SIP*（2nd phase)

Use of Trust Lists in Japan to build global trust spaces

*SIP(Cross-ministerial **S**trategic **I**nnovation Promotion **P**rogram) is a national program led by the Council for Science Technology and Innovation (CSTI) of the Japanese Government(the Cabinet Office).

22nd Sep. 2021

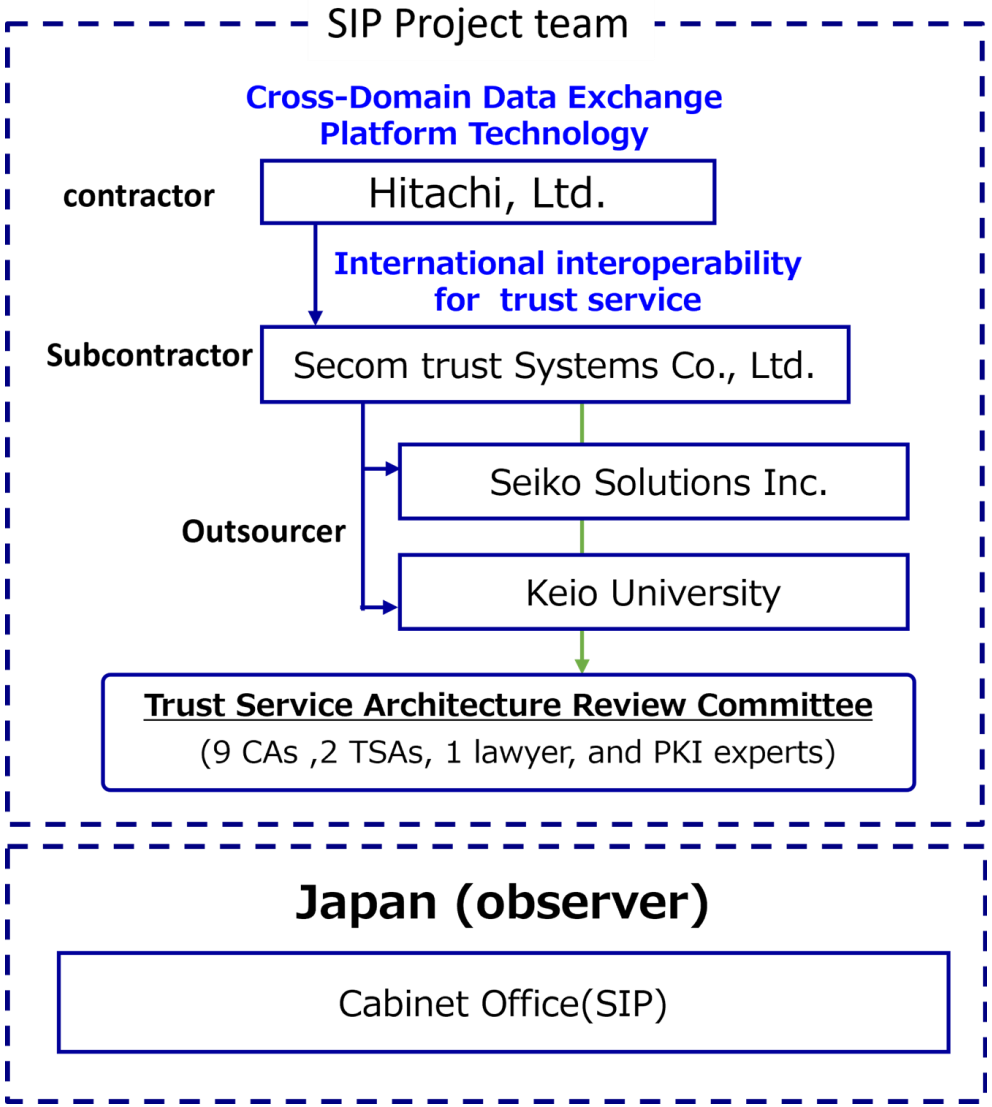
Cosmos Corporation,
a member of Trust Service Architecture review Committee
Soshi Hamaguchi

1. SIP project
    a. Overview
    b. API
    c. Japanese TSL (Prototype)
    d. PoC
    e. Self-Assessment

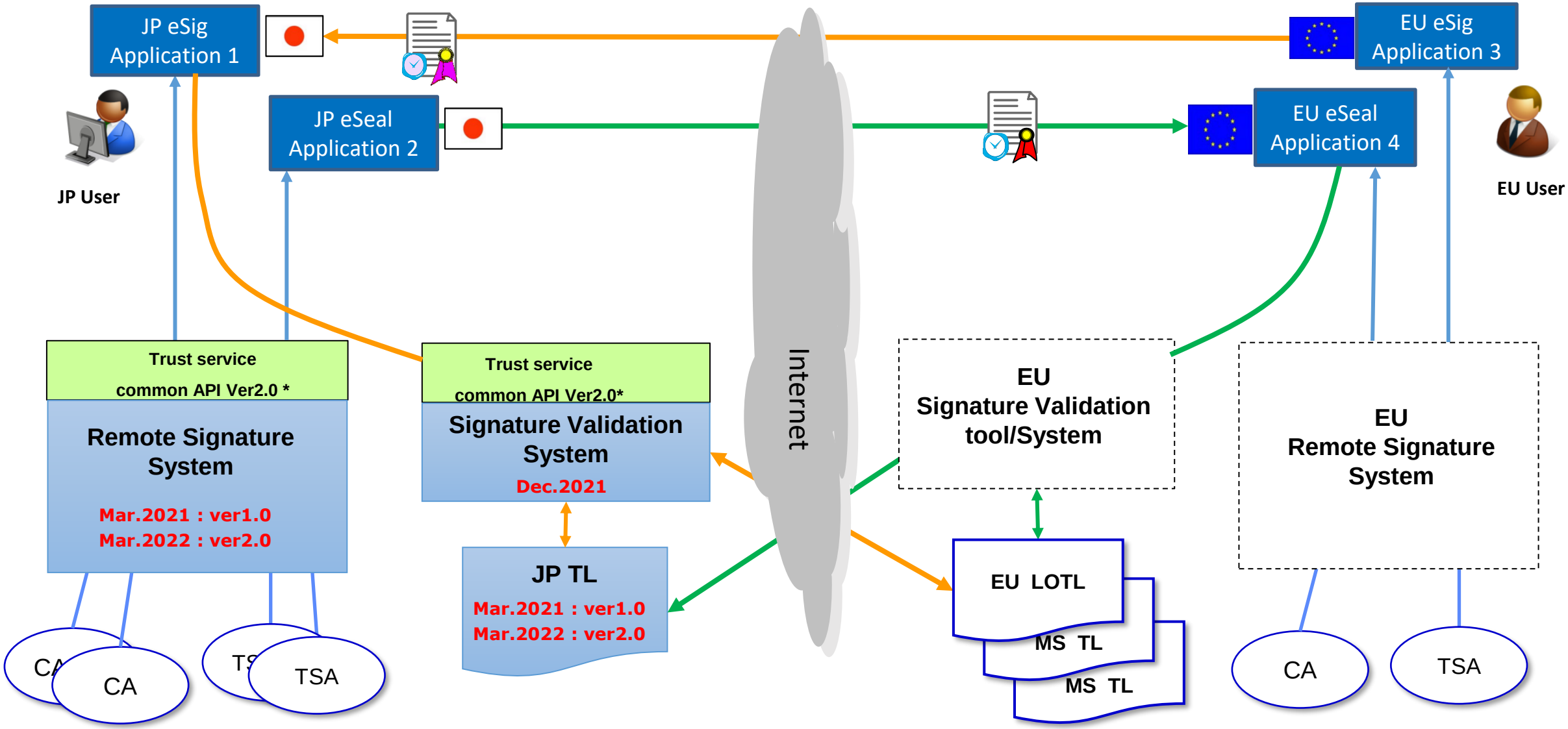
2. Digital Agency and upcoming Legislation on Trust services

1. SIP project

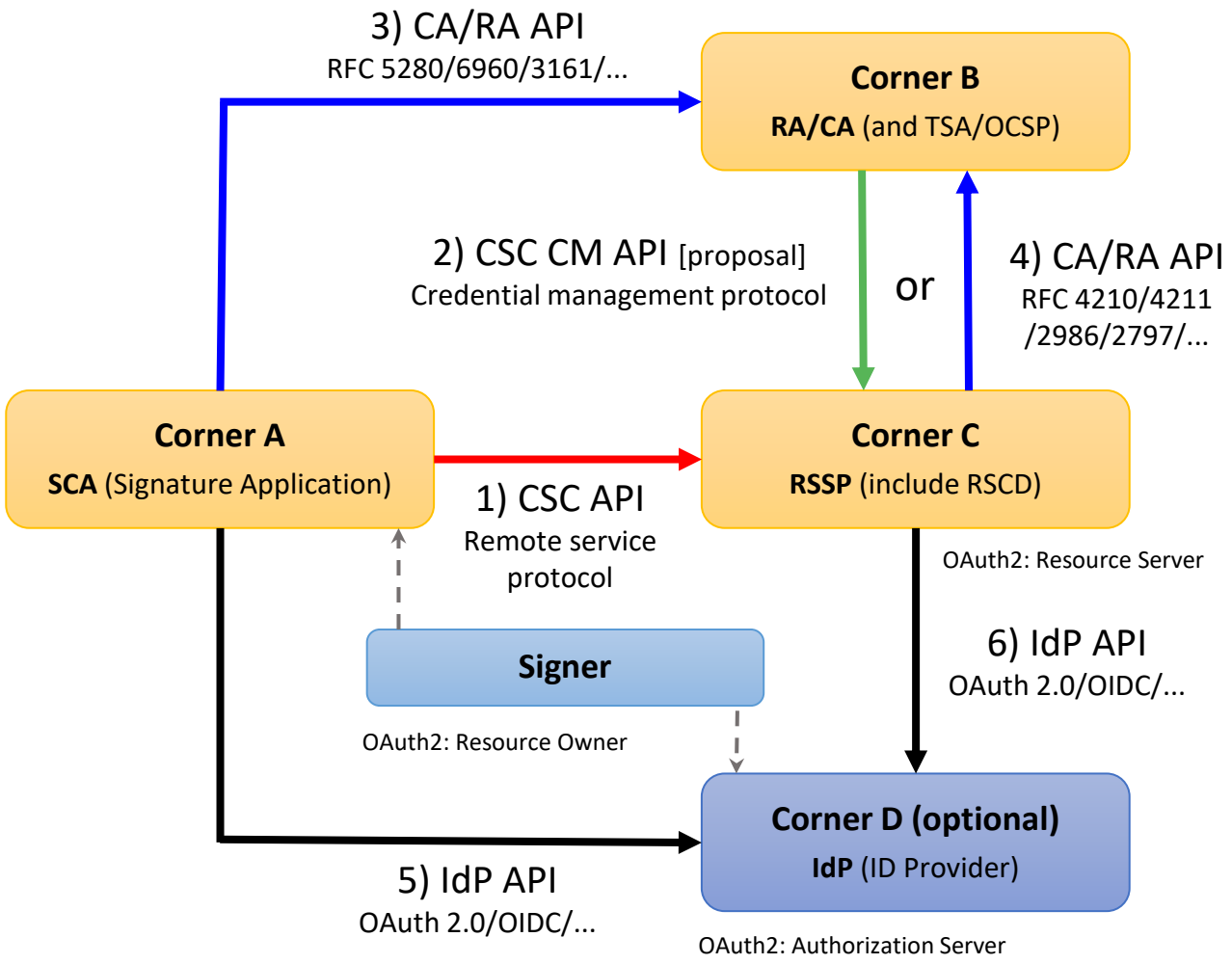
- 3-year project for examining mutual recognition of trust services between Japan and EU from Technical aspect launched in 2020.
- Scope of the Project
  - Mapping best practices
    - AdES format
    - QC
    - TSPs (CAs, TSAs and RSSP)
  - Developing missing APIs
    - Extension of CSC API
  - Implementing Trust representation
    - J-TSL (Japanese Trusted Status List)
  - Proof of Concept (Demonstration)
    - Validation of digital signature with J-TSL and EU LoTL
    - Remote signature creation with extended API



a. Overview of SIP project



b. API

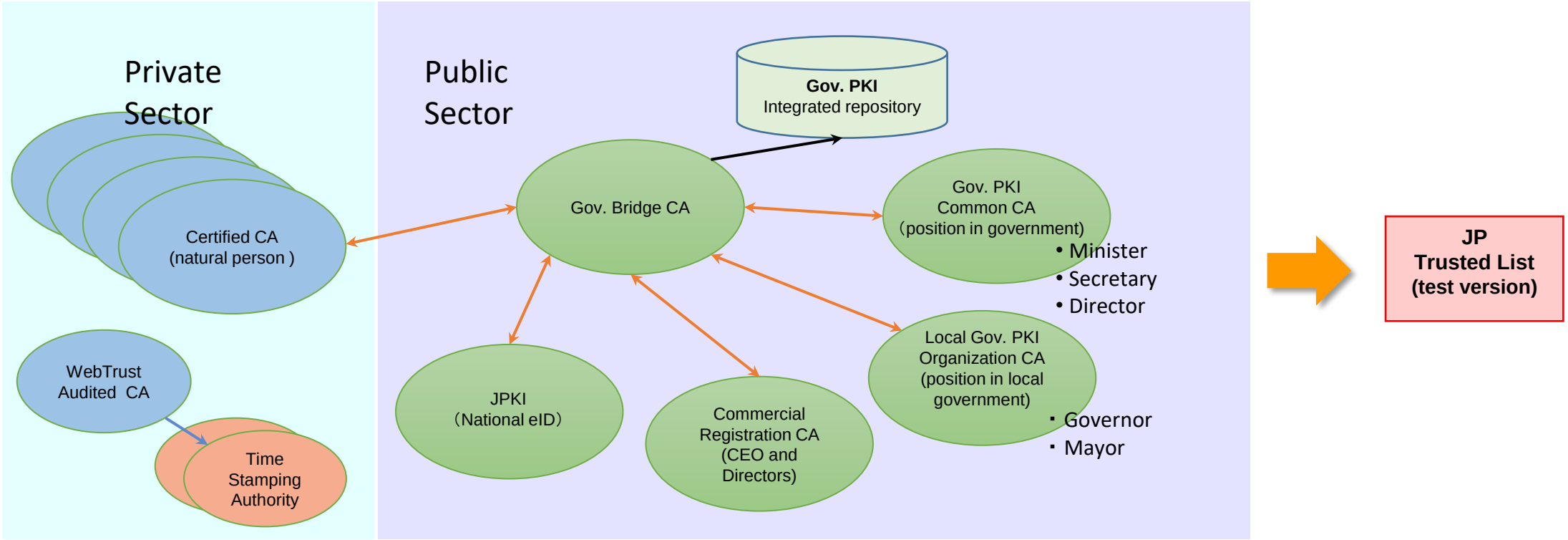


APIs	sender	receiver	standards
1) CSC API	SCA	RSSP	CSC v1 (v2) Remote service API
2) CSC CM API	CA/RA	RSSP	* Proposal to CSC * Credential management API
3) CA/RA API	SCA	CA/RA	RFC 5280 (X.509/CRL) RFC 6960 (OCSP) RFC 3161 (TSA)
4) CA/RA API	RSSP	CA/RA	RFC 4210 (CMP) RFC 4211 (CRMF) RFC 2986 (CSR) RFC 2797 (CMC)
5) IdP API	SCA	IdP	RFC 6749 (OAuth2.0) RFC 7636 (PKCE) OIDF: OpenID Connect
6) IdP API	RSSP	IdP	

➢Current version CSC APIs specified are between SCA to RSSP.
[Proposal]
➢We are proposing new CSC CM APIs from RA/CA to RSSP.

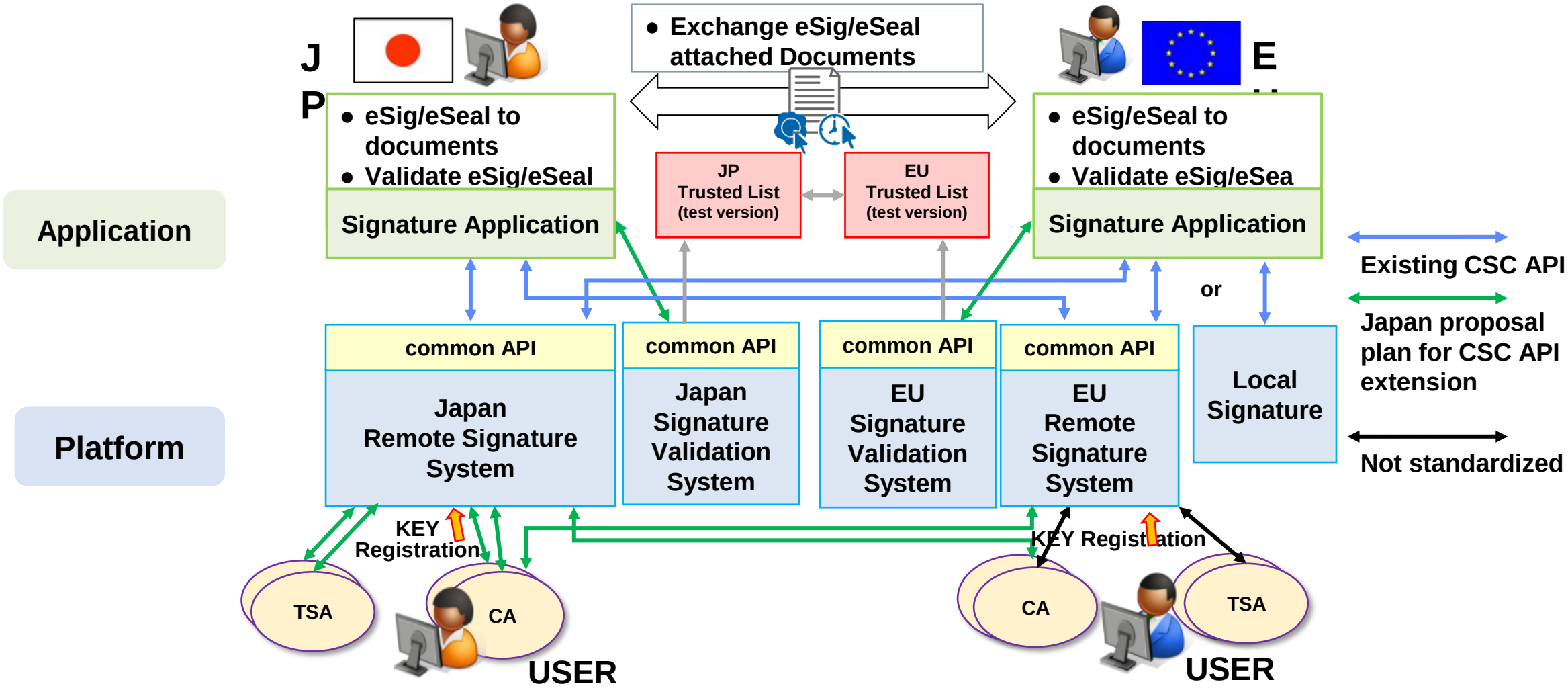
c. Japanese TSL

- **Current Trust representation**
  - **BCA model and "GPKI Interoperability specification" for cross-cert with Gov. BCA.**
  - **Private CAs certified in accordance with "eSignature Act" are also cross-cert with Gov. BCA.**
- **Japanese TSL**
  - **-based on ETSI TS 119 612**
  - **-All CAs cross-certified with Gov. BCA are listed**
  - **-All TSAs certified by the Government are also listed.**



d. PoC

SIP project have plan to demonstrate interoperability of QeSig and QeSeal by using Remote signature system between Japan and EU in 2022.



e. Self-Assessment

- **Self-assessments have conducted on;**
  - **-Electronic signature**
  - **-Time stamping**
  - **-Remote electronic signature**

Examples of identified gaps: Financial stability, Background check for personnel, Penalties, Termination of TSP business, Risk assessment, ISMS perspectives

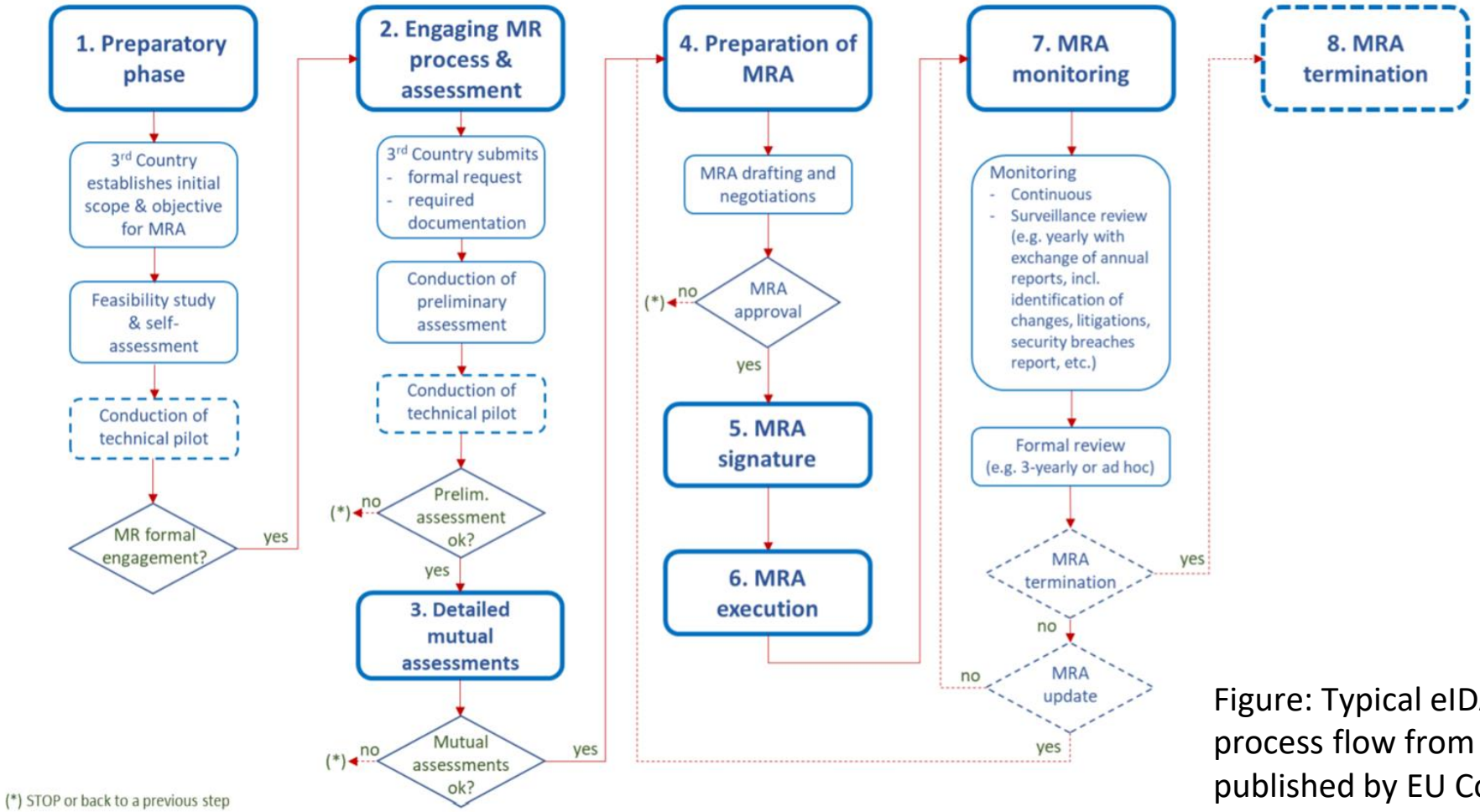


Figure: Typical eIDAS Art.14 MRA life-cycle process flow from "MRA cookbook" published by EU Commission

2. Digital Agency and upcoming Legislation on Trust services

➢ Digital Agency Law enacted in May 2021

> *In order to promote measures for the formation of a digital society in a speedy and focused manner, Digital Agency shall be established to assist the Cabinet, together with the Cabinet Secretariat, in the affairs of the Cabinet relating to the formation of a digital society and to ensure the speedy and focused execution of administrative affairs relating to the formation of a digital society, and matters relating to the affairs under its jurisdiction and organization shall be prescribed.*

- Digital Agency has been launched on September 1st , 2021.
- Roughly 600 officials expected
- Creation of the comprehensive trust legislation and institutions under this agency is proposed by the Comprehensive Data Strategy approved by Cabinet secretariat in June 2021.

➢ Comprehensive Data Strategy

One of the main pillar of the strategy is building a trust Infrastructure which is;

- comprehensive,
- cross-cutting general principles and common requirements for trust services, and
- considered international mutual recognition and international equivalences

Thank you！
ありがとうございました

<Acknowledgments>
The project cited in this document was implemented by the Council for Science, Technology and Innovation (CSTI), Cabinet Office, Government of Japan, through the "SIP/Big Data and AI-based Cyberspace Infrastructure Technology" (managed by the New Energy and Industrial Technology Development Organization (NEDO)).

＜謝辞＞
本資料で引用したプロジェクトは、内閣府総合科学技術・イノベーション会議の「SIP/ビッグデータ・AIを活用したサイバー空間基盤技術」（管理法人：国立研究開発法人新エネルギー・産業技術総合開発機構）によって実施されました。