JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

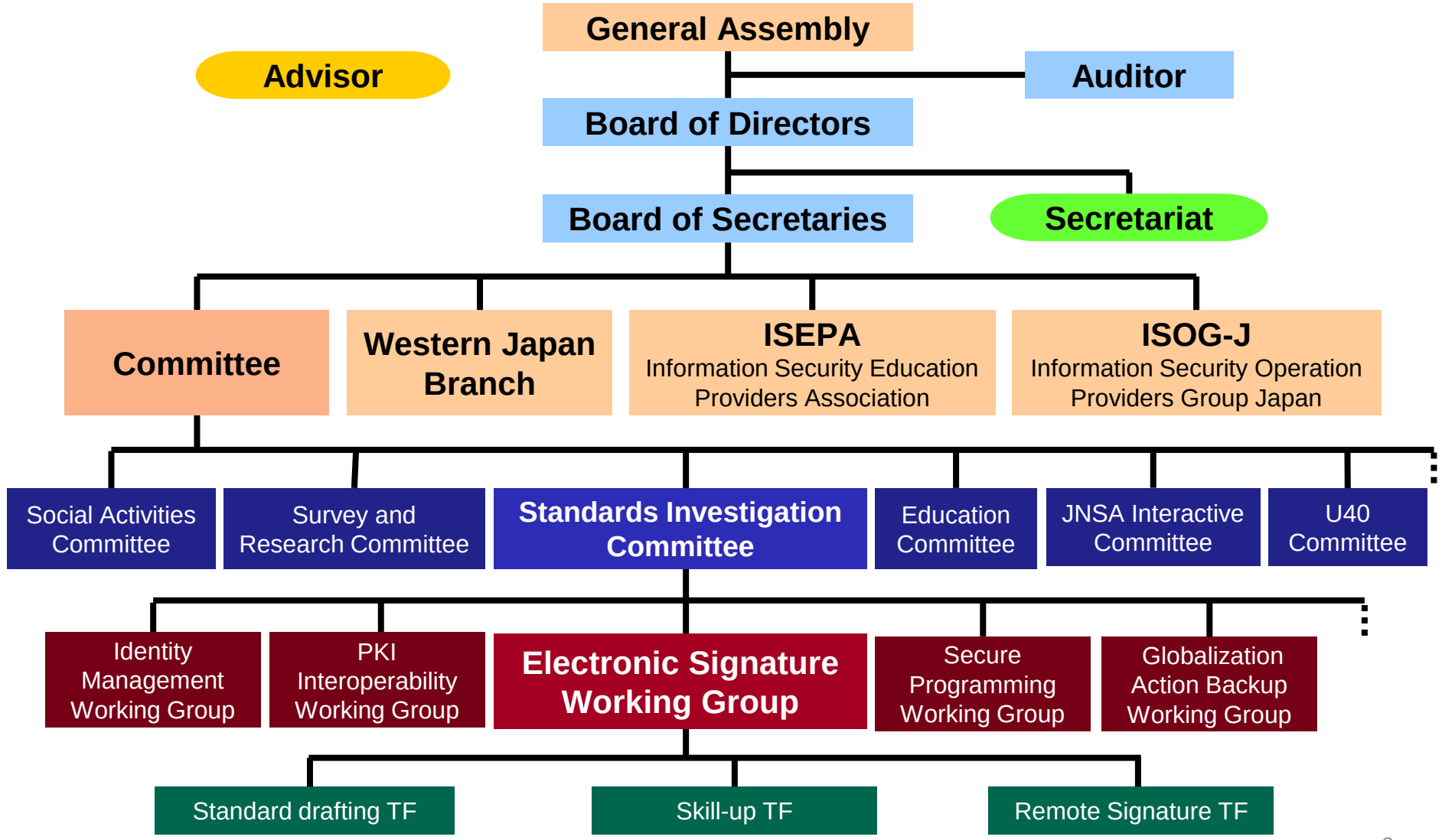
# Status of Remote Signature Adoption and Implementation in Japan

Japan Network Security Association
Remote Signature Task Force Leader
Mizuho Information & Research Institute, Inc.
Management & IT Consulting Div Manager
Hirohisa OGAWA

# Main Topics

- Activities of JNSA & Electronic Signature WG
- Remote Signature Task Force & METI's Projects
- Activities supporting Electronic Signature Adoption and Implementation

# Japan Network Security Association Organization Chart




Member company: 191 companies (as of May 16, 2017)

# Relationship with other organizations

**ETSI/TC ESI**

Associate Member

**JNSA**
**Electronic Signature**
**Work Group**

**JAHIS**

Technical cooperation
ex) Electronic Prescription

**TBF**

Partner
ex) Timestamp, Trust List

**ISO/TC154**

Expert

International Organization for Standardization
ex) PAdES Profile

**ISO/TC171**

Expert

Document management applications
ex) PDF signature

**ISO/SC34**
**Technical committee**

Liaison

Document description and processing languages
ex) Long-term signature of XML

ETSI/TC ESI #42 meetings in Austria

JAHIS : Japanese Association of Healthcare Information Systems Industry
TBF : Time Business Forum in Japan Data Communications Association

# METI Projects involving JNSA

- International Standardization Project
  - Standard drafting TF's responsibility
    - ISO 14533-3:2017, Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)

- Remote Signature Project
  - Remote Signature TF's responsibility
    - In Japan, Electronic Signatures and certification businesses must adhere to the Electronic Signature Act (Act # 102), Electronic Signature Law Study Group studies all aspects of Remote signature
    - During 2016, we examined Remote Signature basic functions and security requirements

METI : Ministry of Economy, Trade and Industry

# Japanese Law as pertains to Electronic Signatures

Electronic Signatures and Certification Business

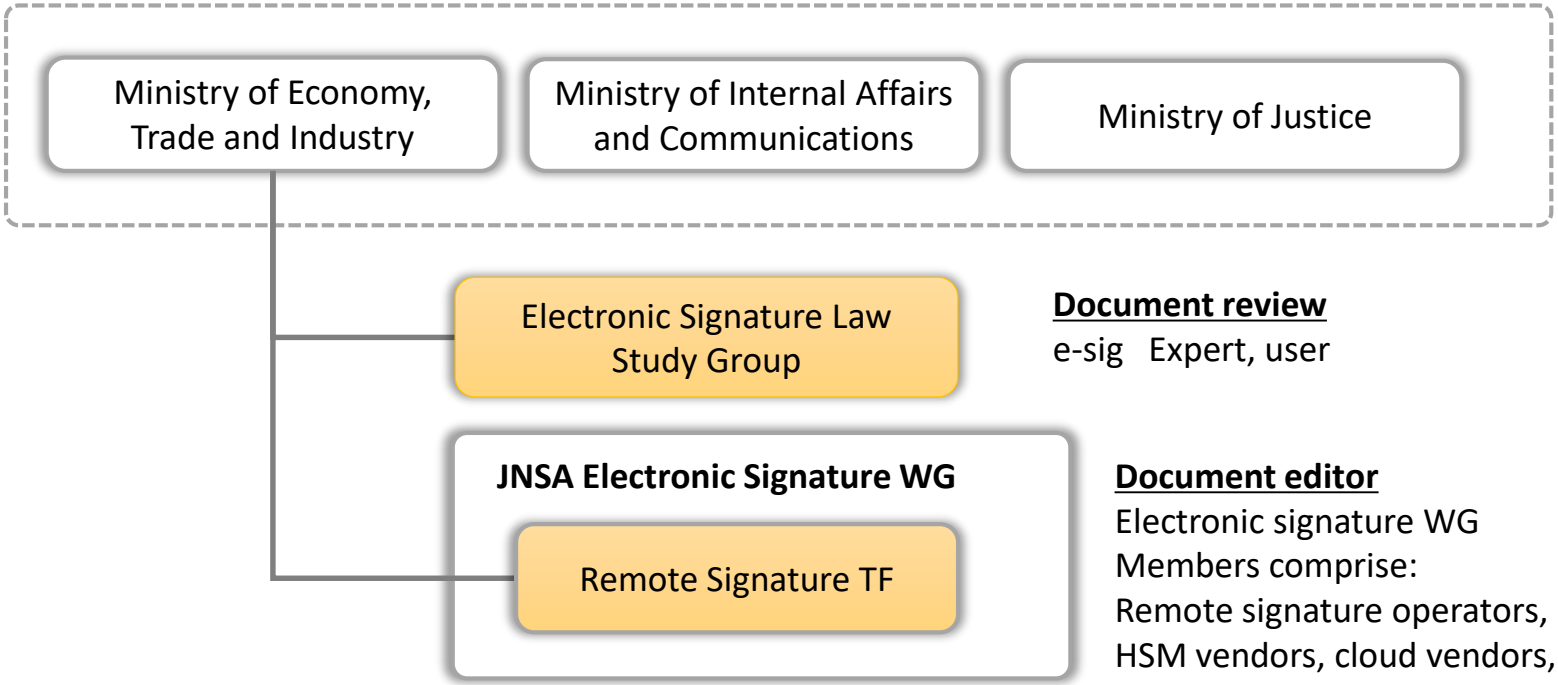
Act No. 102 - May 31, 2000

Article 3 Any electromagnetic record that is made in order to express information (except for that prepared by a public official in the course of duties) shall be presumed to be established authentically if the Electronic Signature (limited to that which can be performed by the principal through appropriate management of codes and properties necessary to perform this) is performed by the principal with respect to information recorded in such electromagnetic record.

Japanese Law Translation
http://www.japaneselawtranslation.go.jp/law/detail/?id=109&vm=04&re=01

# Electronic Signature Law Study Group

- The Electronic Signature Law Study Group holds a meeting on the Electronic Signature Act quarterly
- In 2015 and 2016 the group examined remote signatures
- Last year we implemented the following:

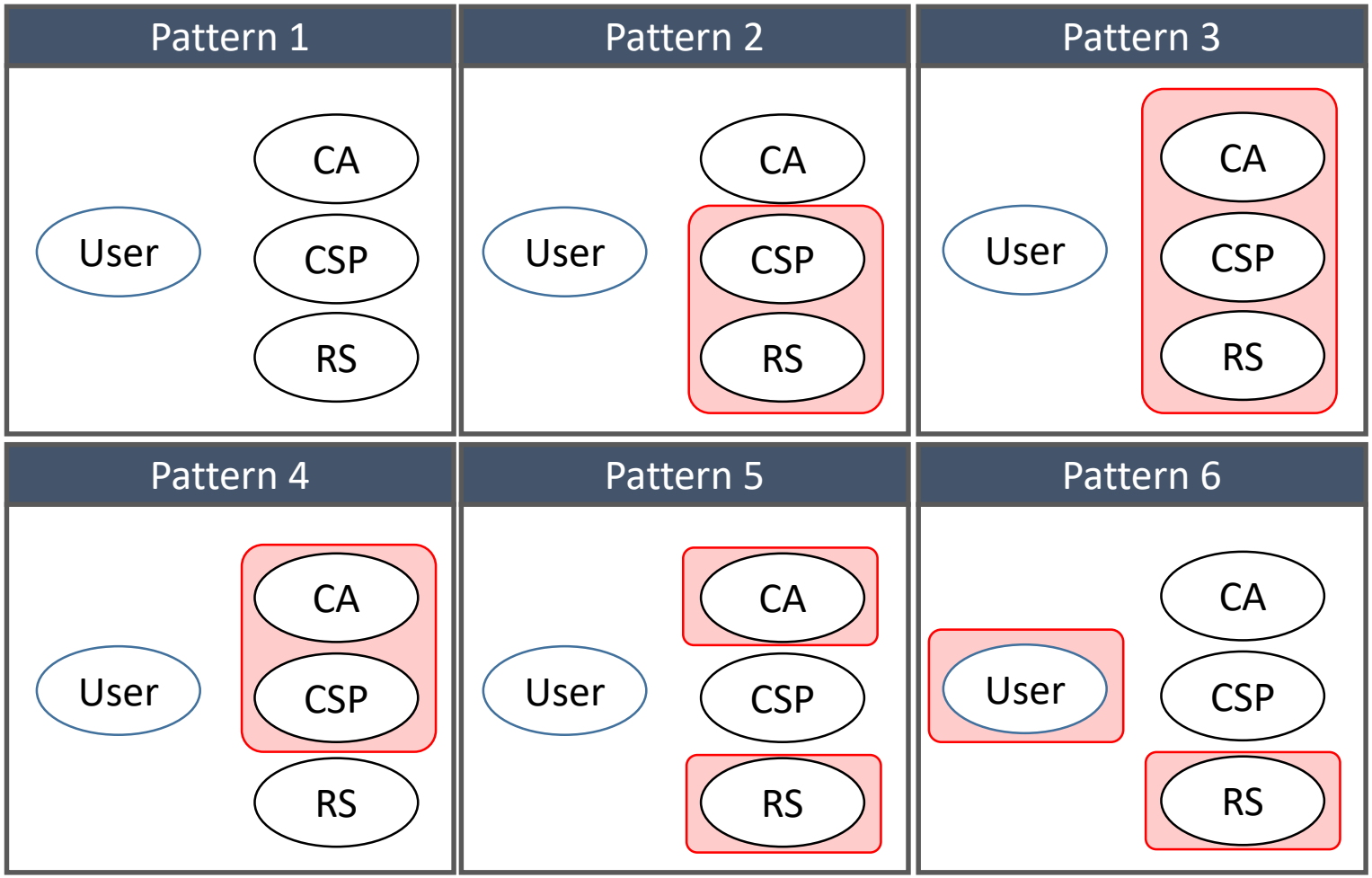


# 20 Items to consider for remote signature

| | | |
|---|---|---|
| I. Player / Role | 1 | Players and roles of remote signatures |
| II. Remote Signature / Provider | 2 | Requirements and assurance levels of remote signature providers |
| | 3 | Consideration of the level according to the use application of the signature |
| | 4 | Remote signature installation environment |
| | 5 | Basic Functional component in Remote Signature |
| IV. Registration Phase | 6 | User registration method |
| | 7 | Installation of Signing key of user (* generation and import of Signing key) |
| | 8 | Protection measures for user's Signing key |
| | 9 | Presence or absence of backup function of Signing key |
| V. Signature Phase | 10 | Requirements for signing instructions |
| | 11 | User authentication method |
| | 12 | Protection measures for user information and Signing key information |
| | 13 | Signature function requirement |
| | 14 | Presence or absence of transmission function of signed data |
| | 15 | Presence or absence of signature generation log function |
| | 16 | Presence or absence of signature verification function |
| | 17 | Confirmation of data to be signed by the user |
| VI. Other | 18 | Distributed signature processing in user environment |
| | 19 | Application of long-term signature |
| | 20 | Relation to Electronic Signature Law |

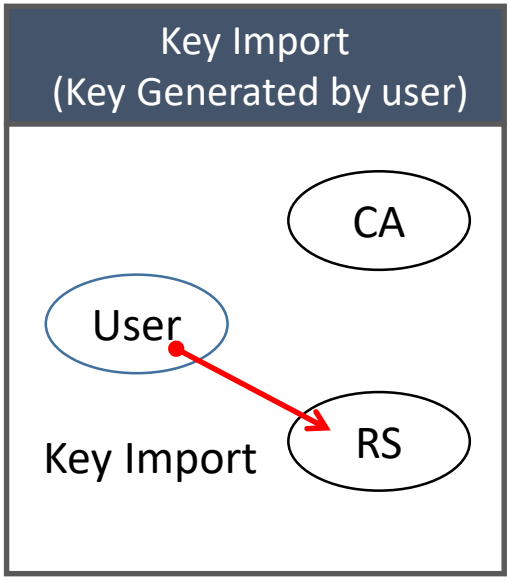
# 1. Players and roles of Remote Signatures

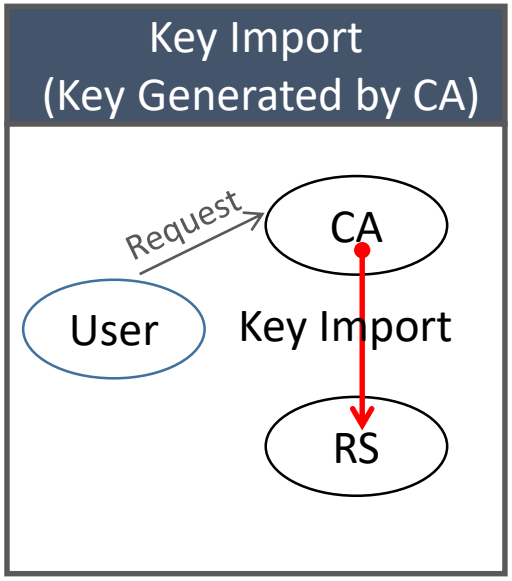
- Assumed remote signature pattern (Including concrete examples)
- A single company carries out the part surrounded by red.
- By implementing it in a single company, efficiency of user registration can be expected. But governance is necessary.

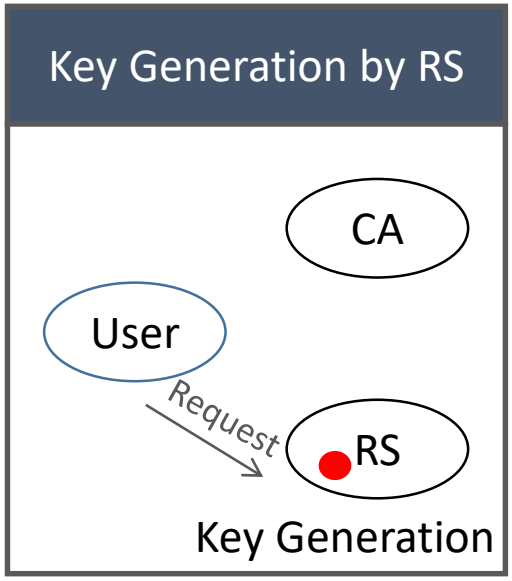


# 7. Installation of Signing key of user

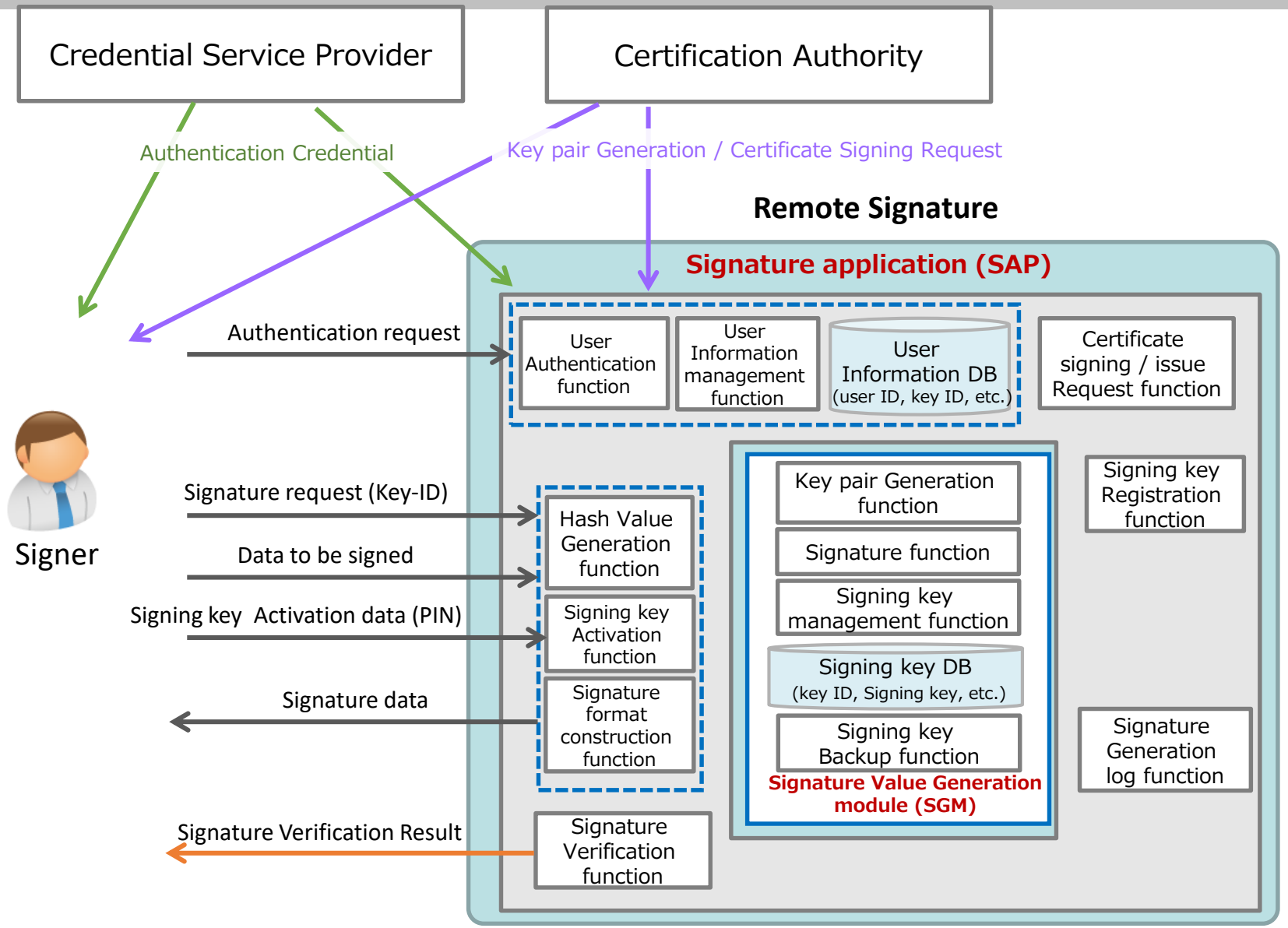
- It is about importing and generating signing keys. The user registers the user in the remote signature and sets the signature key to be used.



# 5. Basic Functional component in Remote Signature



# 5. Basic Functional component in Remote Signature

- SAP : Signature Application
- SGM : Signature value Generation Module

Signer

Signature application (SAP)

Signing key registration function
Certificate signing request (/issue ) function

User authentication function
User information management function
User information DB
(user ID, key ID, etc.)

Hash value generation function
Signing key activation function
Signature format construction function

Signature verification function

Signature generation log function

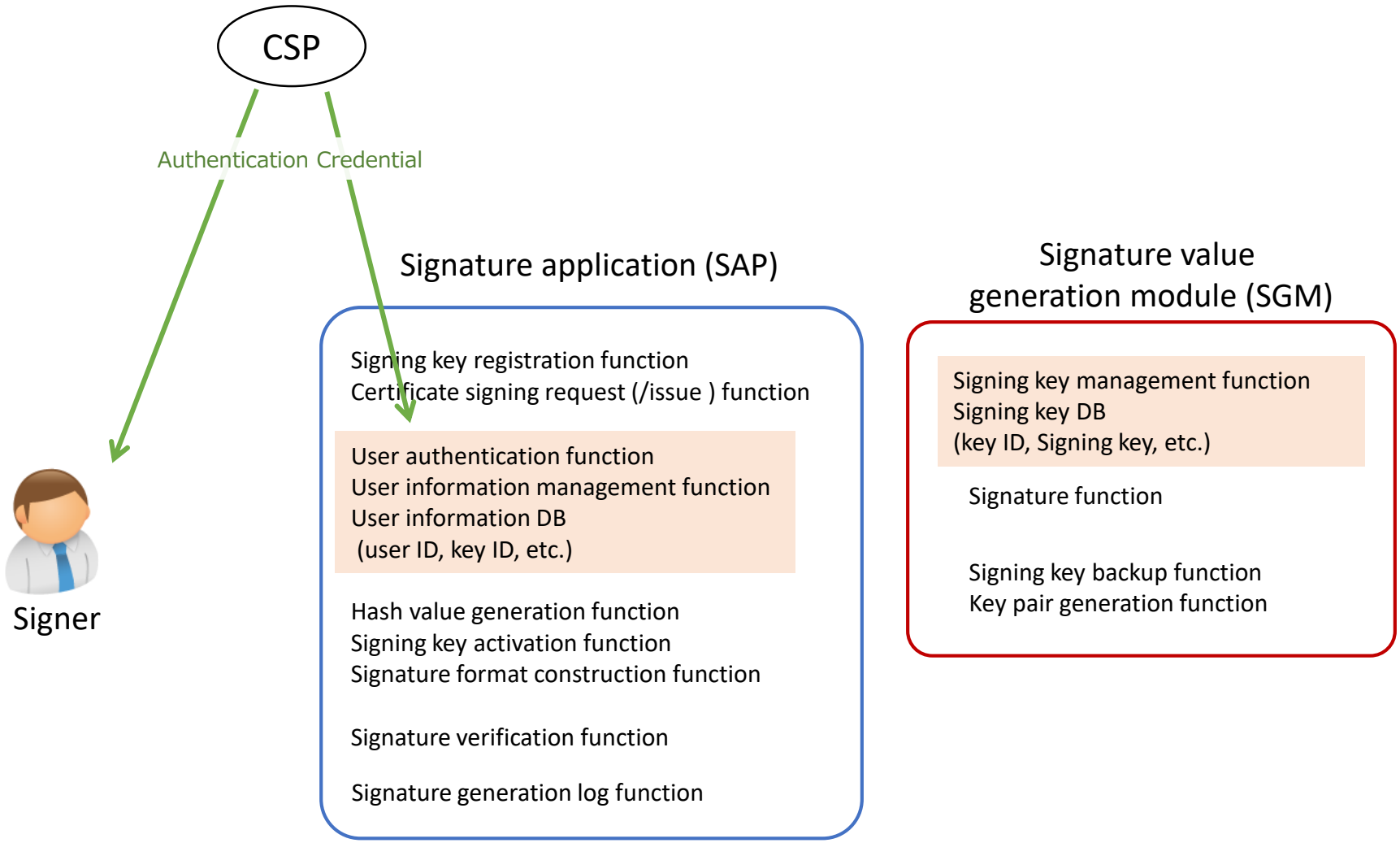
Signature value generation module (SGM)

Signing key management function
Signing key DB
(key ID, Signing key, etc.)

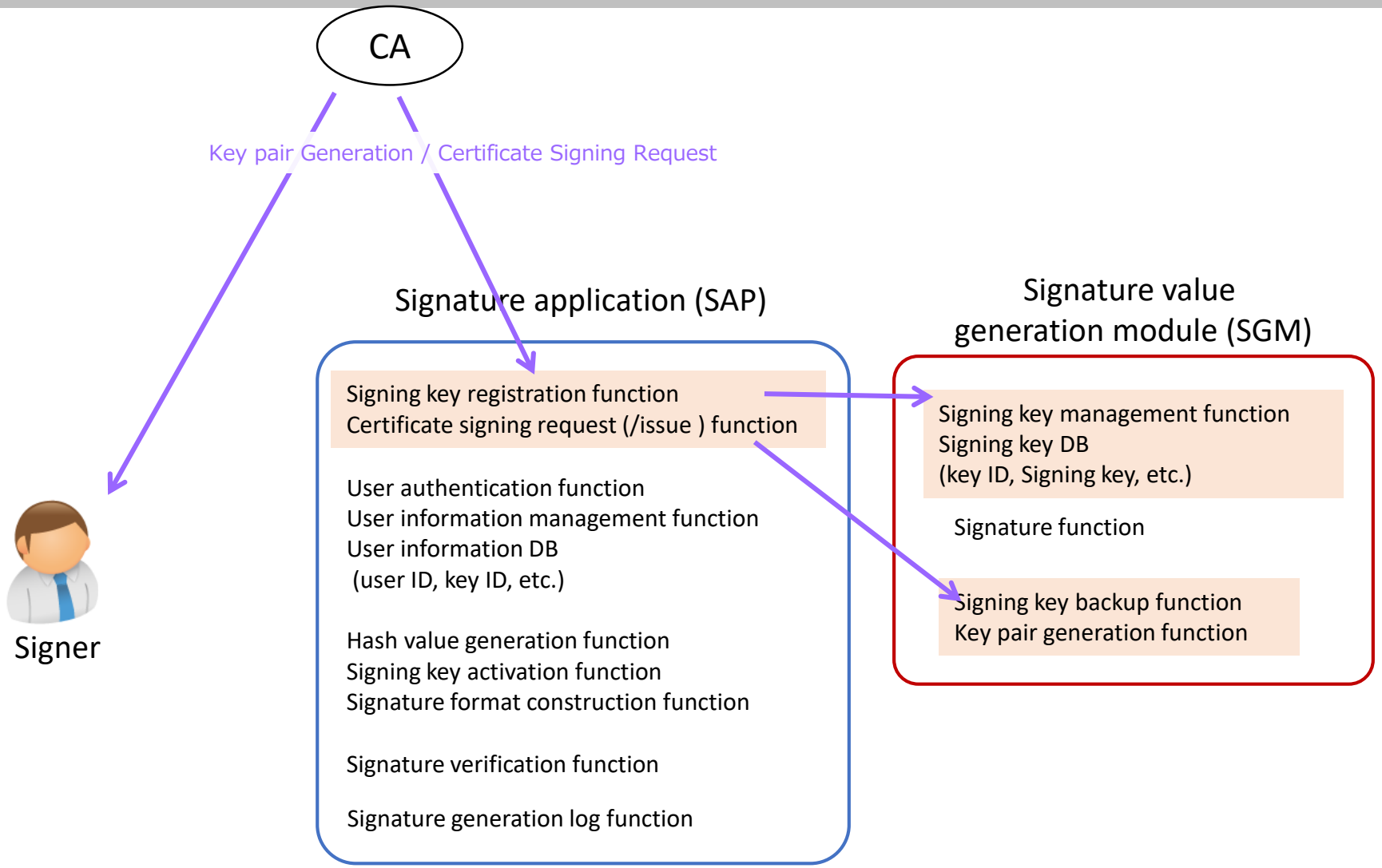
Signature function

Signing key backup function
Key pair generation function

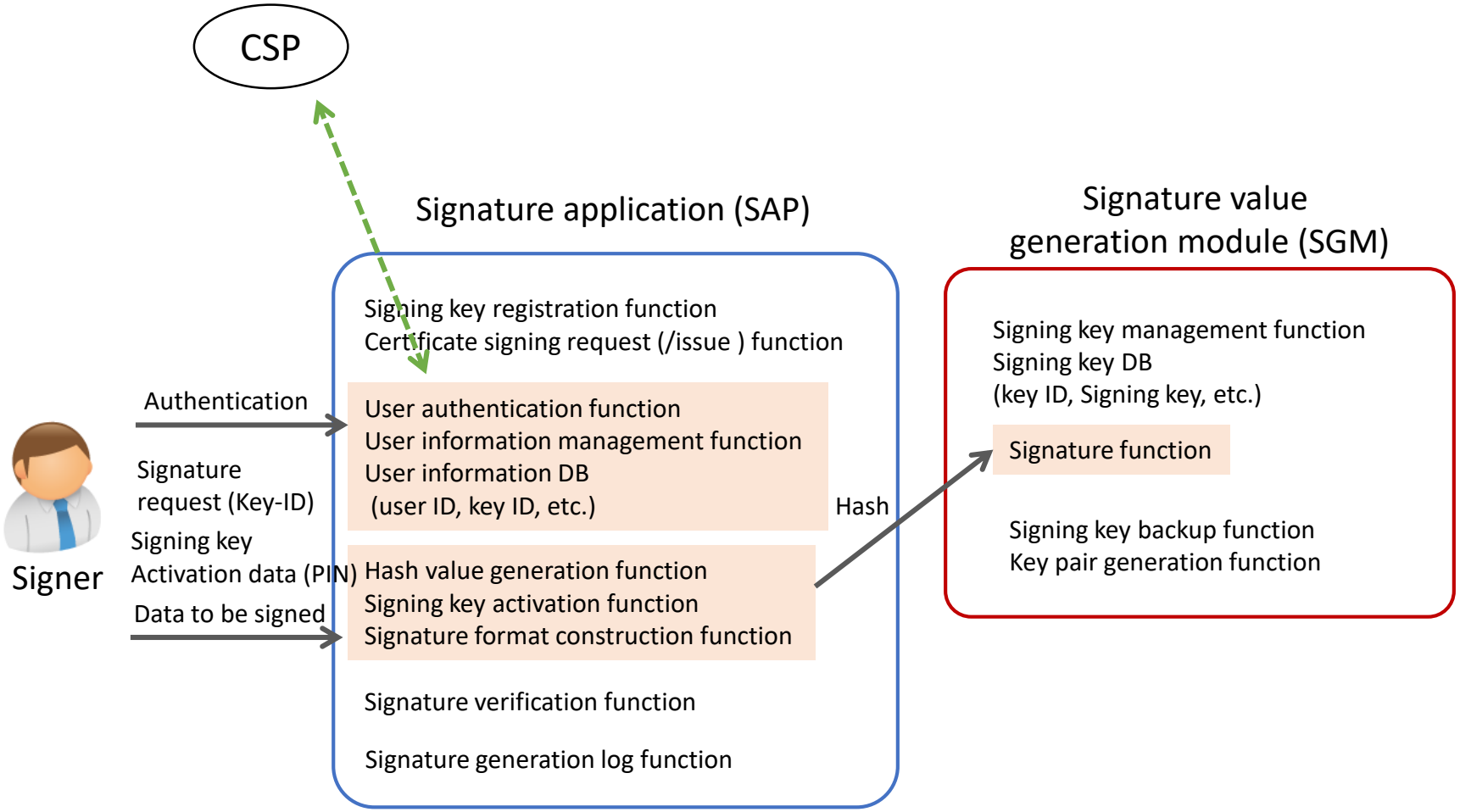
# Registration Phase (User information)



# Registration Phase (Signing Key Generation or Import)



# Signature Phase



# Result Confirmation Phase

Signer

Confirmation of signature result

Signature application (SAP)

Signing key registration function
Certificate signing request (/issue ) function

User authentication function
User information management function
User information DB
(user ID, key ID, etc.)

Hash value generation function
Signing key activation function
Signature format construction function

Signature verification function

Signature generation log function

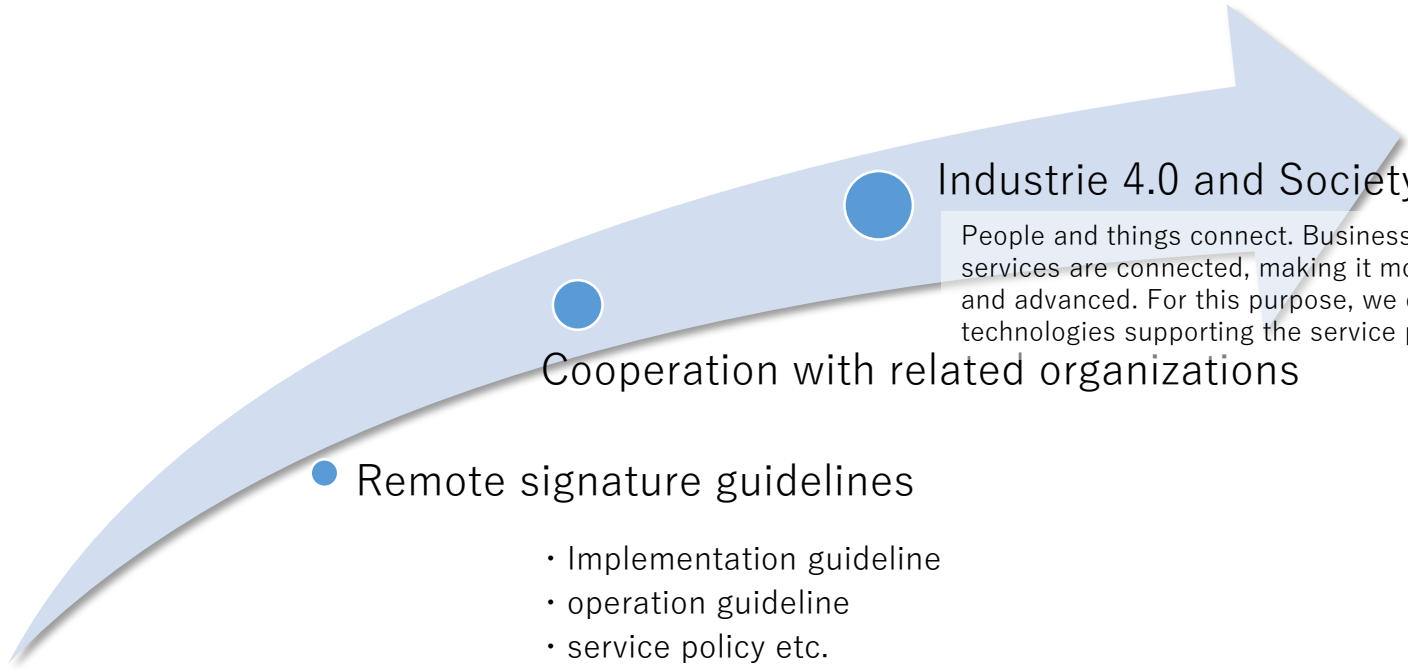
Signature value generation module (SGM)

Signing key management function
Signing key DB
(key ID, Signing key, etc.)

Signature function

Signing key backup function
Key pair generation function

# Next step JP in Remote signature




Establishment of Remote Signature consortium

JTSC

Japan Trusted Signature-service Consortium
(Tentative name)