

# Progress of SIP project and Japanese Trust framework

Speaker: Soshi Hamaguchi, VP @ Cosmos Corporation

Cooperated with;

Secom Trust Systems Co., Ltd

# Progress of SIP project

# Background and Scope

Japanese Cabinet approved the "Integrated Innovation Strategy 2020".

The pilot project between Japan and Europe has been decided to be launched for the establishment of mutual recognition of trust services in that strategy

## PROJECT TASKS

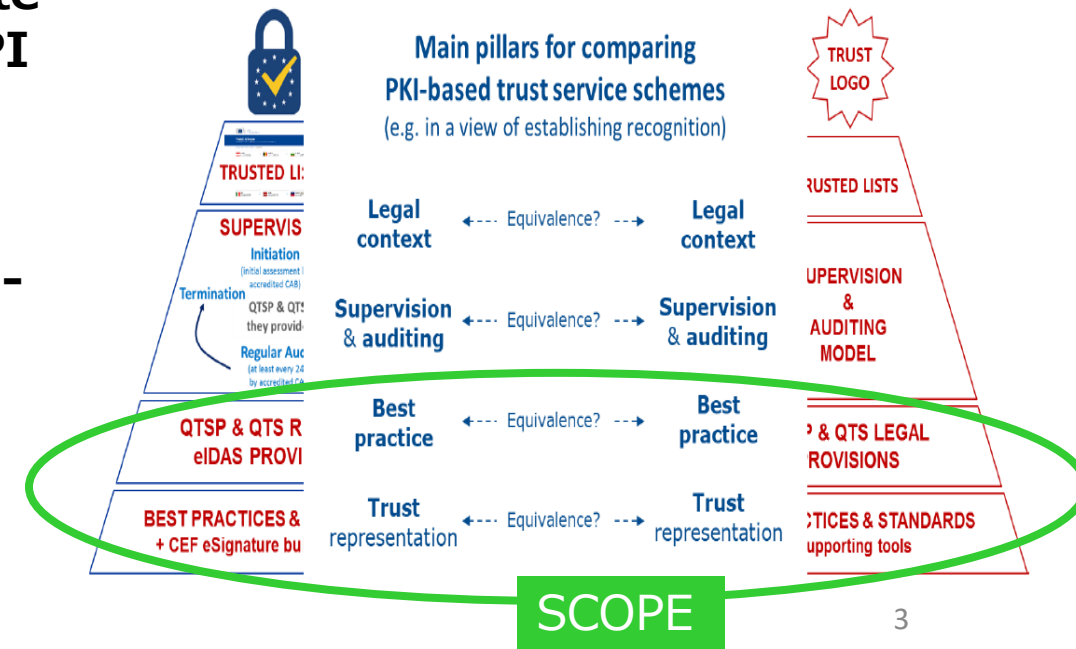
1. Confirmation of the equivalence of technical standards
2. Test implementations of Japan Trusted list
3. The validation of digital signatures in Japan and Europe using the Trusted List
4. Technical demonstration of interoperability between Japan and Europe trust services

(1) Extent of CSC\* API standard to enable certificate issuing from multiple CAs (key management API which is conforming to ETSI 119 431-1) and validation.

\* CSC : Cloud signature Consortium

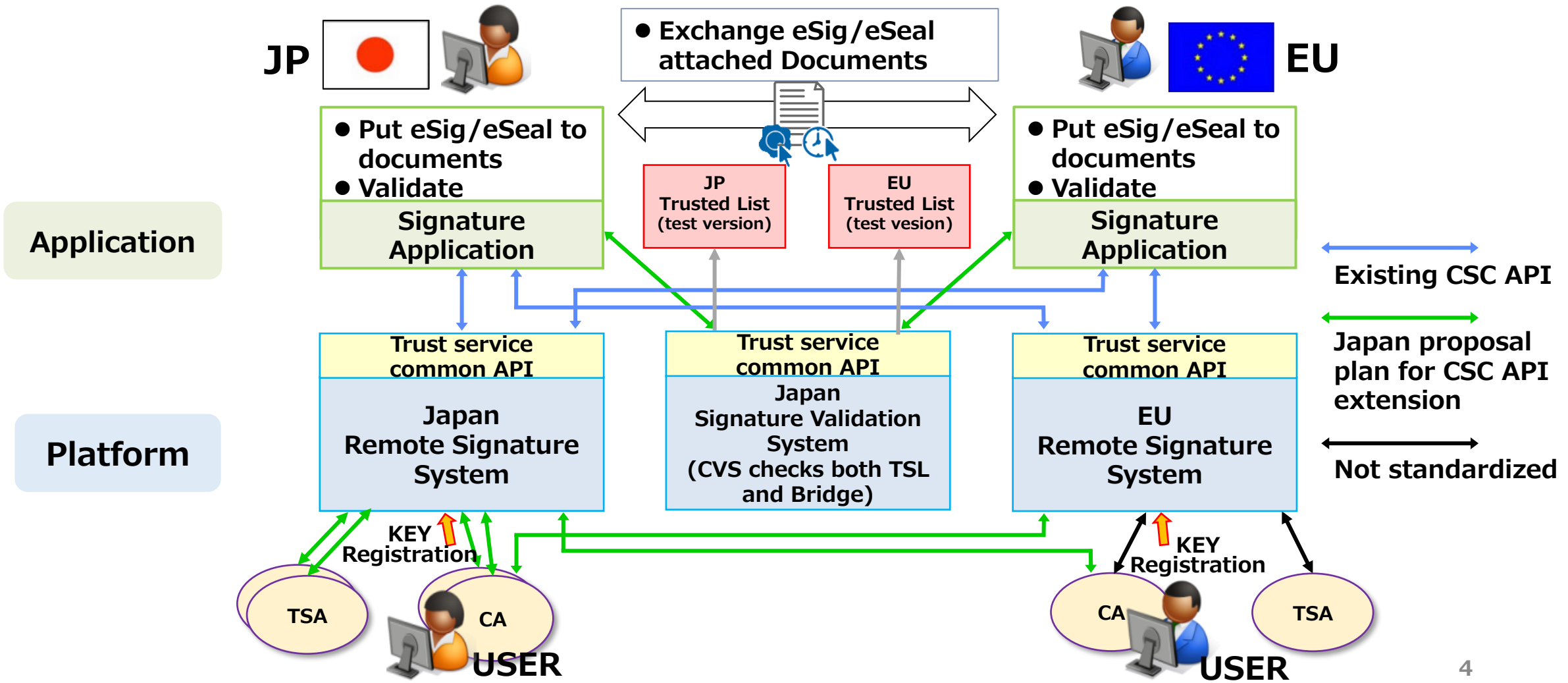
(2) demonstration of the interoperability for Japan-EU trust services by using a remote signature system that implements this API .

Note: Bridge model is adopted in Japan currently and used for validation of domestic Trust services.



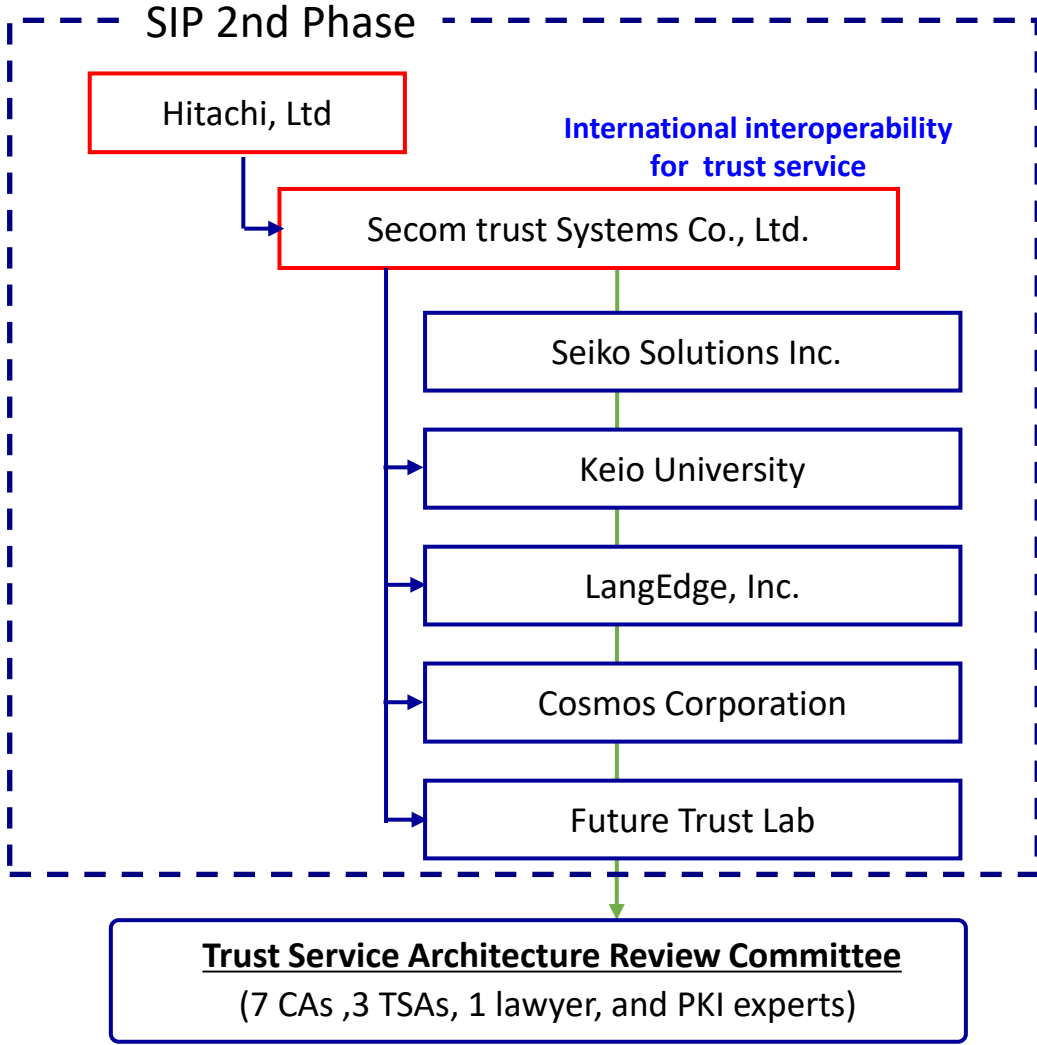
# JP-EU pilot project for interoperability of electronic signature

The project started on last October as 3rd year project with major Japanese TSPs . the actual demonstration will run in 2022 with EU cooperation.

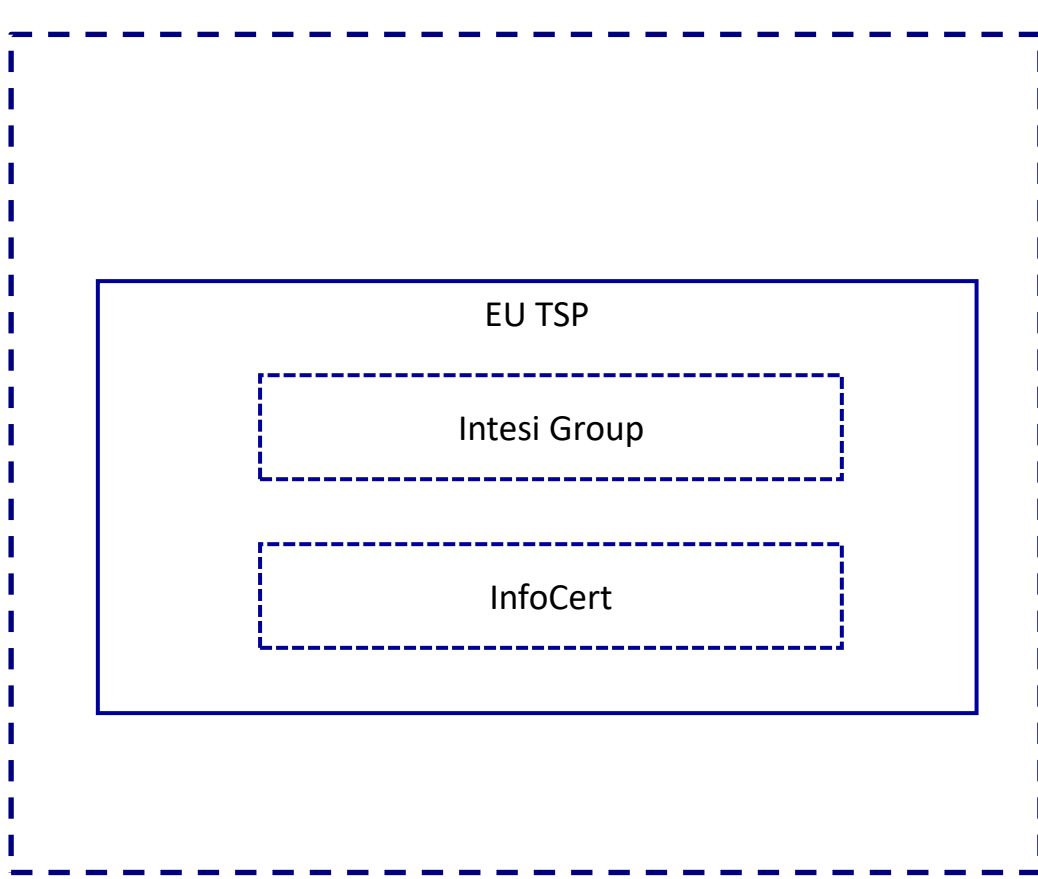


# SIP Trust Team Framework

## JAPAN SIDE



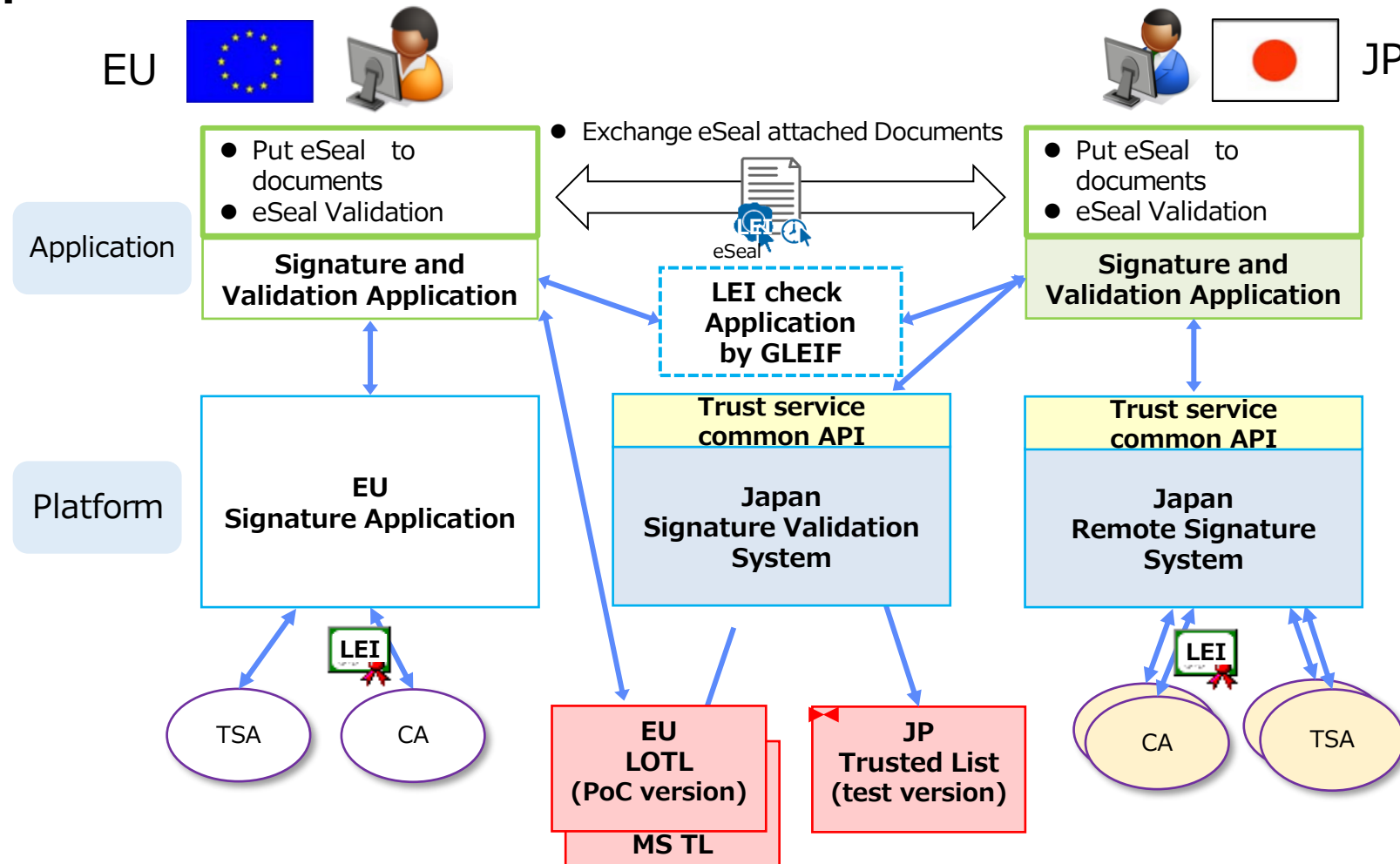
## EU SIDE ( Assumption)



# GLEIF PoC, Demonstration for cross-validation of e-Seal

## ● PoC in 2021:

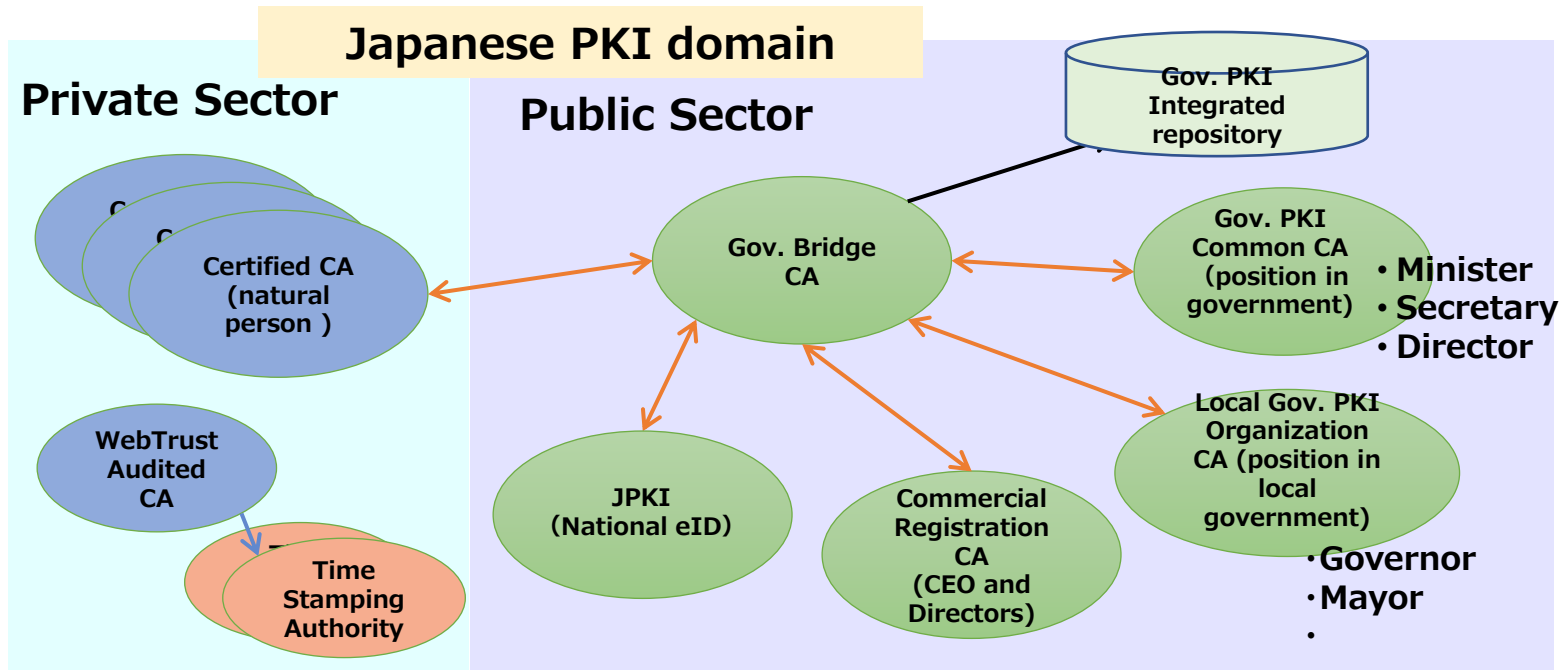
The cross-validation of eSeal with contain LEI was Demonstrated in 2021 with GLEIF. To validate Japanese TSP, the PoC version of JP TL and EU LOTL which has links to JP TL were prepared. Both the EU side and Japan's side successfully could validate eSeal each other.



# Japan Trusted List (test implementation only for PoC)

Scheme information will be Tentative.  
URI will be a test site.

TSP and TS are real.



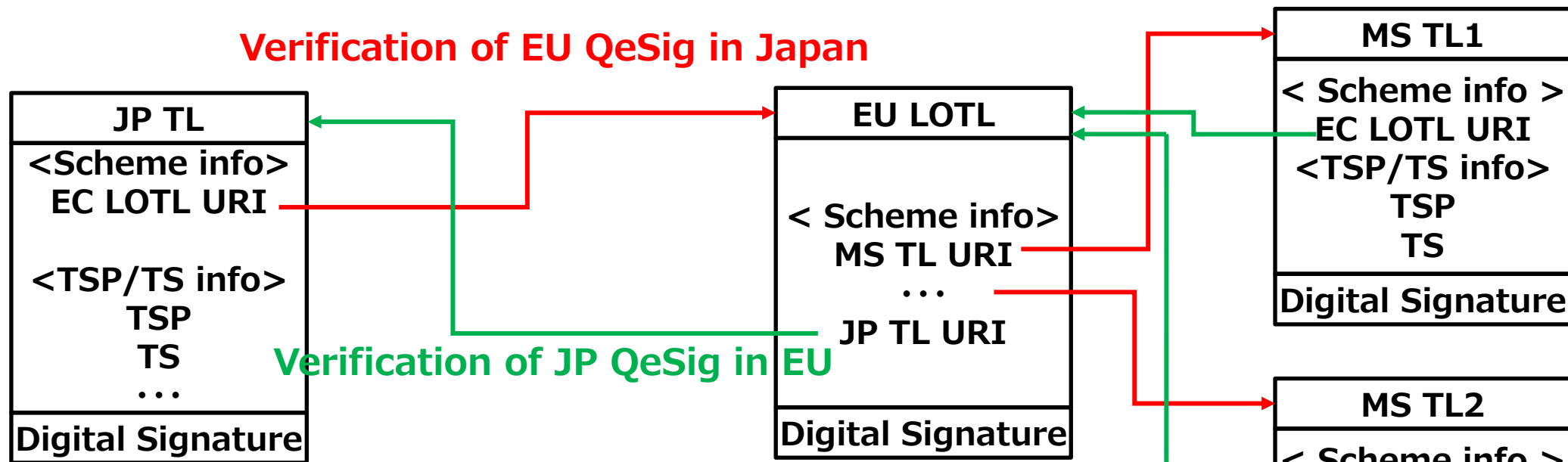
QcStatement will be Tentative.

Digital signature of Scheme operator will be Tentative.

Tag	TSL tag (clause 5.2.1)
	<b>Scheme information</b> TSL version identifier (clause 5.3.1) TSL sequence number (clause 5.3.2) TSL type (clause 5.3.3) Scheme operator name (clause 5.3.4) Scheme operator address (clause 5.3.5) Scheme name (clause 5.3.6) Scheme information URI (clause 5.3.7) Status determination approach (clause 5.3.8) Scheme type/community/rules (clause 5.3.9) Scheme territory (clause 5.3.10) TSL policy/legal notice (clause 5.3.11) Historical information period (clause 5.3.12) Pointers to other TSLs (clause 5.3.13) List issue date and time (clause 5.3.14) Next update (clause 5.3.15) Distribution points (clause 5.3.16) Scheme extensions (clause 5.3.17)
Signed TSL	<b>TSP1 information</b> TSP name (clause 5.4.1) TSP trade name (clause 5.4.2) TSP address (clause 5.4.3) TSP information URI (clause 5.4.4) TSP information extensions (clause 5.4.5)
	<b>Service information (clause 5.5)</b> Service type identifier (clause 5.5.1) Service name (clause 5.5.2) Service digital identity (clause 5.5.3) Service current status (clause 5.5.4) Current status starting date and time (clause 5.5.5) Scheme service definition URI (clause 5.5.6) Service supply points (clause 5.5.7) Service service definition URI (clause 5.5.8) Service information extensions (clause 5.5.9)
	<b>List of services</b>
	<b>Service approval history</b>
	<b>History information (clause 5.6)</b> Service type identifier (clause 5.6.1) Service name (clause 5.6.2) Service digital identity (clause 5.6.3) Service previous status (clause 5.6.4) Previous status starting date and time (clause 5.6.5) Service information extensions (clause 5.6.6)
	<b>TSP1 Service 1 History 2</b> Idem for TSP 1 Service 1 History 2 (prior to history 1)
	<b>TSP1 Service 2</b> Idem for TSP 1 Service 2 (as applicable)
	<b>TSP1 Service 2 History 1</b> Idem for TSP 1 Service 2 History 1
	<b>TSP2 information</b> Idem for TSP 2 (as applicable)
	Idem for TSP 2 Service 1 Idem for TSP 2 Service 1 History 1
<b>Digital Signature</b> Digital signature algorithm identifier (clause 5.7.2) Digital signature value (clause 5.7.3)	

# International Cross-reference of trust anchors

In the SIP project, Both the test version of the Japanese Trusted List and EU LOTL have been developed. the Test version of JP TL and EU LOTL includes reference points for each other to enable interconnection between trust anchors.



JP TL can be used independently to validate Japanese QeSig domestically.

TL: Trusted List  
LOTL: List of Trusted List  
MS: Member State  
TSP: Trust Service Provider  
TS: Trust Service

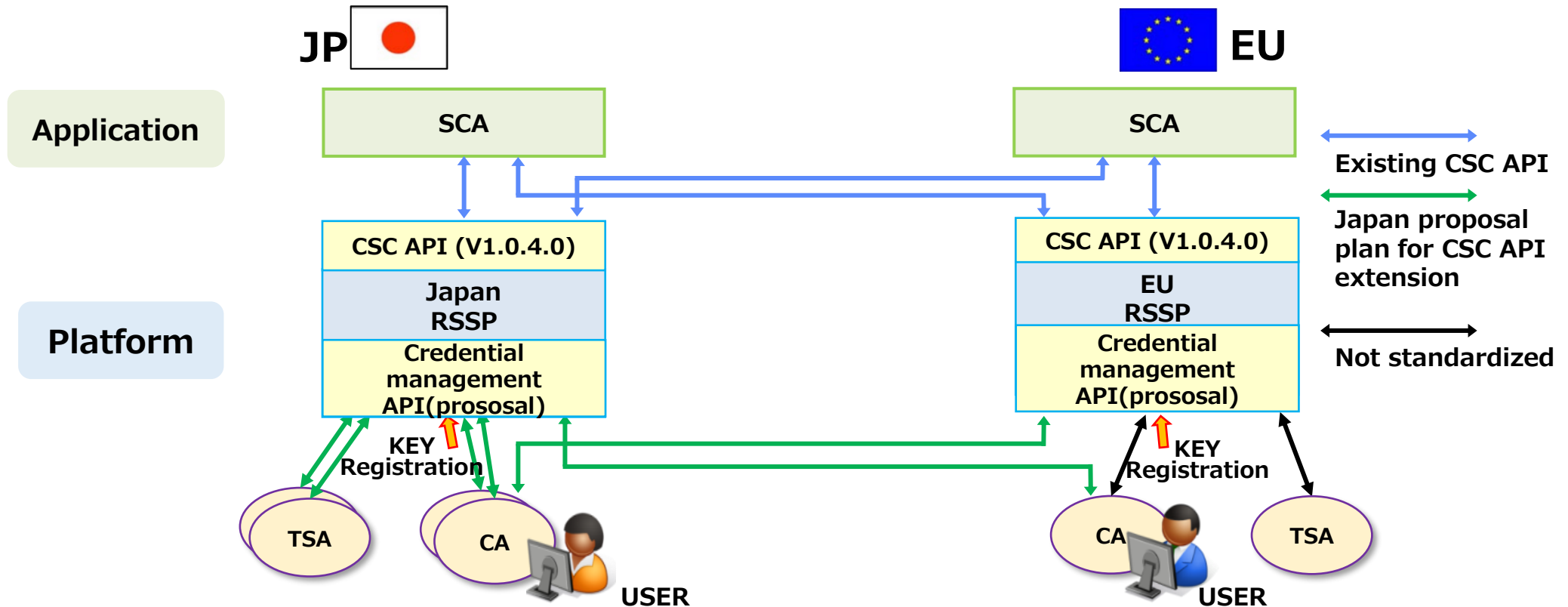


# PoC 2022: Interoperability of trust service

## ● PoC in 2022:

The SIP project has a plan to demonstrate the interoperability of QeSig and QeSeal by using a Remote signature system between EU TSP and JP TSP in 2022. The project needs EU TSP volunteers to perform the following two parts.

- A) Interoperability between RSSP and Signature Creation Application (SCA)
- B) Interoperability between RSSP and CA



# PoC 2022: Interoperability of trust service

We assume each TSP will have the following role in each demonstration.

We are very appreciative if EU TSP joins in this PoC.

A) Interoperability between RSSP and CA

B) Interoperability between RSSP and Signature Creation Application (SCA)

		SCA	RSSP	CA
First priority	A) -1	SECOM	SECOM	EU TSP
	A) -2	EU-TSP	SECOM	EU TSP
	B) -1	SECOM	EU TSP	EU TSP
	B) -2	EU TSP	SECOM	SECOM

We would like to do at least one of them.

# Schedule

	Tasks	Subject	2022			2023		
			Oct.	Nov.	Dec.	Jan.	Feb.	Mar.
	Decision of participation	EU TSP	→					
A	Share the detail of the Credential management API	SECOM/ EU TSP		↔				
	Preparation of the CA(RA) software with new API	EU TSP		↔				
	Preparation of the RSSP system for EU CA	SECOM		↔				
	Actual demonstration	SECOM/ EU TSP				↔		
	Reporting	SECOM					↔	
B	Preparation of the SCA software with CSC API	SECOM/ EU TSP		↔				
	Preparation of the RSSP software with CSC API	SECOM/ EU TSP		↔				
	Actual demonstration	SECOM/ EU TSP				↔		
	Reporting	SECOM					↔	

# Thank You

This work was supported by Council for Science, Technology and Innovation, “Cross-ministerial Strategic Innovation Promotion Program (SIP), Big-data and AI-enabled Cyberspace Technologies” .  
(funding agency: NEDO(New Energy and Industrial Technology Development Organization))

## Japanese Trust framework

- Introducing report from SWG for Trust Assured DX -

# Introducing report from SWG for Trust Assured DX

- The Sub-working Group for Trust-Assured Digital Transformation (DX)
  - Established under the Data Strategy Promotion Working Group on October 2021.
  - Total 11 sessions by July 2022
    - Identifying needs and challenges
    - Discussion of Trust service based on surveys
    - Required Actions
- Report of the Sub-working Group for Trust-Assured Digital Transformation  
[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/0f321c23-517f-439e-9076-5804f0a24b59/3b9ab650/20220729\\_meeting\\_trust\\_dx\\_report\\_en\\_01.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/0f321c23-517f-439e-9076-5804f0a24b59/3b9ab650/20220729_meeting_trust_dx_report_en_01.pdf)

# Identifying needs and challenges

- Needs of Trust services are identified in the below industry/fields
  - government, finance/insurance, telecommunications, real estate, medicine/welfare, and transportation/postal services.
- Challenges identified
  - Difficulty of service selection
  - Lack of recognition
  - Difficulty of aligning actions between companies
  - Limited Digitalization in G to C, G to B.

# Surveys on the needs

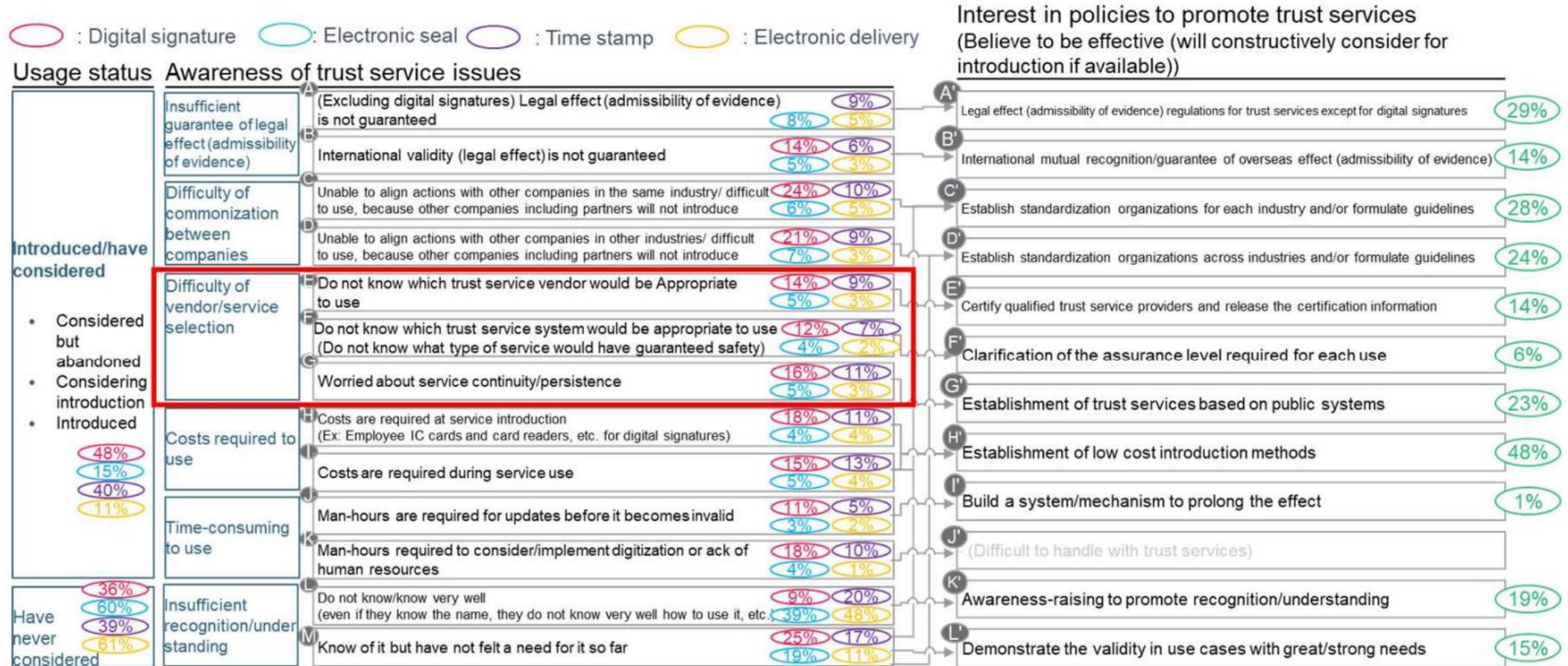
Procedural classification	BtoB, BtoC, BtoB/C	BtoG/GtoB, GtoC/CtoG, GtoB/C	Major industries/fields with many related people in which trust has been introduced in advance even overseas						Other
			Administrative	Private sector	Telecommunications	Real estate	Medicine, welfare	Transportation, postal	Agriculture/forestry/fishery industries, mining, construction, manufacturing, electricity/gas, etc., wholesale/retail, lodging/restaurants, etc.
Large corporate needs		Large individual needs	Family register notification, resident card acquisition, acquisition of copy or abstract of family register, voting, insurance fee account transfer application for employees' pension insurance	Bank account opening, securities account opening, Conclusion of insurance agreements, remittance, international remittance	Mobile telephone/smartphone agreement, rental/sharing service registration/usage, services and other registration/usage that require age verification		Telemedicine, medical interviews, PHR		
Applications/procedures, etc. that require strict identity verification			Resident card related applications, driver's license, international driver's license, guardianship registration and other applications, passport, residence card, vaccine passport, car storage location badge	Issuance of insurance policy document	Customer information linking for marketing	Internal sales information reporting	Issuance of medical exam/test results, medical certificate, medicine prescription, medical record creation/storage, linking of patient information between medical institutions,	Issuance of student commuter pass, mobility ID (vehicle data acquisition)	Smart grid (smart meter data acquisition)
Applications/deliveries/information transfers which require content tamper-resistance/authenticity			Tax returns, automobile procedures, subsidies and other requests, pension procedures, health insurance procedures, labor procedures, Labor Standards Act notifications (Article 36, etc.)	Financing/loan agreements, trade financing, currency trading	Net connection agreements, pay-TV agreements	Real estate sale/rental agreements	Creation, saving, and transfer of clinical trial data	International distribution procedures (customs clearance, etc.)	
Creation, transfer, and saving of documents/records, etc. which require legal admissibility of evidence				External company transactions	expense settlement, exchange of purchase order and acceptance of order, exchange of agreements, invoice transfer, product and other traceability guarantees				
				Internal company records	creation/saving of account books, creation/saving of decision-making records (internal memos, Board of Directors meetings, shareholders meetings resolutions, etc.), internal memos, approvals...				
				Regulatory compliance	creation/saving of ledgers, account books, records, etc. stipulated by other laws, etc. (pharmaceutical product/medical device ledgers, identity verification records for foreign currency exchanges, etc.)				

Source: Individual/company questionnaire surveys

Figure 3 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency



# Challenges identified



Note: Each percentage is the ratio with respect to all respondents (N = 347). The total for those who "have introduced/have considered" and "have never considered" excludes the "do not know" results, so it does not reach a 100% total. Arrows are written in locations which are not based on a clear analysis result but are believed to have a deep relationship.  
Source: BCG analysis from company questionnaire surveys

Figure 6 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Digitalization in administrative process

While digitization is making progress in applications, etc. from the private sector to the government (approx. 70%), progress is limited (approx. less than 20%) in other areas which consist primarily of disciplinary notification/delivery, etc. from the government to the private sector

Delays in the online systematization of disciplinary notification/delivery, etc. from the government to the private sector

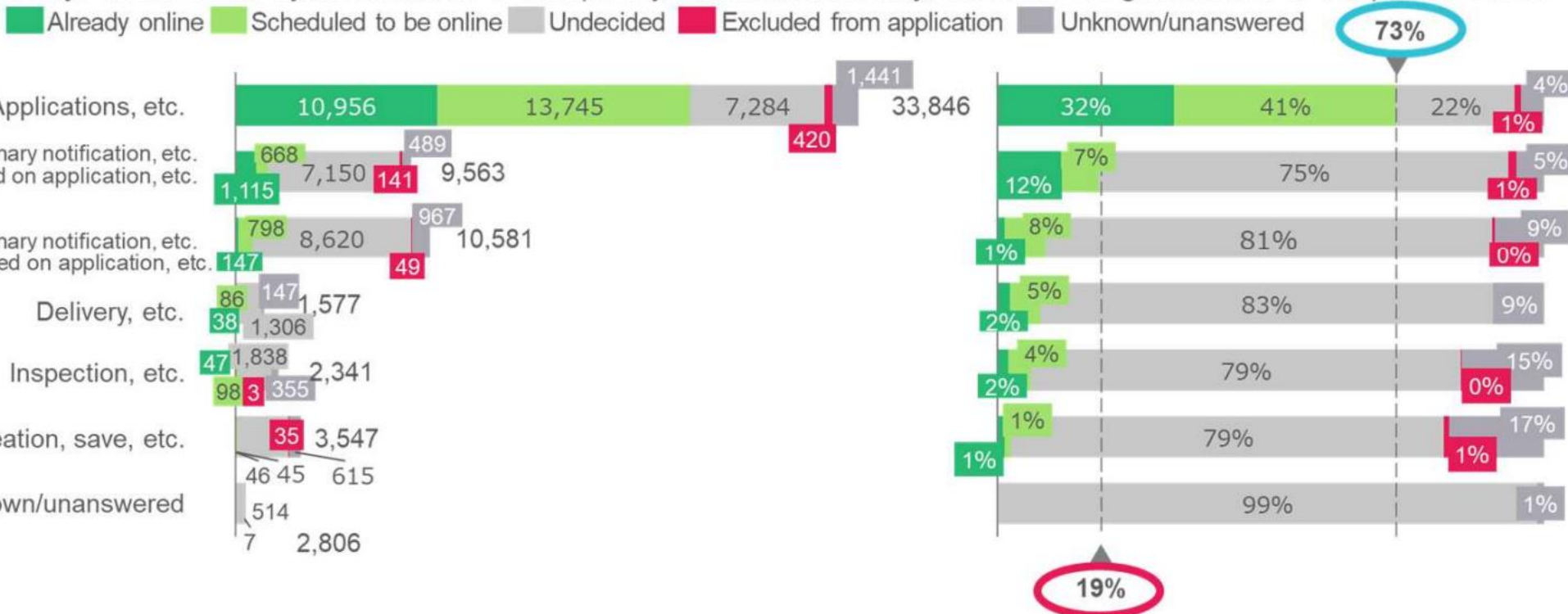


Figure 7 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Discussion of Trust Service

- Assurance level for Trust
  - Smooth service selection
- Promotion of the utilization of trust services in administrative procedures
  - Review of “regulations requiring face2face meetings and paper documentation”
    - Trust services is effective for “Digital Completion”
- Promotion in private sector
  - Trust service policies discussed by Multi Stakeholder Model
- Trust Policy
  - basic ideas for the framework assuring trust
  - Key principles of the policy were agreed

# Assurance level for Trust

- Organization of IAL and AAL
  - Mapping use cases in Japan to assurance levels (eIDAS, NIST SP800-63-3 and NZ government standards)

IAL	Identifier	Identity verification method	Use case
IAL-3	Item that can be electronically identified through a trustworthy institution	Verified face-to-face	Face-to-face application using an Individual Number Card
		Non-face-to-face	Digital signature using an Individual Number Card
		Verified face-to-face by a qualified person	
IAL-3	Item that is assured by the issuer and can be identified	Face-to-face equivalent online (eKYC)	Online matching of an individual's identification card photo and a real time image of the person
		⋮	⋮
?	Item that is assured by the issuer and can be identified	Verify face-to-face after online registration	Open a bank account online -> identity verification at card pickup
IAL-2	Item that can be electronically identified through a trustworthy institution	Verified without face-to-face contact	Open an account online using an Individual Number Card reader
	Item that is guaranteed by the issuer and can be identified	Verified without face-to-face contact	Online EC site member registration using identity verification documents (image upload, etc.)
IAL-1	Can be self-asserted with no identity verification	No identity verification	Confirm notification at an email address during service registration

Figure 9 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Assurance level for Trust

	Authentication process	Use case
AAL-3	In addition to AAL2, the use of a certified hardware-based authenticator with resistance to impersonation is essential.	Mynportal: log in via user authentication using an electronic certificate for verifying the user of an Individual Number Card e-Tax: Declaration through the use of an IC card based remote signature Business banking: remittance of large sums of money by two factor
AAL-2	The use of multifactor authentication and certified encryption methods is essential. The use of an authenticator with resistance to impersonation is recommended.	e-Tax: Declaration through the use of a Smart-ID based remote signature Internet broker: change the transfer destination bank using one-time password authentication based on a certified encryption method using the user name, password, and software token
	⋮	⋮
AAL-1	Single factor authentication	Internet broker: log in via user name and password Business chat service: send a link to an AAL-1 email address and user authentication based on following that link
AAL-0	No authentication	E-commerce: maintain a new customer cart through a new cookie

Figure 10 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Assurance level for Trust

Factors relating to Assurance level for Trust are discussed.

- Role of the State
  - Developing standards
    - Referencing international standards by provisions
  - Legislation
    - Legal value of Trust services are “Presumption” and presumed fact may be denied by contrary evidence. 100% guarantee is not sought.
    - Common law vs Civil law, w/wo QSCD
- Technical specifications(standards)
  - To be same level with ETSI, CEN works, a massive amount of work required...
    - some ingenuity needed
- Relation with assurance level for Digital Identity
  - No dependency between IAL and Trust Service Assurance Level
- Audit requirements
  - Point in time audit + Operational Transparency (such as AI based monitoring)
  - Audit/Certification vs Assurance Level
- UX
  - The universality of electronic documents shall not be denied only for the reason that they are in an electronic format (no exception should be allowed)
  - Trust service should indicate its assurance level somehow

# Promotion of Trust services

## Public Sector

- Digital Completion
  - The government will play a central role in discussing the technology standards and utilization policies of trust services used in official certificates and will provide input aiming for June 2025

## Private Sector

- Followings will be discussed by MSM
  - Technical specification for Remote signature and eSeal
  - Hearing of opinions regarding trust services in which public institutions are involved

# Multi Stakeholder Model

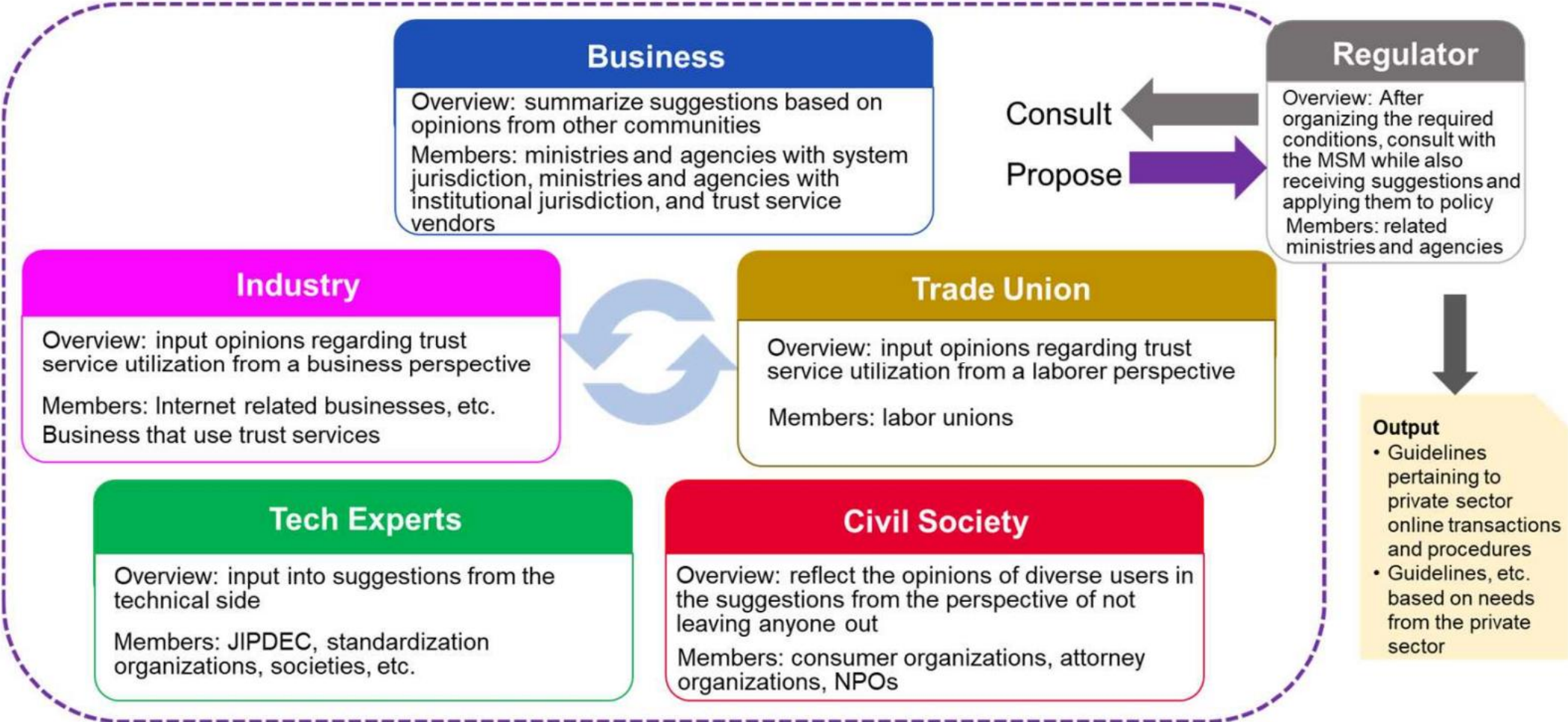


Figure 13 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency



# Key Principles of Trust Policy

Layer 7 Create new value	Basic principles for the formation of a digital society: (1) Open and transparent, (2) Fair and ethical, (3) Safe and secure, (4) Continuous, stable, and robust, (5) Solve social issues, (6) Rapid and flexible, (7) Inclusive and diverse, (8) Widespread, (9) Create new value, (10) Advance, international contribution)
<b>Digital principles</b>	
Layer 6 Operational reforms, BPR/organization	<b>Principle (1)</b> <b>Digital completion and automation principal</b>
Layer 5 Rules	<b>Principle (2)</b> <b>Agile governance principal</b> (agile and flexible governance)
Layer 4 Utilization environment	<b>Principle (3)</b> <b>Public-private partnership principal</b> (G to B to C model)
Layer 3 Collaboration platform	<b>Principle (4)</b> <b>Interoperability insurance principal</b>
Layer 2 Data	<b>Principle (5)</b> <b>Common foundation usage principle</b>
Layer 1 Infrastructure	

**Key Principles of trust policy**

- Ensure the long-term validity of trust services and social validity (**Stability**) to contribute to digital completion
- Ensure the implementation of trust services tailored to the category of procedure (**Consistency**)
- Develop the minimum legal infrastructure and respond through interpretation and operation (**Agility**)
- Ensure technical agility (**Flexibility**)
- Thoroughly implement EBPM based on data (**Transparency**) to ensure trust as well as agile and continuous revisions
- Ensure trust services that are easy to use from a user perspective (**User-friendliness**)
- Suggest a vision and ensure incentive design for users and providers to promote public-private partnerships (**Set a vision**)
- Introduce competitive market principle, and ensure a perspective that respects and utilizes private sector ingenuity (**Competitiveness**)
- Ensure international coordination in anticipation of international standards institutions discussions and various overseas systemic trends and state of use (**Interoperability**)
- Include ensuring trust through new technologies associated with technology innovation (**Technical neutrality**)
- Prepare a common foundation through public-private partnerships

Figure 14 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Action Required

- The government takes the lead in promoting the use of trust services in digital completion.
- Operation of MSM
- Trust framework for eSeal
  - Guidelines Pertaining to Electronic Seals announced by MIC
  - Technical specifications and conformity assessment framework will be discussed
- Promote internationally harmonized rule-making

# Plan


Period	Details to be studied	Study approach
Short-term	<ul style="list-style-type: none"> <li>• Promote the utilization of trust services for “digital completion”               <ul style="list-style-type: none"> <li>• Identity verification guidelines within administrative procedures</li> <li>• Authenticity guidelines within administrative procedures (tentative name) (Trust service technology standards and utilization policies used in official certificates)</li> </ul> </li> <li>• JPKI (study the next Identification Number Card)</li> <li>• Trust services operated in which public institutions are involved</li> </ul>	<p>Discuss at the Digital Agency based on the opinions of diverse stakeholders</p>
	<ul style="list-style-type: none"> <li>• Explore the issues in private sector online transactions and procedures</li> <li>• Address remote signatures and electronic seals, etc. based on the Act on Electronic Signatures and Certification Business and Explore updating of technology standards</li> </ul>	<p> Digital Agency to provide a place for discussion</p>
Medium to long-term	<ul style="list-style-type: none"> <li>• Explore DIW, etc. with international interoperability</li> <li>• Organize trust legal framework considering existing legal systems and international trends</li> <li>• Organize video and image data from drones and infrared sensors, instruments, time and other needs and issues pertaining to trust</li> </ul>	<p>Start by gathering information and research and study</p>

Figure 15 from Report of the Sub-working Group for Trust-Assured Digital Transformation, Digital Agency

# Thank you

- If you have questions, please contact [s.Hamaguchi@cosmos-corp.com](mailto:s.Hamaguchi@cosmos-corp.com).