. SP-TSM
   - A TSM operated by an SP.
   - Responsible for accepting user usage applications and SE personalization.

4. JPKI (Public Certification Service for Individuals)
   - A certification service operated by J-LIS.

### Smartphone

5. JPKI Smartphone App
   - An Android application used when applying to use or using services.
   - Downloadable from Google Play. Used when applying for or using a certification service.

6. GP-SE
   - An SE that is installed on Android smartphones.
   - The GP-SE conforms to the GlobalPlatform and makes it possible to download Java applets.

7. JPKI Applet
   - A Java applet that implements the JPKI function.

# GP-SE outline

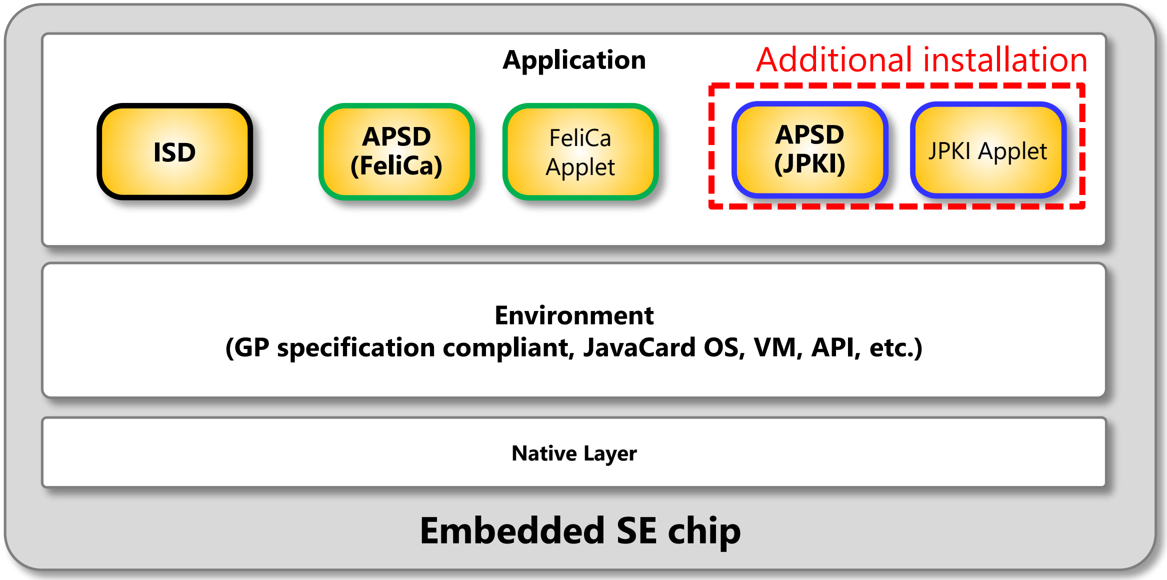
**[GP-SE]**

The GP-SE is a secure element (SE) embedded in the main board of smartphones. The GP-SE has a JavaCard execution environment that supports the specifications of the GlobalPlatform (GP) and is an IC chip that can install and operate Java applets developed by service providers. The GP-SE chip outline and software configuration diagram are shown below. If users install a Java applet that implements the JPKI function, they will be able to use their smartphones for login authentication to the Mynaportal or get their certificate of residence, for example, at convenience stores.

**[Status of rollout]**

FeliCa Networks, Inc. developed the GP-SE, and smartphone models equipped with the GP-SE have been on sale since spring 2019. In April 2020, about 30% of newly released Android smartphones in Japan were GP-SE-equipped smartphones, and it is expected that this number will continue to increase in future. Currently, smartphones are shipped with the FeliCa applet preinstalled, which implements FeliCa functionality, and is used in payment services, such as Suica, iD, and QUICPay.

**GP-SE**

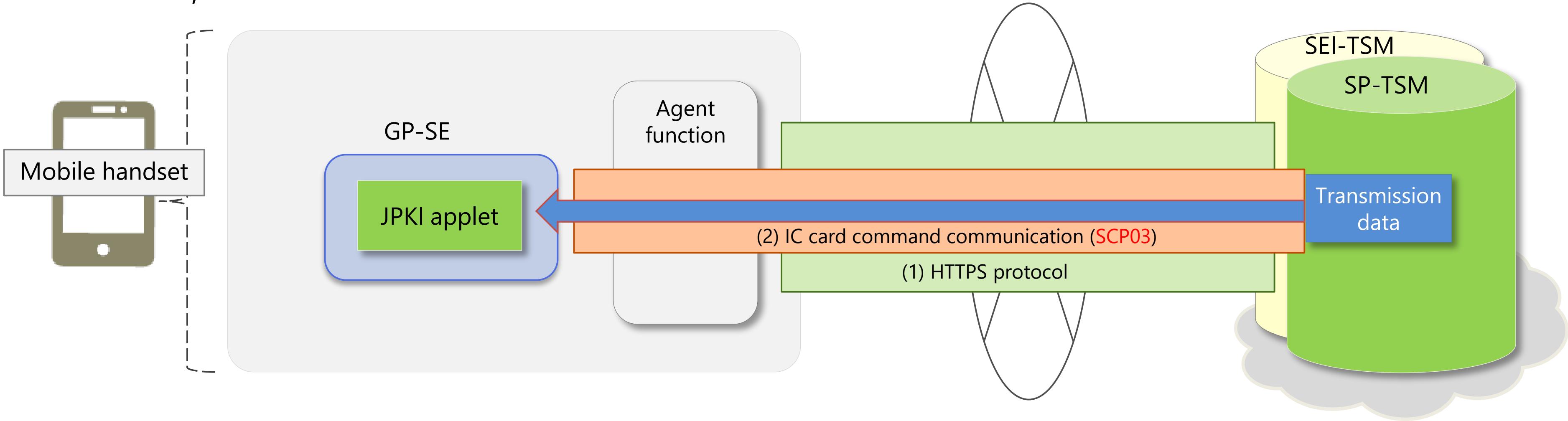


- **ISD: Issuer Security Domain**
  The Security Domain (SD) for the publisher. The SD mainly manages publisher-related content. Creating a new APSD is subject to approval from the ISD.
- **APSD: Application Provider Security Domain**
  An SD to install original applications (the FeliCa applet and JPKI applet shown in the figure on the left) on SE.
- **JPKI Applet**
  An applet that implements the JPKI function. The JPKI applet stores electronic certificates and private keys for smartphones.
- **FeliCa applet**
  The FeliCa applet processes the FeliCa file system, commands, encryption, etc.

# GP-SE security functionality (1)

(1) Secure channel protocol

Data communication is carried out between the GP-SE and TSM through the secure channel protocol (SCP03). SCP03 is an encrypted communication protocol defined by the GlobalPlatform, which exchanges key sharing and encrypted data between the GP-SE and TSM. It is extremely difficult to decipher or tamper with data, even if the data in the middle of the route is skimmed.



(2) GP-SE encryption function

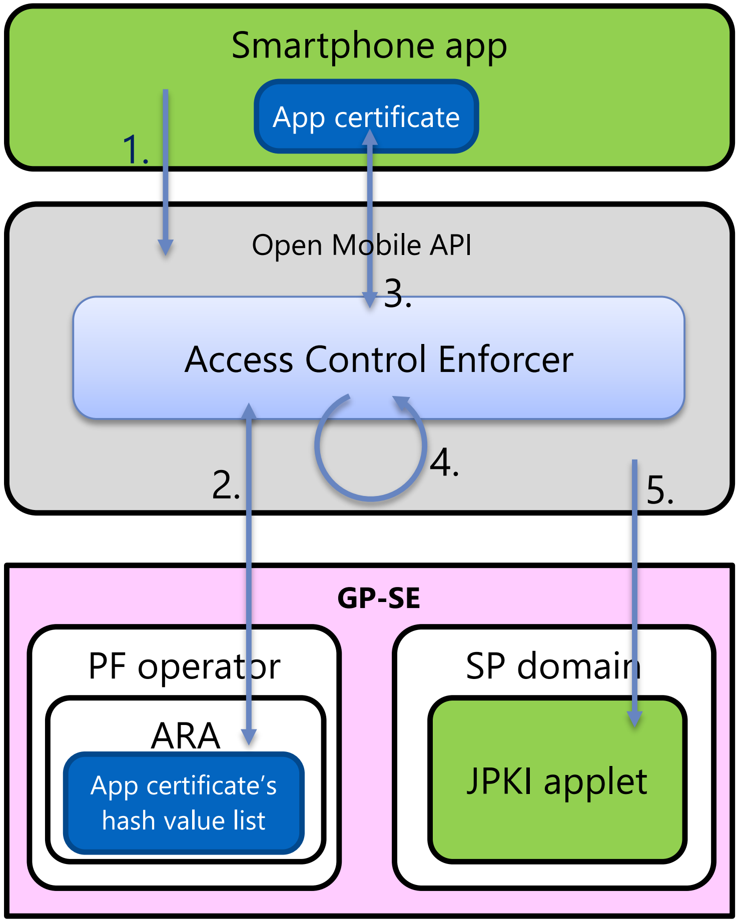
The GP-SE supports the following cryptographic algorithms required by the JPKI. Also, rsa-2048bit-key-pair generation is possible.

| No. | Cryptographic algorithm | Support status | Remarks |
|---|---|---|---|
| 1 | RSA 2048-bit | Yes | Signature supports RSA SSA-PKCS # 1_v1.5 |
| 2 | AES 128-bit | Yes | SCP03 encryption protocol |
| 3 | Random number generation | Yes | Used by SCP |

# GP-SE security functionality (2)

## (3) Security functionality related to access from smartphone apps

The applet (JPKI applet) stored in the GP-SE can be accessed only by a legitimate Android application (smartphone application) by authenticating the access source application by the mechanism shown in the figure below. With this mechanism, it is extremely difficult for a third party to create a smartphone application to access the GP-SE.



[Reference] GlobalPlatform, Secure Element Access Control v1.0

■ How to register a list of applications that can access applets

1. The SP creates a whitelist of applications that can access JPKI applets (certificate hash value list of Android applications) and registers it with the SEI-TSM.
2. When the SEI-TSM stores JPKI applets in the GP-SE, the above list is stored in ARA (Access Rule Application).

■ Authentication procedure (numbers corresponds to the figure on the left)

1. Smartphone app accesses the Open Mobile API.
   Open Mobile API: An API for Android provided to access the GP-compliant secure area in the GP-SE.
2. The ACE (Access Control Enforcer) inside the Open Mobile API acquires access rules from the ARA (Access Rule Application) in the PF operator area.
3. The ACE calculates the hash values of the public key certificate given to the Android application that is the access source.
4. The ACE compares the hash values obtained in step 2 and step 3. If they match, it is judged that access is from the correct application.
5. If they match in step 4, the Open Mobile API processing requested in step 1 is executed.

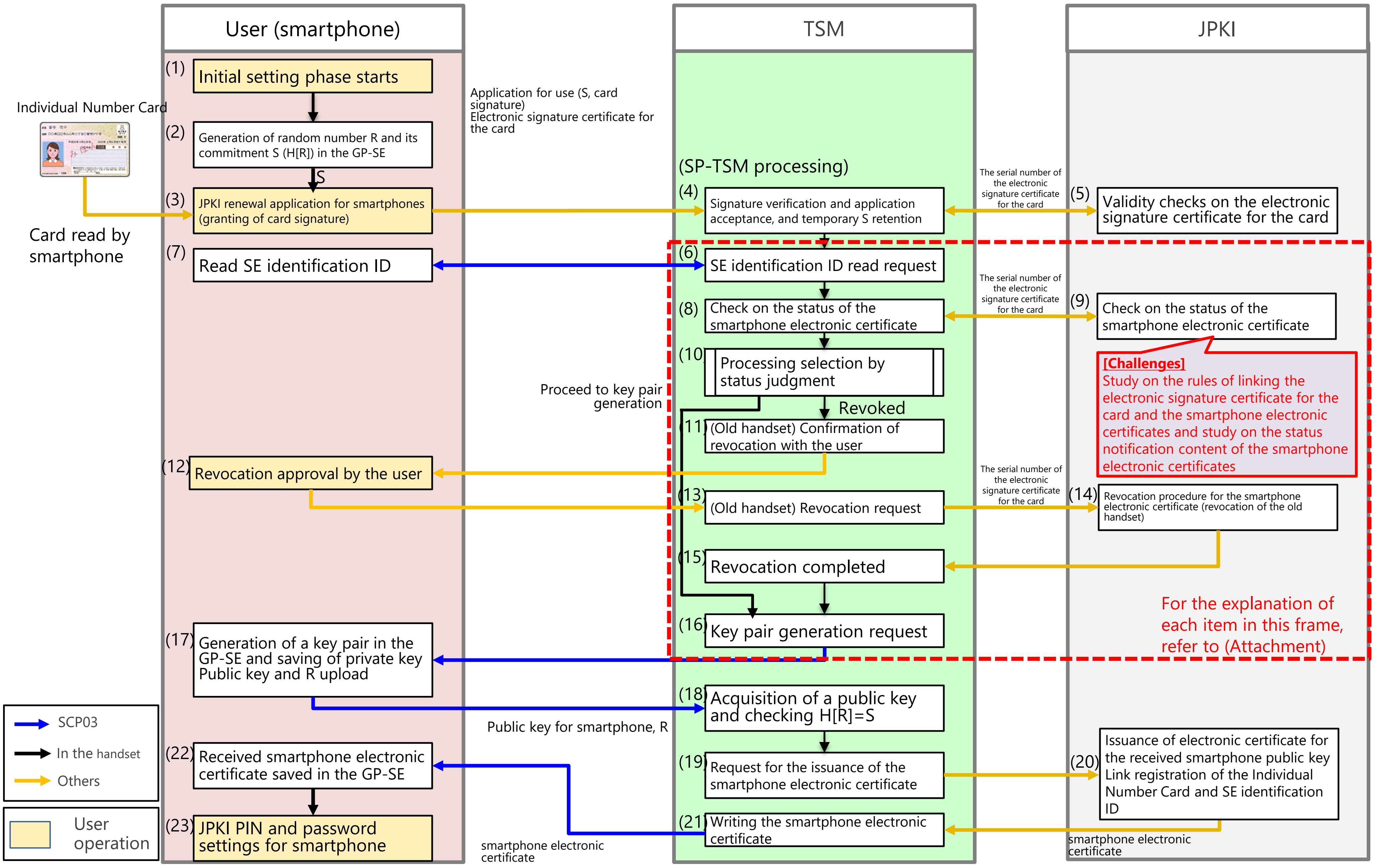
# Security evaluation of GP-SE

The GP-SE uses an IC chip that has acquired CC certification or EMV certification as a platform (HW + OS). A comparison table for the security evaluation of the Individual Number Card and GP-SE is shown below.

| Item | Individual Number Card security evaluation (CC certification) | GP-SE platforms security evaluation | |
|---|---|---|---|
| | | CC certification (HW+OS) | EMV certification (HW+OS) |
| Security requirements | Protection profile created based on ISO/IEC 15408 (public)<br>EAL4+(AVA_VAN.5) | Protection profile created based on ISO/IEC 15408 (public)<br>EAL4+(AVA_VAN.5) | Security Guideline defined by EMVCo (private)<br>EAL4+(AVA_VAN.5) |
| Evaluation range | Product evaluation and evaluation, including its development process | Product evaluation and evaluation, including its development process | |
| Vulnerability evaluation | Countermeasures against attacks indicated in a JIWG document | Countermeasures against attacks indicated in a JIWG document | |
| Validity period | Depends on the country of certification | Depends on the country of certification | One year (one year after re-evaluation, up to six years) |
| Evaluation agency | Evaluation body accredited by a certification body | Evaluation body accredited by a certification body | Evaluation body accredited by EMVCo |
| Certification body | Certification body based on the certification system<br>(Public institution) | Certification body based on the certification system (public institution) | EMVCo |

AVA_VAN.5, which is the highest level in the vulnerability analysis, is also applied to the Individual Number Card, and has been achieved in the CC certification and EMV certification of the GP-SE. The GP-SE can be evaluated as having the same tamper resistance level as the Individual Number Card.

# Issuance flow for smartphone electronic certificates (1)



User (smartphone)

TSM

JPKI

Individual Number Card

Card read by smartphone

(1) Initial setting phase starts

(2) Generation of random number R and its commitment S (H[R]) in the GP-SE

S

(3) JPKI renewal application for smartphones (granting of card signature)

Application for use (S, card signature)
Electronic signature certificate for the card

(SP-TSM processing)

(4) Signature verification and application acceptance, and temporary S retention

The serial number of the electronic signature certificate for the card

(5) Validity checks on the electronic signature certificate for the card

(6) SE identification ID read request

(7) Read SE identification ID

(8) Check on the status of the smartphone electronic certificate

The serial number of the electronic signature certificate for the card

(9) Check on the status of the smartphone electronic certificate

**[Challenges]**
Study on the rules of linking the electronic signature certificate for the card and the smartphone electronic certificates and study on the status notification content of the smartphone electronic certificates

(10) Processing selection by status judgment

Proceed to key pair generation

Revoked

(11) (Old handset) Confirmation of revocation with the user

(12) Revocation approval by the user

(13) (Old handset) Revocation request

The serial number of the electronic signature certificate for the card

(14) Revocation procedure for the smartphone electronic certificate (revocation of the old handset)

(15) Revocation completed

(16) Key pair generation request

For the explanation of each item in this frame, refer to (Attachment)

(17) Generation of a key pair in the GP-SE and saving of private key
Public key and R upload

Public key for smartphone, R

(18) Acquisition of a public key and checking H[R]=S

(19) Request for the issuance of the smartphone electronic certificate

(20) Issuance of electronic certificate for the received smartphone public key
Link registration of the Individual Number Card and SE identification ID

(21) Writing the smartphone electronic certificate

smartphone electronic certificate

(22) Received smartphone electronic certificate saved in the GP-SE

smartphone electronic certificate

(23) JPKI PIN and password settings for smartphone

SCP03

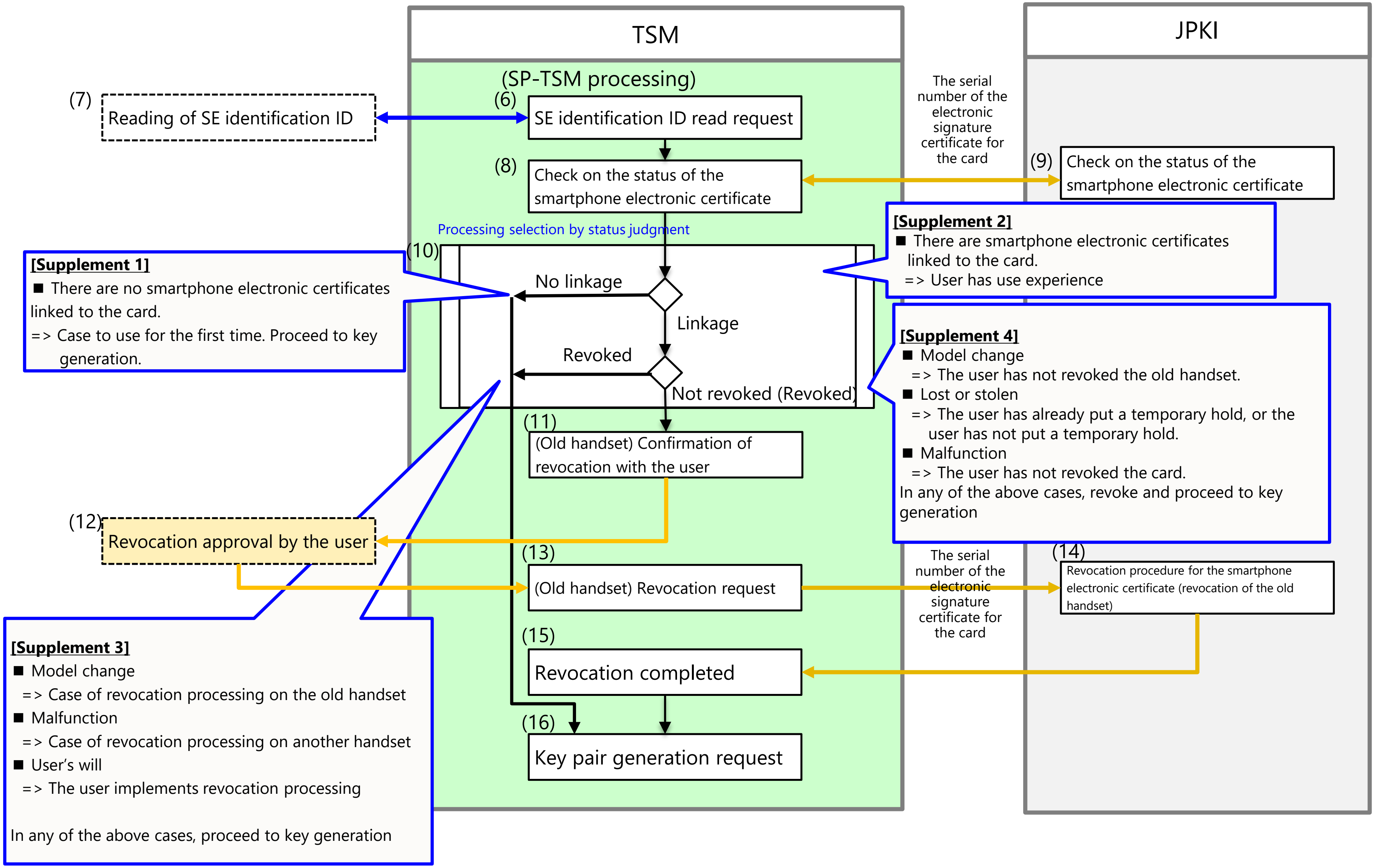
In the handset

Others

User operation

# Issuance flow for smartphone electronic certificates (2) (Attachment)

Relationship with the smartphone-specific life cycle in connection with the red frame on the previous slide



TSM

JPKI

(SP-TSM processing)

(7) Reading of SE identification ID

(6) SE identification ID read request

(8) Check on the status of the smartphone electronic certificate

The serial number of the electronic signature certificate for the card

(9) Check on the status of the smartphone electronic certificate

Processing selection by status judgment

(10)

No linkage

Linkage

Revoked

Not revoked (Revoked)

(11) (Old handset) Confirmation of revocation with the user

(12) Revocation approval by the user

(13) (Old handset) Revocation request

The serial number of the electronic signature certificate for the card

(14) Revocation procedure for the smartphone electronic certificate (revocation of the old handset)

(15) Revocation completed

(16) Key pair generation request

**[Supplement 1]**

■ There are no smartphone electronic certificates linked to the card.

=> Case to use for the first time. Proceed to key generation.

**[Supplement 2]**

■ There are smartphone electronic certificates linked to the card.

=> User has use experience

**[Supplement 3]**

■ Model change

=> Case of revocation processing on the old handset

■ Malfunction

=> Case of revocation processing on another handset

■ User's will

=> The user implements revocation processing

In any of the above cases, proceed to key generation

**[Supplement 4]**

■ Model change

=> The user has not revoked the old handset.

■ Lost or stolen

=> The user has already put a temporary hold, or the user has not put a temporary hold.

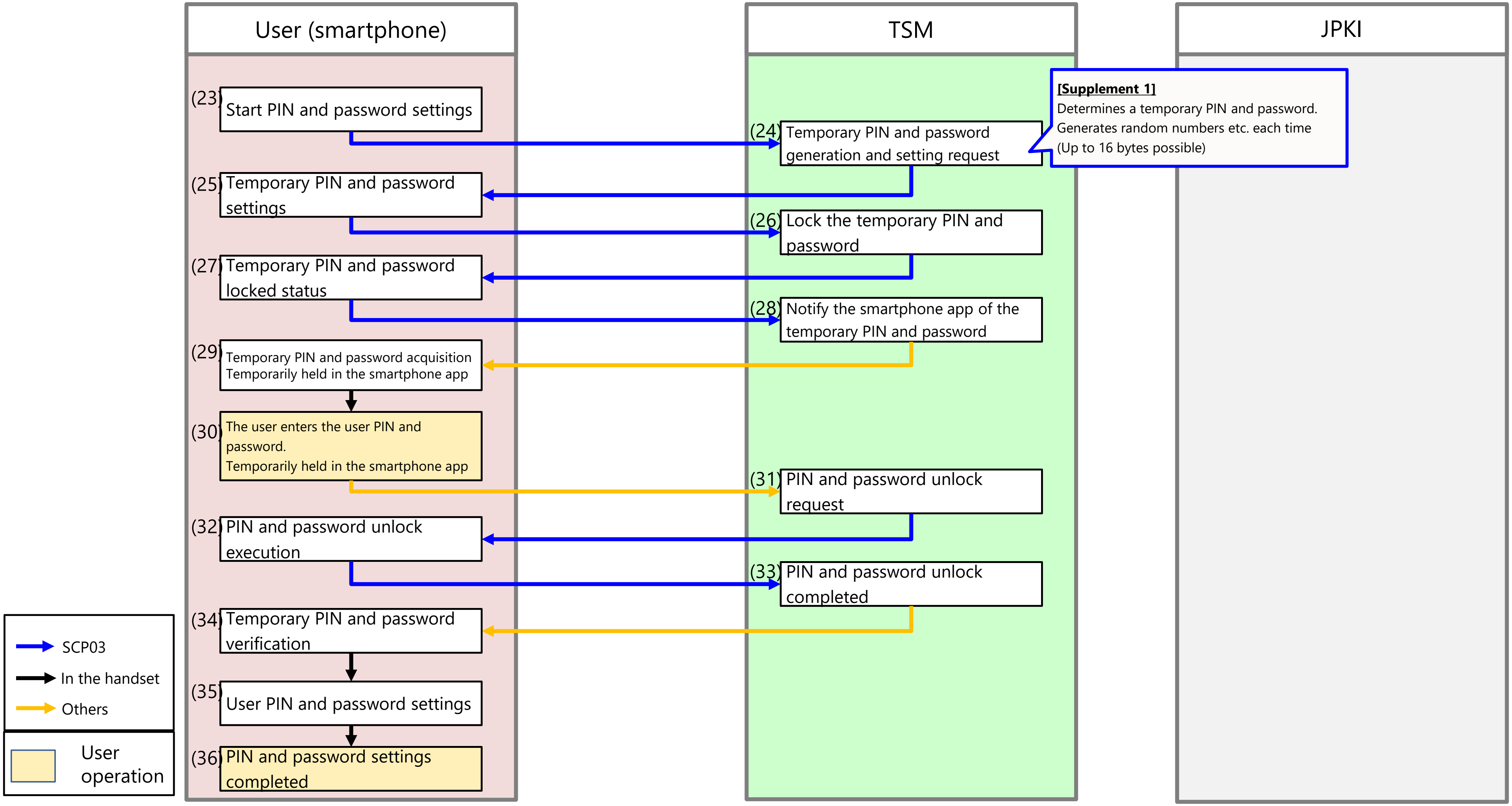
■ Malfunction

=> The user has not revoked the card.

In any of the above cases, revoke and proceed to key generation

# PIN/password initial setting flow

- Start from the flow of issuing smartphone electronic certificates (23). Executed in a series of sessions as a continuation of the issuing flow (a session with valid card signature).
- A temporary PIN and password will be used in the system, but the user will not be unaware of the existence of the temporary PIN or password.



User (smartphone)

TSM

JPKI

(23) Start PIN and password settings

(24) Temporary PIN and password generation and setting request

**[Supplement 1]**
Determines a temporary PIN and password.
Generates random numbers etc. each time
(Up to 16 bytes possible)

(25) Temporary PIN and password settings

(26) Lock the temporary PIN and password

(27) Temporary PIN and password locked status

(28) Notify the smartphone app of the temporary PIN and password

(29) Temporary PIN and password acquisition
Temporarily held in the smartphone app

(30) The user enters the user PIN and password.
Temporarily held in the smartphone app

(31) PIN and password unlock request

(32) PIN and password unlock execution

(33) PIN and password unlock completed

(34) Temporary PIN and password verification

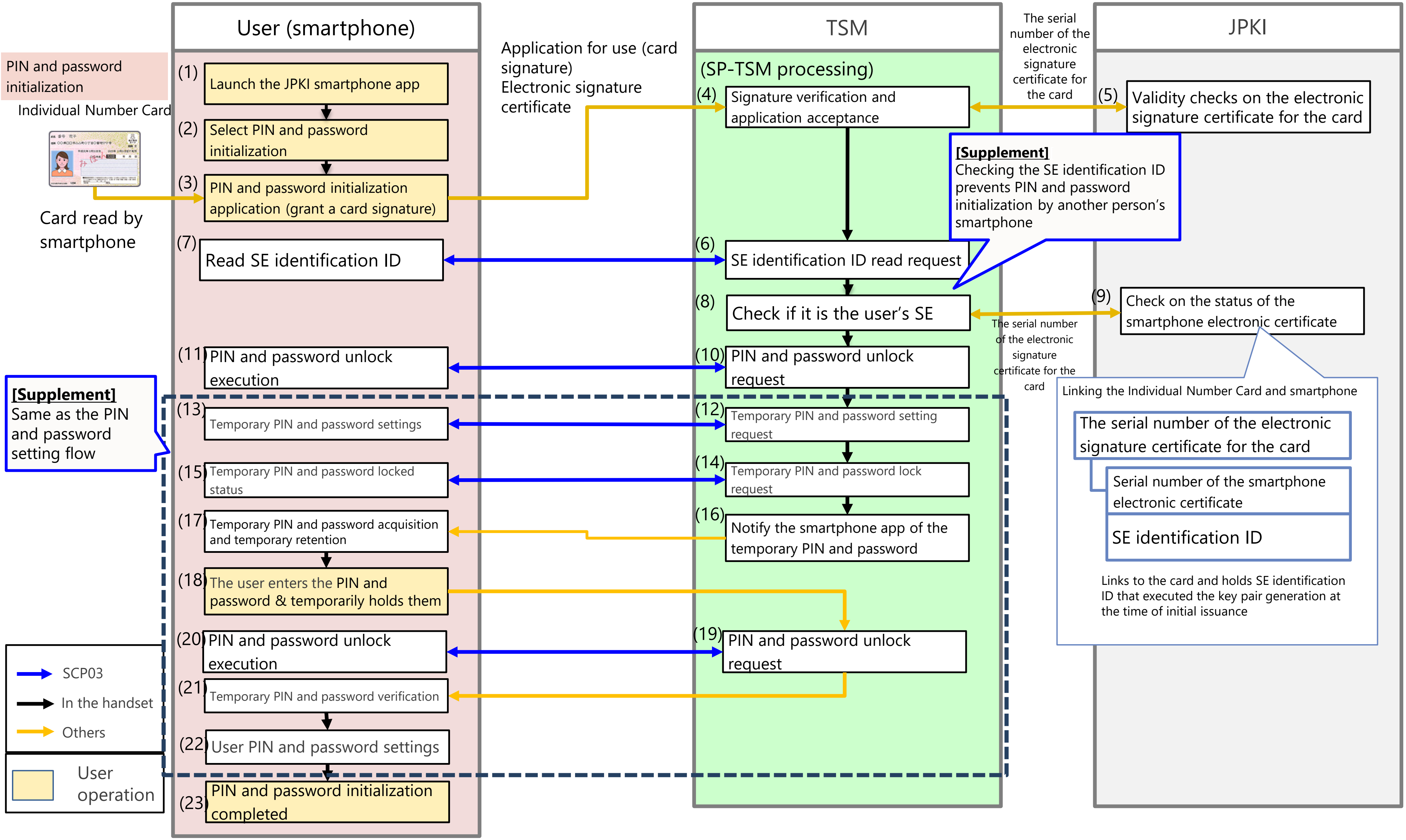
(35) User PIN and password settings

(36) PIN and password settings completed

→ SCP03
→ In the handset
→ Others
□ User operation

# PIN/password initialization flow

PIN and password initialization can be executed by card signature verification (identity verification) (can be done online).



User (smartphone)

TSM

JPKI

PIN and password initialization

Individual Number Card

Card read by smartphone

(1) Launch the JPKI smartphone app

(2) Select PIN and password initialization

(3) PIN and password initialization application (grant a card signature)

Application for use (card signature)
Electronic signature certificate

(SP-TSM processing)

(4) Signature verification and application acceptance

The serial number of the electronic signature certificate for the card

(5) Validity checks on the electronic signature certificate for the card

**[Supplement]**
Checking the SE identification ID prevents PIN and password initialization by another person's smartphone

(6) SE identification ID read request

(7) Read SE identification ID

(8) Check if it is the user's SE

The serial number of the electronic signature certificate for the card

(9) Check on the status of the smartphone electronic certificate

Linking the Individual Number Card and smartphone

- The serial number of the electronic signature certificate for the card
  - Serial number of the smartphone electronic certificate
  - SE identification ID

Links to the card and holds SE identification ID that executed the key pair generation at the time of initial issuance

(10) PIN and password unlock request

(11) PIN and password unlock execution

**[Supplement]**
Same as the PIN and password setting flow

(12) Temporary PIN and password setting request

(13) Temporary PIN and password settings

(14) Temporary PIN and password lock request

(15) Temporary PIN and password locked status

(16) Notify the smartphone app of the temporary PIN and password

(17) Temporary PIN and password acquisition and temporary retention

(18) The user enters the PIN and password & temporarily holds them

(19) PIN and password unlock request

(20) PIN and password unlock execution

(21) Temporary PIN and password verification

(22) User PIN and password settings

(23) PIN and password initialization completed

→ SCP03
→ In the handset
→ Others
□ User operation

# User operation for each purpose (1)

## Phase 1 App preparation

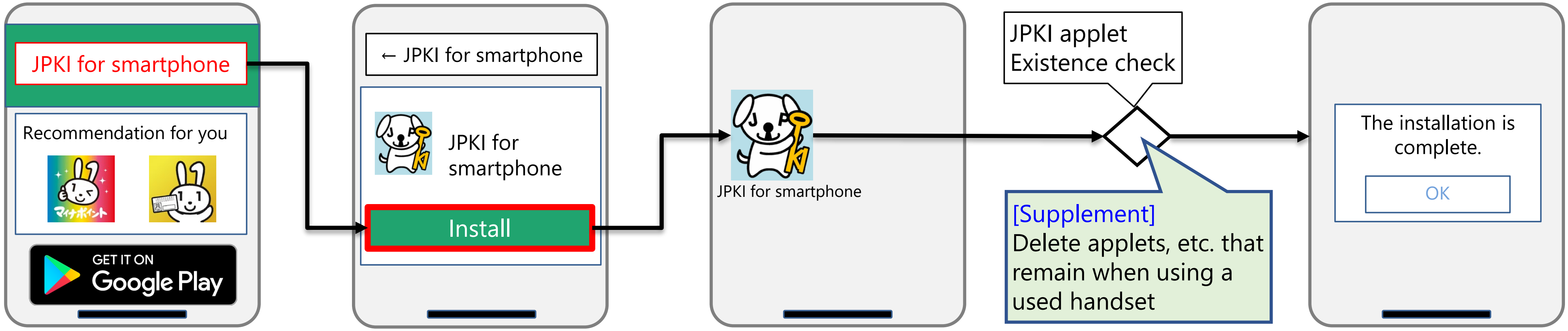
## Phase 2 Applet preparation

**(1) Search for apps**

**(2) Install the app**

**(3) Launch the app for the first time**

**(4) Applet ready for initial settings**



JPKI for smartphone

Recommendation for you

GET IT ON Google Play

← JPKI for smartphone

JPKI for smartphone

Install

JPKI for smartphone

JPKI applet Existence check

[Supplement]
Delete applets, etc. that remain when using a used handset

The installation is complete.

OK

## Phase 3 Initial setting

**(1) Start issuing procedure**

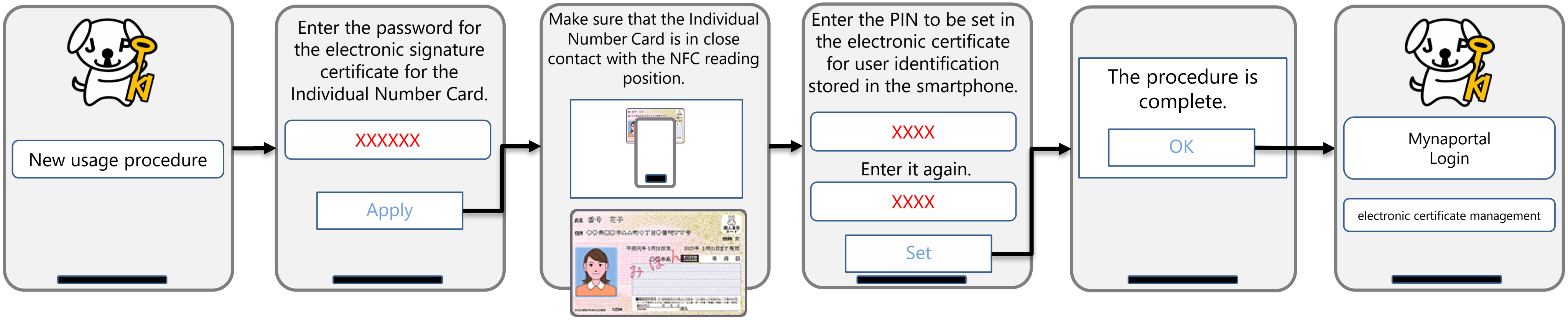
**(2) Enter the password for the electronic signature certificate for the card**

**(3) Hold the Individual Number Card to add the electronic signature**

**(4) Set the PIN and password for the smartphone electronic certificate**

**(5) Initial setting phase completed**

**(6) Start of usage phase**



New usage procedure

Enter the password for the electronic signature certificate for the Individual Number Card.

XXXXXX

Apply

Make sure that the Individual Number Card is in close contact with the NFC reading position.

Enter the PIN to be set in the electronic certificate for user identification stored in the smartphone.

XXXX

Enter it again.

XXXX

Set

The procedure is complete.

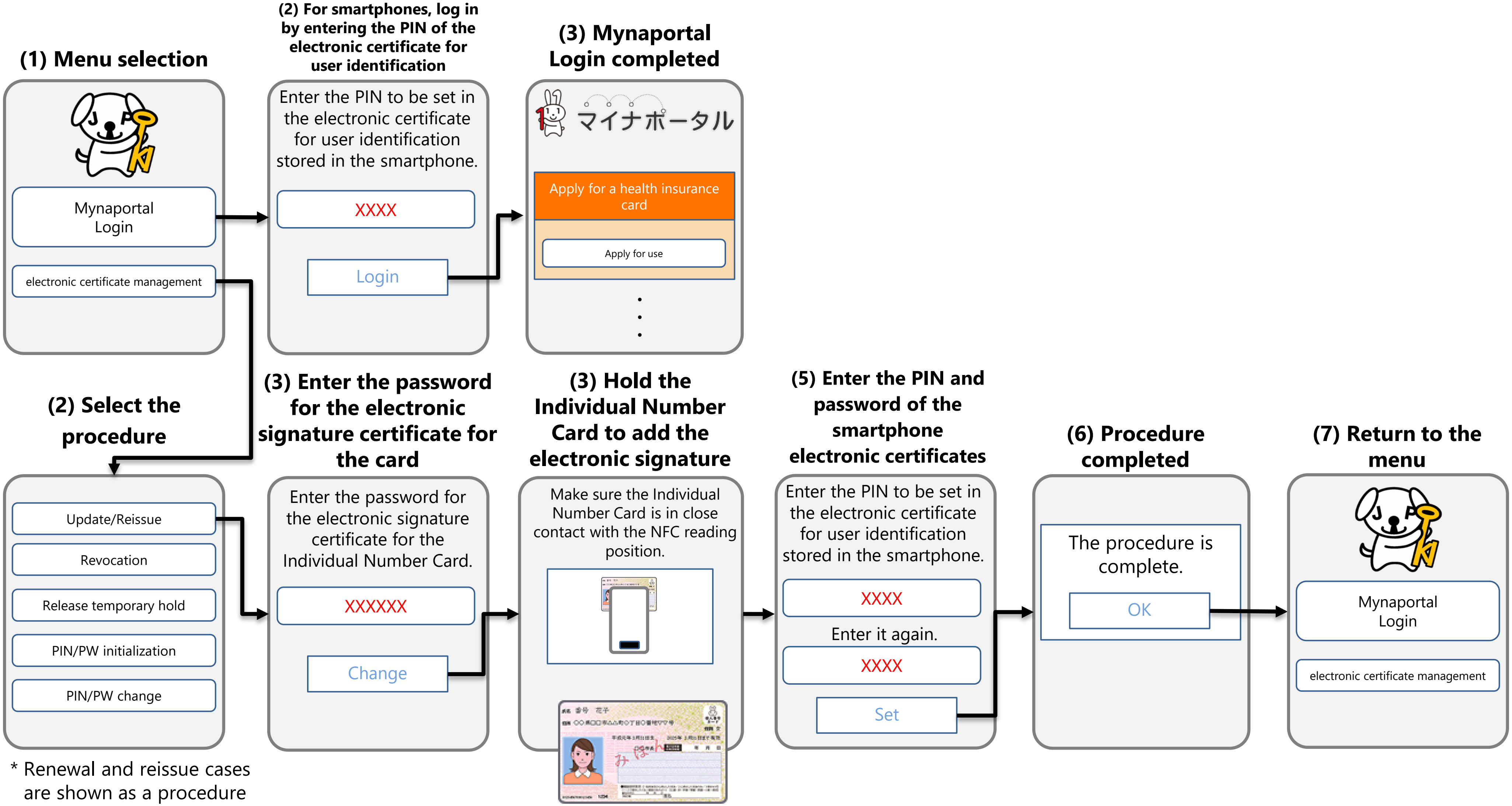
OK

Mynaportal Login

electronic certificate management

# User operation for each purpose (2)

## Phase 4 Service usage/certificate management



**(1) Menu selection**

Mynaportal Login

electronic certificate management

**(2) For smartphones, log in by entering the PIN of the electronic certificate for user identification**

Enter the PIN to be set in the electronic certificate for user identification stored in the smartphone.

XXXX

Login

**(3) Mynaportal Login completed**

マイナポータル

Apply for a health insurance card

Apply for use

**(2) Select the procedure**

Update/Reissue

Revocation

Release temporary hold

PIN/PW initialization

PIN/PW change

**(3) Enter the password for the electronic signature certificate for the card**

Enter the password for the electronic signature certificate for the Individual Number Card.

XXXXXX

Change

**(3) Hold the Individual Number Card to add the electronic signature**

Make sure the Individual Number Card is in close contact with the NFC reading position.

**(5) Enter the PIN and password of the smartphone electronic certificates**

Enter the PIN to be set in the electronic certificate for user identification stored in the smartphone.

XXXX

Enter it again.

XXXX

Set

**(6) Procedure completed**

The procedure is complete.

OK

**(7) Return to the menu**

Mynaportal Login

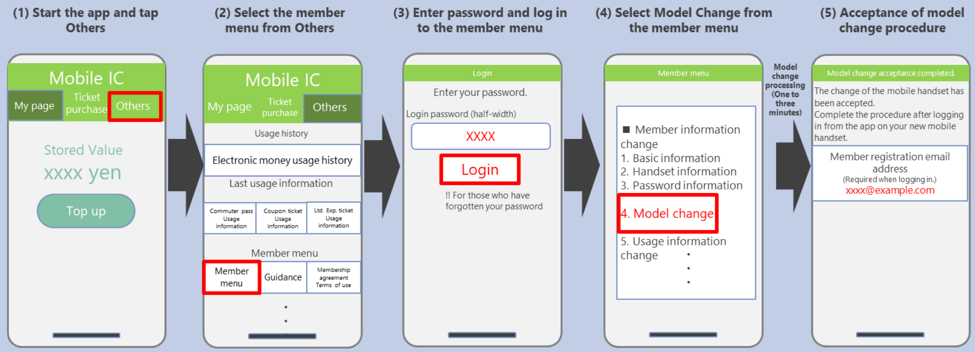
electronic certificate management

* Renewal and reissue cases are shown as a procedure example.

# Comparison with transportation IC card app when changing models

## Transportation IC

## Old handset



(1) Start the app and tap Others

(2) Select the member menu from Others

Mobile IC
My page
Ticket purchase
Others
Usage history
Electronic money usage history
Last usage information
Commuter pass Usage information
Coupon ticket Usage information
Ltd. Exp. ticket Usage information
Member menu
Member menu
Guidance
Membership agreement Terms of use

(3) Enter password and log in to the member menu

Enter your password.

Login password (half-width)

XXXX

!! For those who have forgotten your password

(4) Select Model Change from the member menu

■ Member information change

1. Basic information
2. Handset information
3. Password information
4. Model change
5. Usage information change

Model change processing (One to three minutes)

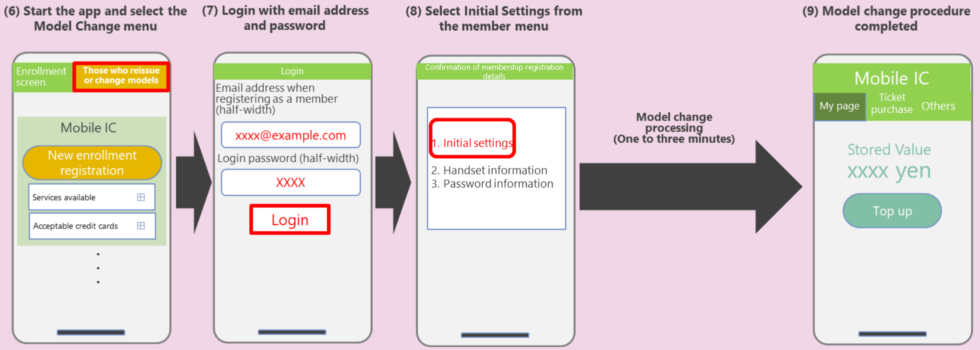
(5) Acceptance of model change procedure

Model change acceptance completed.

The change of the mobile handset has been accepted. Complete the procedure after logging in from the app on your new mobile handset.

Member registration email address (Required when logging in.) xxxx@example.com

## New handset



(6) Start the app and select the Model Change menu

(7) Login with email address and password

Email address when registering as a member (half-width)

xxxx@example.com

Login password (half-width)

XXXX

(8) Select Initial Settings from the member menu

Confirmation of membership registration details

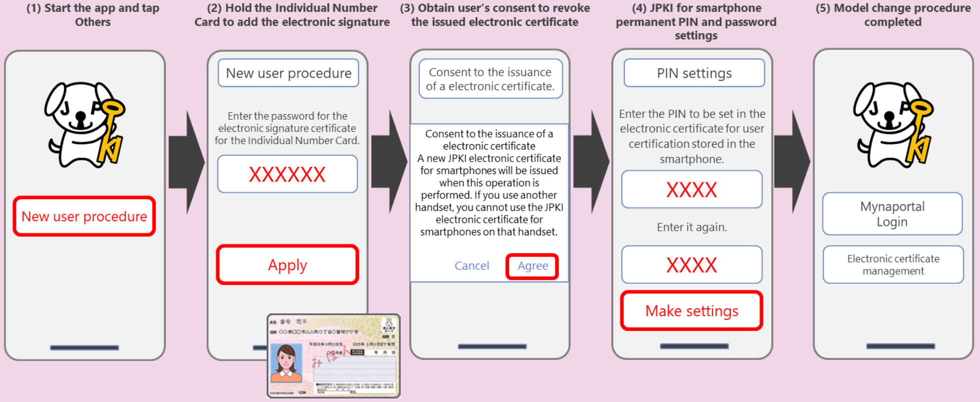
1. Initial settings
2. Handset information
3. Password information

Model change processing (One to three minutes)

(9) Model change procedure completed

## JPKI for smartphone

The user does not need to operate an old handset to use the JPKI for smartphones, even after changing models.
Revoking the electronic certificate of the old handset is also carried out through the new use procedure on the new handset.
* A different means is prepared for the old handset, which can delete the electronic certificate and private keys remaining on the old handset to prevent unauthorized data use.



(1) Start the app and tap Others

(2) Hold the Individual Number Card to add the electronic signature

Enter the password for the electronic signature certificate for the Individual Number Card.

XXXXXX

(3) Obtain user's consent to revoke the issued electronic certificate

Consent to the issuance of a electronic certificate.

Consent to the issuance of a electronic certificate
A new JPKI electronic certificate for smartphones will be issued when this operation is performed. If you use another handset, you cannot use the JPKI electronic certificate for smartphones on that handset.

(4) JPKI for smartphone permanent PIN and password settings

Enter the PIN to be set in the electronic certificate for user certification stored in the smartphone.

XXXX

Enter it again.

XXXX

(5) Model change procedure completed

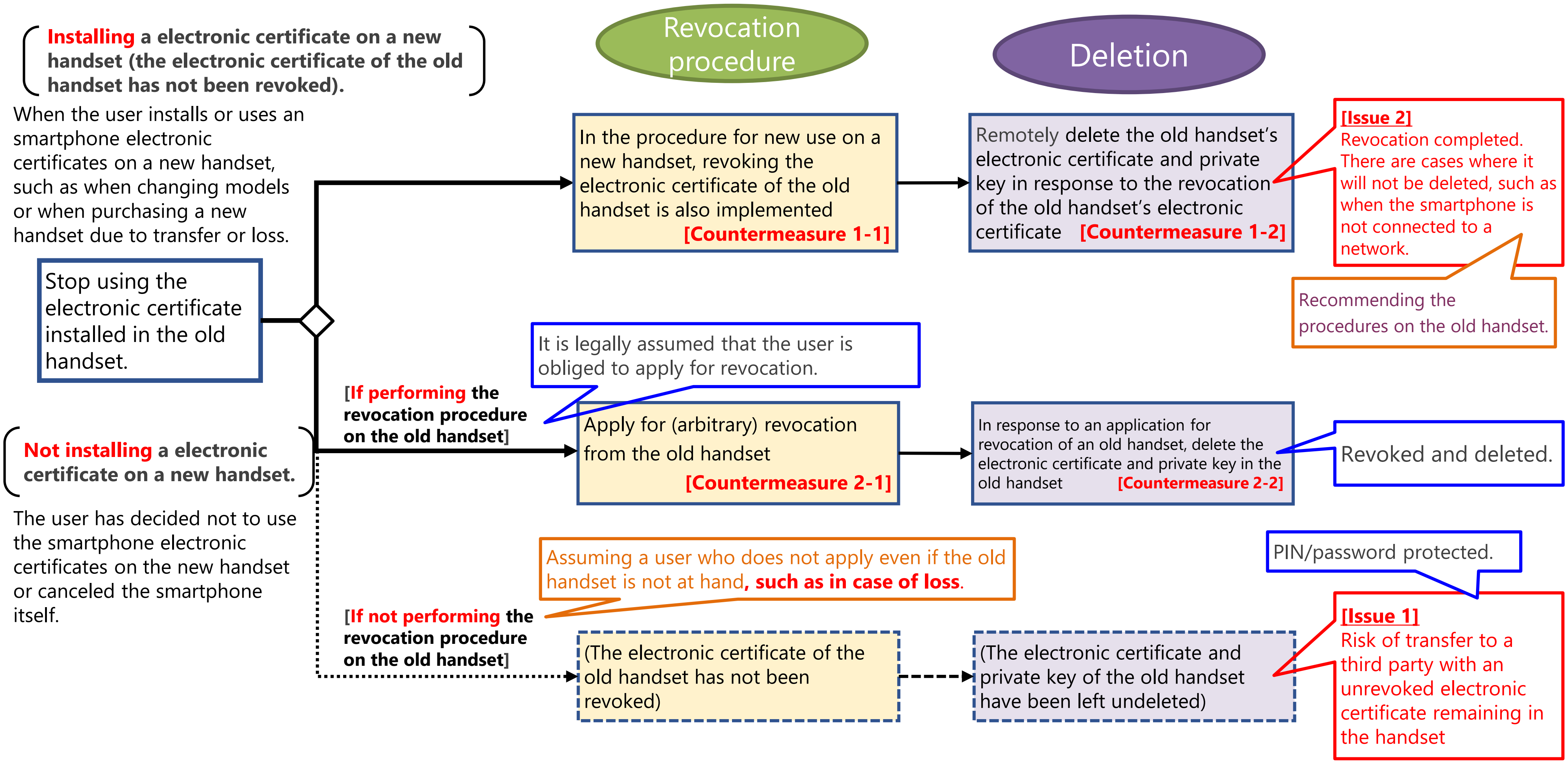
# Prevention of the unauthorized use of electronic certificates and private keys installed in old handsets

In the case of stopping the use of an electronic certificate installed on a user's smartphone (old handset) due to a model change, transfer, loss, etc.:

(1) It is necessary to revoke the electronic certificate installed in the old handset (It is assumed that the user is legally obliged to apply for revocation).

(2) Besides, these electronic certificates and private keys should be properly deleted to prevent them from being transferred to a third party and misused while remaining in the old handset.

As with the case of a card, it is assumed that it is an obligation without penalties, so some users may not apply.



**Installing a electronic certificate on a new handset (the electronic certificate of the old handset has not been revoked).**

When the user installs or uses an smartphone electronic certificates on a new handset, such as when changing models or when purchasing a new handset due to transfer or loss.

Stop using the electronic certificate installed in the old handset.

**Not installing a electronic certificate on a new handset.**

The user has decided not to use the smartphone electronic certificates on the new handset or canceled the smartphone itself.

Revocation procedure

Deletion

In the procedure for new use on a new handset, revoking the electronic certificate of the old handset is also implemented **[Countermeasure 1-1]**

Remotely delete the old handset's electronic certificate and private key in response to the revocation of the old handset's electronic certificate **[Countermeasure 1-2]**

**[Issue 2]**
Revocation completed. There are cases where it will not be deleted, such as when the smartphone is not connected to a network.

Recommending the procedures on the old handset.

It is legally assumed that the user is obliged to apply for revocation.

**[If performing the revocation procedure on the old handset]**

Apply for (arbitrary) revocation from the old handset **[Countermeasure 2-1]**

In response to an application for revocation of an old handset, delete the electronic certificate and private key in the old handset **[Countermeasure 2-2]**

Revoked and deleted.

Assuming a user who does not apply even if the old handset is not at hand**, such as in case of loss**.

**[If not performing the revocation procedure on the old handset]**

(The electronic certificate of the old handset has not been revoked)

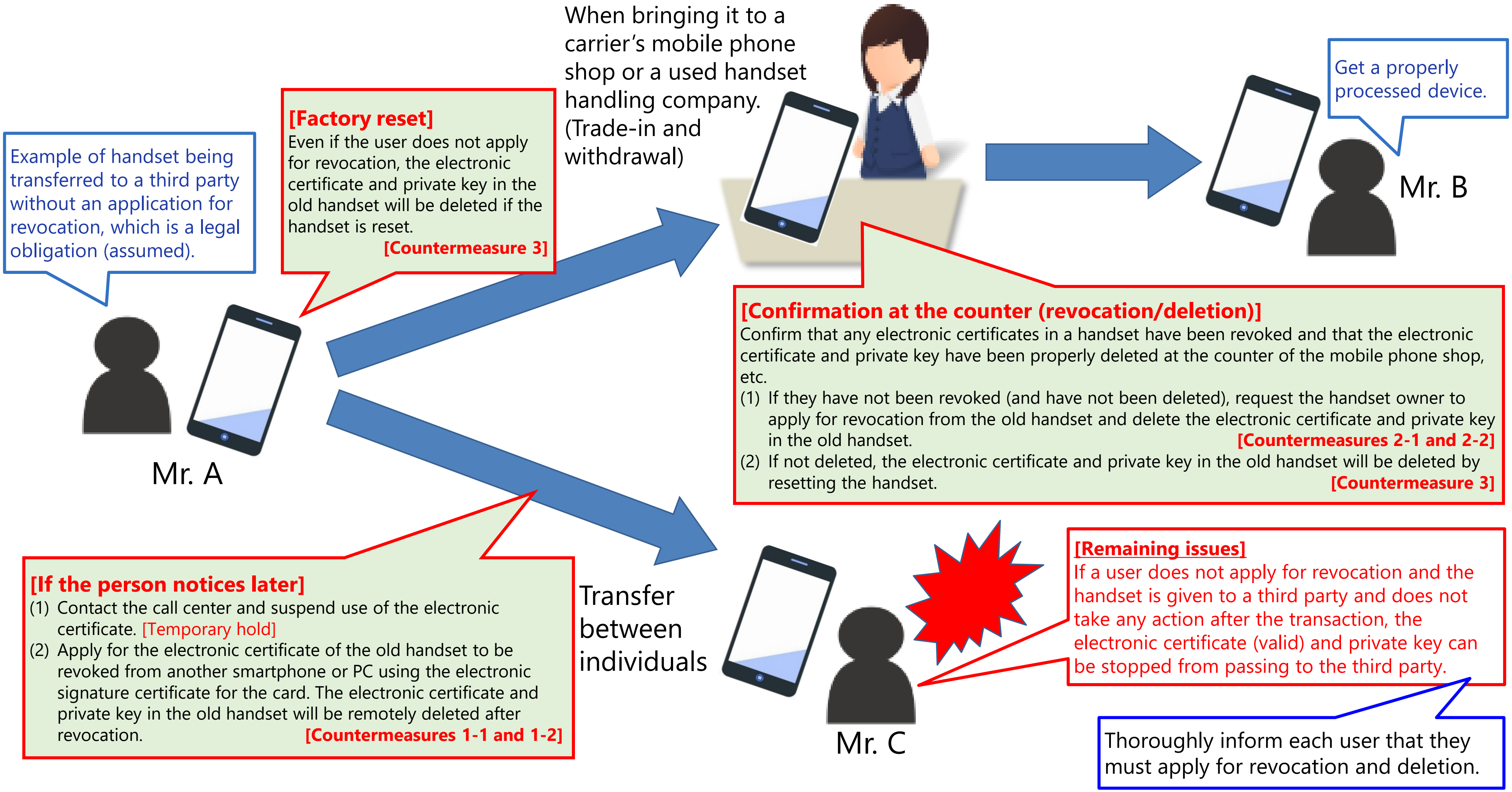
(The electronic certificate and private key of the old handset have been left undeleted)

PIN/password protected.

**[Issue 1]**
Risk of transfer to a third party with an unrevoked electronic certificate remaining in the handset

# Countermeasure plan for unrevoked electronic certificates remaining in handsets (Issue 1)

When suspending smartphone electronic certificates, it is legally assumed that users are obliged to apply for revocation. Still, it is also assumed that they will not apply for revocation in reality. In that case, since any remaining unrevoked electronic certificates in a smartphone will be transferred to a third party, the following measures will be considered to eliminate the risk of unauthorized use. (Note: As with the case of a lost card, smartphone electronic certificates are also protected with a PIN/password, so the risk of misuse is considered low).



Example of handset being transferred to a third party without an application for revocation, which is a legal obligation (assumed).

**[Factory reset]**
Even if the user does not apply for revocation, the electronic certificate and private key in the old handset will be deleted if the handset is reset.
**[Countermeasure 3]**

When bringing it to a carrier's mobile phone shop or a used handset handling company. (Trade-in and withdrawal)

Get a properly processed device.

**[Confirmation at the counter (revocation/deletion)]**
Confirm that any electronic certificates in a handset have been revoked and that the electronic certificate and private key have been properly deleted at the counter of the mobile phone shop, etc.

(1) If they have not been revoked (and have not been deleted), request the handset owner to apply for revocation from the old handset and delete the electronic certificate and private key in the old handset. **[Countermeasures 2-1 and 2-2]**

(2) If not deleted, the electronic certificate and private key in the old handset will be deleted by resetting the handset. **[Countermeasure 3]**

Transfer between individuals

**[If the person notices later]**

(1) Contact the call center and suspend use of the electronic certificate. [Temporary hold]

(2) Apply for the electronic certificate of the old handset to be revoked from another smartphone or PC using the electronic signature certificate for the card. The electronic certificate and private key in the old handset will be remotely deleted after revocation. **[Countermeasures 1-1 and 1-2]**

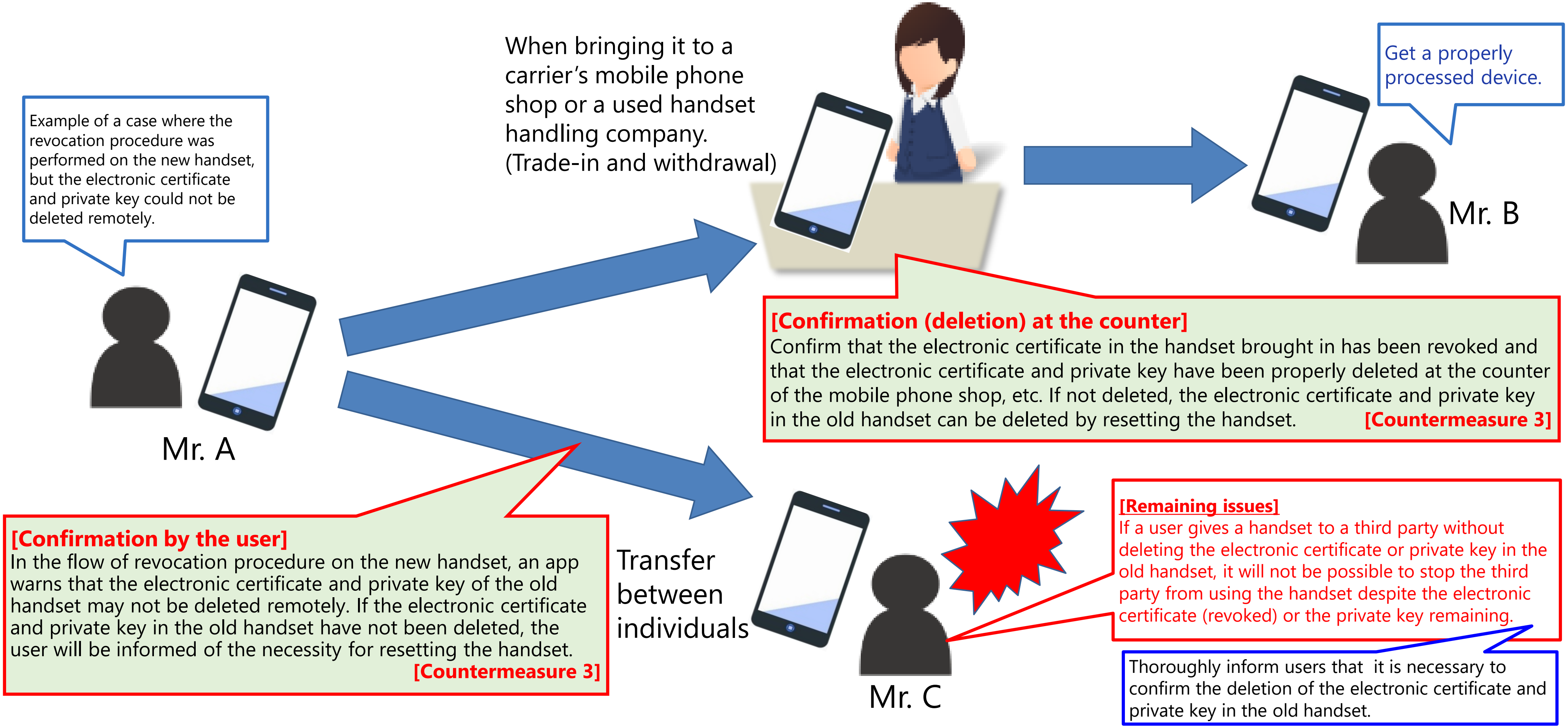
**[Remaining issues]**
If a user does not apply for revocation and the handset is given to a third party and does not take any action after the transaction, the electronic certificate (valid) and private key can be stopped from passing to the third party.

Thoroughly inform each user that they must apply for revocation and deletion.

# Countermeasure plan for remaining electronic certificates and private keys in handsets (Issue 2)

In the new usage procedure on the new handset, there are cases where an old handset is not connected to a network when the electronic certificate in the old handset is revoked, and the electronic certificate or private key in the old handset is **not deleted remotely**. Also, there are cases where the user has created settings to not receive push notifications.

=> The electronic certificate itself has been revoked and cannot be used, but there is a risk of unauthorized use* as a result of a handset being given to a third party while a electronic certificate or private key remains in the old handset. The following measures should be taken to prevent this.


Example of a case where the revocation procedure was performed on the new handset, but the electronic certificate and private key could not be deleted remotely.
Mr. A
When bringing it to a carrier's mobile phone shop or a used handset handling company. (Trade-in and withdrawal)
Get a properly processed device.
Mr. B
Transfer between individuals
Mr. C

**[Confirmation (deletion) at the counter]**
Confirm that the electronic certificate in the handset brought in has been revoked and that the electronic certificate and private key have been properly deleted at the counter of the mobile phone shop, etc. If not deleted, the electronic certificate and private key in the old handset can be deleted by resetting the handset. **[Countermeasure 3]**

**[Confirmation by the user]**
In the flow of revocation procedure on the new handset, an app warns that the electronic certificate and private key of the old handset may not be deleted remotely. If the electronic certificate and private key in the old handset have not been deleted, the user will be informed of the necessity for resetting the handset. **[Countermeasure 3]**

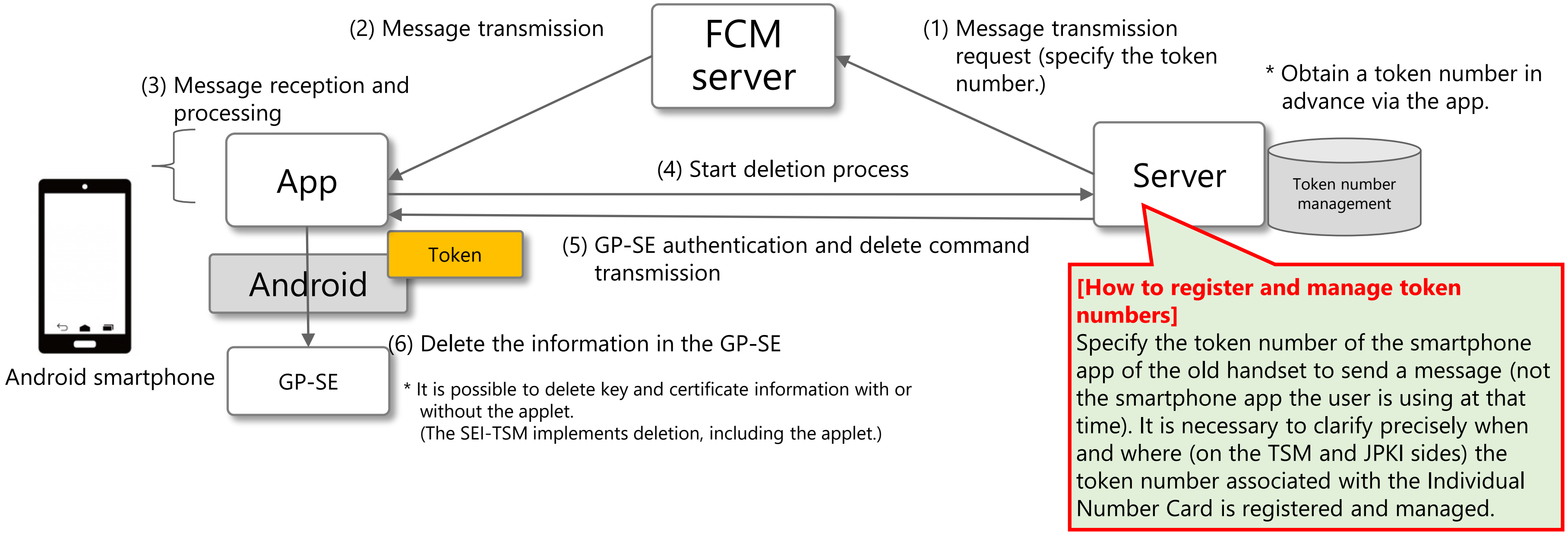
**[Remaining issues]**
If a user gives a handset to a third party without deleting the electronic certificate or private key in the old handset, it will not be possible to stop the third party from using the handset despite the electronic certificate (revoked) or the private key remaining.

Thoroughly inform users that it is necessary to confirm the deletion of the electronic certificate and private key in the old handset.

* The basic four information items recorded in the electronic signature certificates may be read, or the electronic signature may be digitally signed with the private key associated with the revoked electronic signature certificates. Regarding the latter, technical measures to prevent electronic signatures will be considered separately.

# Remote deletion of information in a GP-SE

- **It is technically possible to initiate a request from a server, access a GP-SE, and delete GP-SE information.**
- **FCM (Firebase Cloud Messaging) can be used, this is a service provided by Google that sends messages from a server to an application on a smartphone.**
- **A unique number called a token is issued for each smartphone by the FCM mechanism, and a server sends a message using the token number as a key.**
- **It is possible to perform processing by communication between this server and the application without the app being operated by the user.**
- **It is not a service that guarantees that remote processing will always succeed, and there may be cases where information cannot be deleted.**
  - If a smartphone is not connected to a network, then message transmission will fail.
  - Message transmission will also fail if the app is deleted, the device is rest, or the token is deleted or invalidated.
  - Message transmission from the FCM server may fail for other reasons.


(2) Message transmission
FCM server
(1) Message transmission request (specify the token number.)
(3) Message reception and processing
App
(4) Start deletion process
Server
Token number management
Token
Android
(5) GP-SE authentication and delete command transmission
(6) Delete the information in the GP-SE
GP-SE
Android smartphone

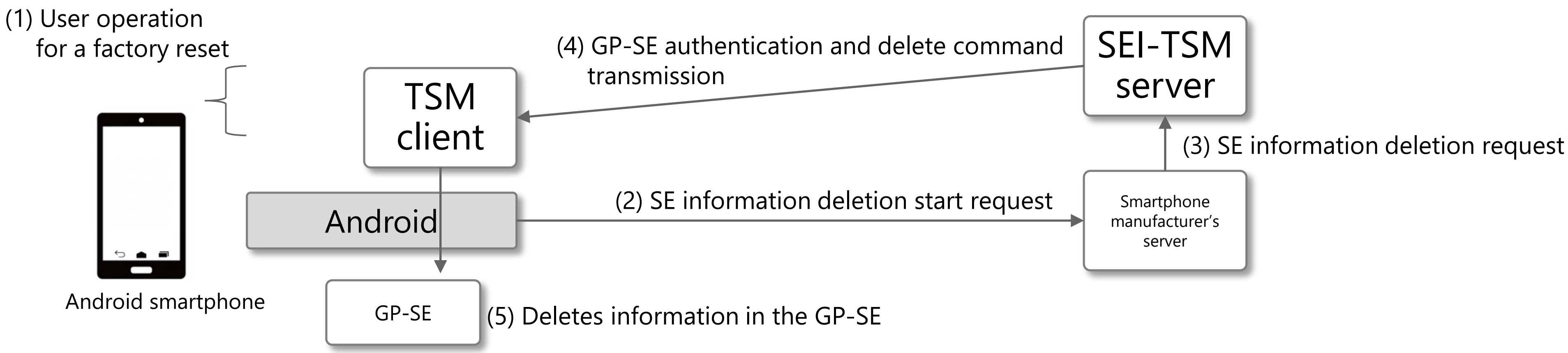
* Obtain a token number in advance via the app.

* It is possible to delete key and certificate information with or without the applet.
(The SEI-TSM implements deletion, including the applet.)

**[How to register and manage token numbers]**
Specify the token number of the smartphone app of the old handset to send a message (not the smartphone app the user is using at that time). It is necessary to clarify precisely when and where (on the TSM and JPKI sides) the token number associated with the Individual Number Card is registered and managed.

# GP-SE information deletion via factory reset

- **It is technically possible to delete (clear) GP-SE information when a user resets their smartphone.**
  However, to achieve this it is necessary to obtain the cooperation of Google, which is the provider of Android OS, and smartphone makers.
- **When a handset is reset it makes a request to the server to delete GP-SE information.**


(1) User operation for a factory reset
Android smartphone
TSM client
Android
GP-SE
(4) GP-SE authentication and delete command transmission
SEI-TSM server
(3) SE information deletion request
(2) SE information deletion start request
Smartphone manufacturer's server
(5) Deletes information in the GP-SE

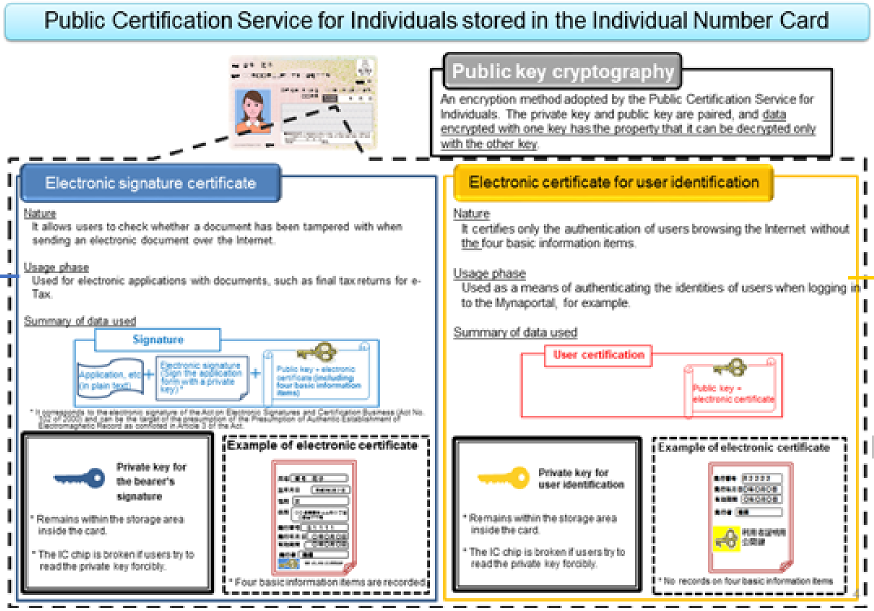
# Utilization of biometric authentication

## 1. Utilization of Biometric Authentication on Smartphones

Biometric authentication on smartphones has become popular and matured by industrial collaboration including NTT DOCOMO's efforts, which started from the biometrics and FIDO adoption in docomo's Android smartphones with the world-first Iris scanner equipped device in May 2015. In view of the mechanism that realizes this, we'd like to propose to utilize biometrics authentication functionality on FeliCa-SE built-in smartphones starting with electric certificates for "user identification."

Signature password:
an alphanumeric password of
6 to 16 single-byte characters

A continuous study is required to confirm whether it is possible to verify the holder of the certificate using the built-in biometric authentication functionality of smartphones in the market.



Public Certification Service for Individuals stored in the Individual Number Card

**Public key cryptography**

An encryption method adopted by the Public Certification Service for Individuals. The private key and public key are paired, and data encrypted with one key has the property that it can be decrypted only with the other key.

**Electronic signature certificate**

Nature
It allows users to check whether a document has been tampered with when sending an electronic document over the Internet.

Usage phase
Used for electronic applications with documents, such as final tax returns for e-Tax.

Summary of data used

Signature
Application, etc (in plain text)
+
Electronic signature (Sign the application form with a private key)*
+
Public key + electronic certificate (including four basic information items)

* It corresponds to the electronic signature of the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000) and can be the target of the presumption of the Presumption of Authentic Establishment of Electromagnetic Record as confirmed in Article 3 of the Act.

Private key for the bearer's signature

* Remains within the storage area inside the card.

* The IC chip is broken if users try to read the private key forcibly.

Example of electronic certificate

* Four basic information items are recorded.

**Electronic certificate for user identification**

Nature
It certifies only the authentication of users browsing the Internet without the four basic information items.

Usage phase
Used as a means of authenticating the identities of users when logging in to the Mynaportal, for example.

Summary of data used

Private key for user identification

* Remains within the storage area inside the card.

* The IC chip is broken if users try to read the private key forcibly.

Example of electronic certificate

* No records on four basic information items

User identification password:
(PIN) 4-digit number

It is possible to verify the holder of the certificate with the built-in biometric authentication function of smartphones in the market.

© 2020 NTT DOCOMO, INC. All Rights Reserved.

Second meeting of the Study Group on Smartphones with Individual Number Card Functionality
Document 7 "Proposals Based on the Knowledge Gained Through the Installation of Biometric Authentication on Smartphones and the Application of FIDO Authentication" (Moriyama, a member of the Study Group)

# Overview of FIDO authentication

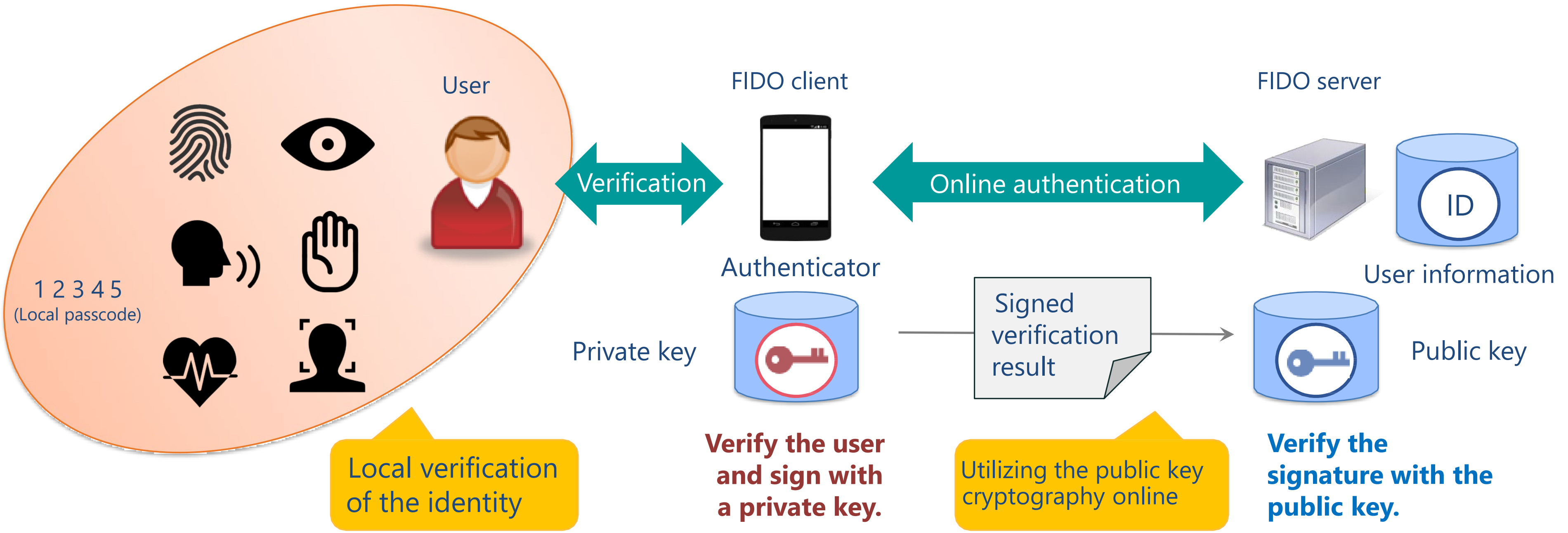
- FIDO ALLIANCE, INC. (A NONPROFIT MUTUAL BENEFIT CORPORATION) -

## FIDO Alliance

FIDO Alliance was established in 2012, and consists of about 250 companies. It is a global nonprofit organization (mutual interest corporation) based on Californian law, USA.

To solve problems related to passwords and authentication, it promotes further introduction and development through the formulation of technical specifications based on a FIDO authentication model, as well as program management for introducing and deploying technical specifications, and collaboration with each standardization organization.

## FIDO authentication model (do not share secrets between the handset and server)



Local verification of the identity

**Verify the user and sign with a private key.**

Utilizing the public key cryptography online

**Verify the signature with the public key.**

Authentication is realized by verifying that the user has an appropriate private key in the authenticator, and (dynamic) multi-factor authentication is achieved with the authenticator's simple operation.