For Japan Financial Service Agency,

Final Report of
JFSA Multilateral Joint Research on Digital Identity

Nomura Research Institute, Ltd.

NRI Secure Technologies, Inc.

31st, March 2021

Background and Purpose of the Research

Background

- Recently, as technological innovation develops, digitalization of financial services has rapidly increase and various financial services are provided via wide range of devices and digital platforms. To keep up with these trends, Japanese Financial Service Agency (“JFSA”) stipulated “Finance Digitalization Strategy” and actively engaging in data utilization and protection of consumer privacy, etc. in the financial sector.
- Digital Identity is one of indispensable elements for financial digitalization. Regardless of modes of service, financial service providers are required to properly handle identity information for consumer protection, anti-money laundering / combating the financing of terrorism (AML/CFT). Financial service providers are expected to build and operate digital identity systems compliant with appropriate frameworks so that they can provide individualized services according to each customers’ needs and circumstances based on understanding them appropriately and efficiently.
- It is important for JFSA to understand recent activities in technological developments and standardization. In addition, Self-Sovereign Identity / Decentralized Identity (SSI/DID) attracts a lot of attentions because of recent concerns for privacy protection on centrally controlled digital identity, developments of regulations on data protection, avoidance of rock-in, and financial inclusion.
- For development of SSI/DID, as some experts insist that decentralize architectures such as blockchain technologies would be suitable, such new trend have to be taken in account in advance.
- As such, JFSA needs to have a deep understanding on wide range of issues, such as technological elements of digital identity including authentication, access control, cryptography, and blockchain as well as operational and governance frameworks. JFSA also needs to set up dialogues with various stakeholders around digital identity.

Purpose

- Based on above background NRI will conduct this multilateral joint research focus on possible utilization of digital identity in the financial sector. This research will be an important input for JFSA, the financial regulator, to analyze digitalization of finance in the future and have a deep understanding on current digital identity systems, desirable digital identity systems and its operations.

Table of Contents

Acknowledgments and Disclaimer

■Acknowledgments

- While conducting this research, we received substantial contributions from following persons;
  - Mr. Nat Sakimura, Chairman of the Open ID Foundation;
  - Professor Kazue Sako, Waseda University;
  - Professor Shigeya Suzuki, Keio University; and
  - Professor Shin'ichiro Matsuo, Georgetown University.
  - We would like to extend our gratitude to the JFSA officials for their contributions to this research as partners.
- Please kindly note that only contractors of this research, Nomura Research Institute, Ltd. and NRI Secure Technologies, Inc. shall be responsible for possible errors contained in this report.

■Disclaimer

- This report does not necessarily reflect official views of the JFSA.
- Contents other than past or present facts written in this report are our prospects based on information available at the time this report written and can fluctuate according to variable factors.

Glossary (digital identity)

■ The following terms are mainly in accordance with the ISO/IEC 24760 series*1).

用語		定義
entity	・	item relevant for the purpose of operation of a domain that has recognizably distinct existence
identity	・	set of attributes related to an entity
attribute	・	characteristic or property of an entity
identifier	・	attribute or set of attributes that uniquely characterizes an identity in a domain
credential	・	representation of an identity for use in authentication
verification	・	process of establishing that identity information associated with a particular entity is correct
authentication	・	formalized process of verification that, if successful, results in an authenticated identity for an entity
identity management system: IMS	・	mechanism comprising of policies, procedures, technology and other resources for maintaining identity including associated metadata

*1)
ISO/IEC 24760-1:2019 A framework for identity management — Part 1: Terminology and concepts
ISO/IEC 24760-2:2015 A framework for identity management — Part 2: Reference architecture and requirements
ISO/IEC 24760-3:2016 A framework for identity management — Part 3: Practice

Glossary (AML/CFT)

■ The terminology used in this study is in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and related laws and regulations in Japan. Some terms used in overseas cases refer to overseas regulations.

terminology	Definition.
Suspicious Activity Report	• Financial institutions, etc. that fall under the category of specified business operators under "Act on Prevention of Transfer of Criminal Proceeds"[*2)] shall, with regard to transactions pertaining to the specified business, determine whether or not there is any suspicion that the property received in such transactions is related to crime, or whether or not there is any suspicion that customers, etc. are committing acts that constitute crimes under Article 10 of "Act on Punishment of Organized Crime and Control of Crime"[*3)] or crimes under Article 6 of "Narcotics and Psychotropics Control"[*4)] with regard to such transactions. In cases where such suspicion is detected, it is obliged to promptly report the matters specified by Cabinet Order pursuant to the provisions of Cabinet Order (Article 8, Paragraph 1 of "Act on Prevention of Transfer of Criminal Proceeds" and Article 16 of the Enforcement Order[*5)] of the same Act). （Reference: FATF Recommendation 20[*6)]) • If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).
Financial Inclusion [*7)]	• Individuals and businesses have access to useful and affordable financial products and services that meet their needs - transactions, payments, savings, credit and insurance - delivered in a responsible and sustainable way.

*1) Frequently Asked Questions (FAQ) on Anti-Money Laundering and Terrorist Financing Guidelines https://www.fsa.go.jp/news/r2/2021_amlcft_faq/2021_amlcft_guidelines_FAQ.pdf

*2) Act on Prevention of Transfer of Criminal Proceeds https://elaws.e-gov.go.jp/document?lawid=419AC0000000022

*3) Act on Punishment of Organized Crime and Control of Crime https://elaws.e-gov.go.jp/document?lawid=411AC0000000136

*4) Act Concerning Special Provisions for the Narcotics and Psychotropics Control Act, etc. and Other Activities Involving Controlled Substances through International Cooperation https://elaws.e-gov.go.jp/document?lawid=403AC0000000094

*5) Order for Enforcement of Act on Prevention of Transfer of Criminal Proceeds https://elaws.e-gov.go.jp/document?lawid=420CO0000000020

*6) The FATF Recommendations https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

*7) The World Bank Financial Inclusion https://www.worldbank.org/en/topic/financialinclusion

Glossary (AML/CFT)

terminology	Definition.
Onboarding due diligence	• When financial institutions, etc. conduct transactions with customers, they should appropriately investigate basic information about the customer, such as who the customer is, who is the ultimate beneficial owner of the organization, what is the purpose of the transaction, what is the flow of funds, and determine and implement mitigating measures.
Ongoing due diligence	• A series of processes to re-evaluate and determine customer risk and implement risk reduction measures by continuously updating customer information and verifying the details of transactions conducted by the relevant customers.
Ultimate Beneficial Owner*3)	• Those who are in charge of corporate management and who control the business management.
Customer Filtering*2)	• A method to reduce risk by preventing transactions by antisocial forces, etc., through checking the list of related parties and existing customers against the list of antisocial forces and sanctioned parties, etc., before transactions or when the list is updated. Include name screening operations.
Transaction Monitoring*2)	• A method to reduce risk by detecting, investigating, and judging abnormal transactions in comparison with past transaction patterns, and notifying suspicious transactions while reflecting them in the risk assessment of the relevant customer.
Risk-based approach*1)	• Financial institutions, etc. should identify and assess their own money laundering and terrorist financing risks and take appropriate measures in order to effectively reduce such risks based on their risk tolerance.

*1) Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism https://www.fsa.go.jp/common/law/amlcft/2021_amlcft_guidelines.pdf
*2) Frequently Asked Questions (FAQ) regarding the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism defined with reference to *1)
*3) Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds https://elaws.e-gov.go.jp/document?lawid=420M60000f5a001

Glossary (AML/CFT)

terminology	Definition.
AAL*1)	• Authentication Assurance Level: Robustness of the authentication process itself, and of the linkage between the authentication code and the identifier of a specific individual
AML/CFT*2)	• Anti-Money Laundering and Combating the Financing of Terrorism
eKYC*3)	• electric Know Your Customer: Verifying the identity of a customer online
IAL*1)	• Identity Assurance Level: Robustness of the identity proofing process to confidently determine an individual's identity
FATF*2)	• Financial Action Task Force
KYC*4)	• Know Your Customer: Verifying the identity of a customer
LEI*5)	• Legal Entity Identifier
LoA*6)	• Level of Assurance: The level of confidence in the identity of the individual received
NPI*5)	• Natural Persons Identifier

*1) NIST Special Publication 800-63-3 Digital Identity Guidelines
(Japanese) https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html (English) https://pages.nist.gov/800-63-3/sp800-63-3.html

*2) Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism
(Japanese) https://www.fsa.go.jp/common/law/amlcft/2021_amlcft_guidelines.pdf (English) https://www.fsa.go.jp/common/law/amlcft/en_amlcft_ guidelines.pdf

*3) Publication of "Order to Amend Part of the Enforcement Regulations of the Act on Prevention of Transfer of Criminal Proceeds"
https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html

*4) Guidance for banks on customer verification: https://www.fsa.go.jp/inter/bis/f-20011004-2.html

*5) Bank of Japan Payment and Settlement Systems Department ISO Panel (1st) https://www.boj.or.jp/paym/iso/iso_panel/data/isop201127.pdf

*6) eID Documentation https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+assurance

Chapter 1: Fundamentals of Digital Identity -Technologies and Operations-

1. Summary of the Chapter

Summary of the Chapter

1-1. Digital Identity and Identity Management Systems (IMS)

- An Identity is "the representation of a set of attributes related to an entity," and an Identity Management System (IMS) is needed as a mechanism to manage the constantly changing and growing state of identity. An IMS is a mechanism consisting of policies, procedures, technologies, and other resources to maintain identity information.
- A Digital Identity is "an electronic representation of a set of attributes related to an entity. In the past, many systems still handled the exchange of identity information between IMS in an analog style, using paper media, etc. However, with the use of digital identities, there is a movement toward digitizing this mutual exchange (e.g., linking identity evidence in a machine-readable format). (e.g., asserting identity evidence in a machine-readable format) (= digitization of IMS).

1-2. Main IMS Models and Components

- Currently, the main IMS models are the Centralized model and the Federation model, and technical standards for protocols related to provisioning management, authentication, authorization, and identity coordination have been established as technical elements to support these models.
- In addition, in order to properly operate IMS, it is important to design and operate IMS based on not only technical elements such as standard protocols, but also governance elements. For example, Europe has enacted legislation in the form of eIDAS regulations, and the US, UK, Canada, and other countries have developed governance frameworks (trust frameworks) for the appropriate design, development, operation, and use of digital identities. The use of digital identities in compliance with these regulations and frameworks is required.

1-3. Self-Sovereign Identity (SSI)

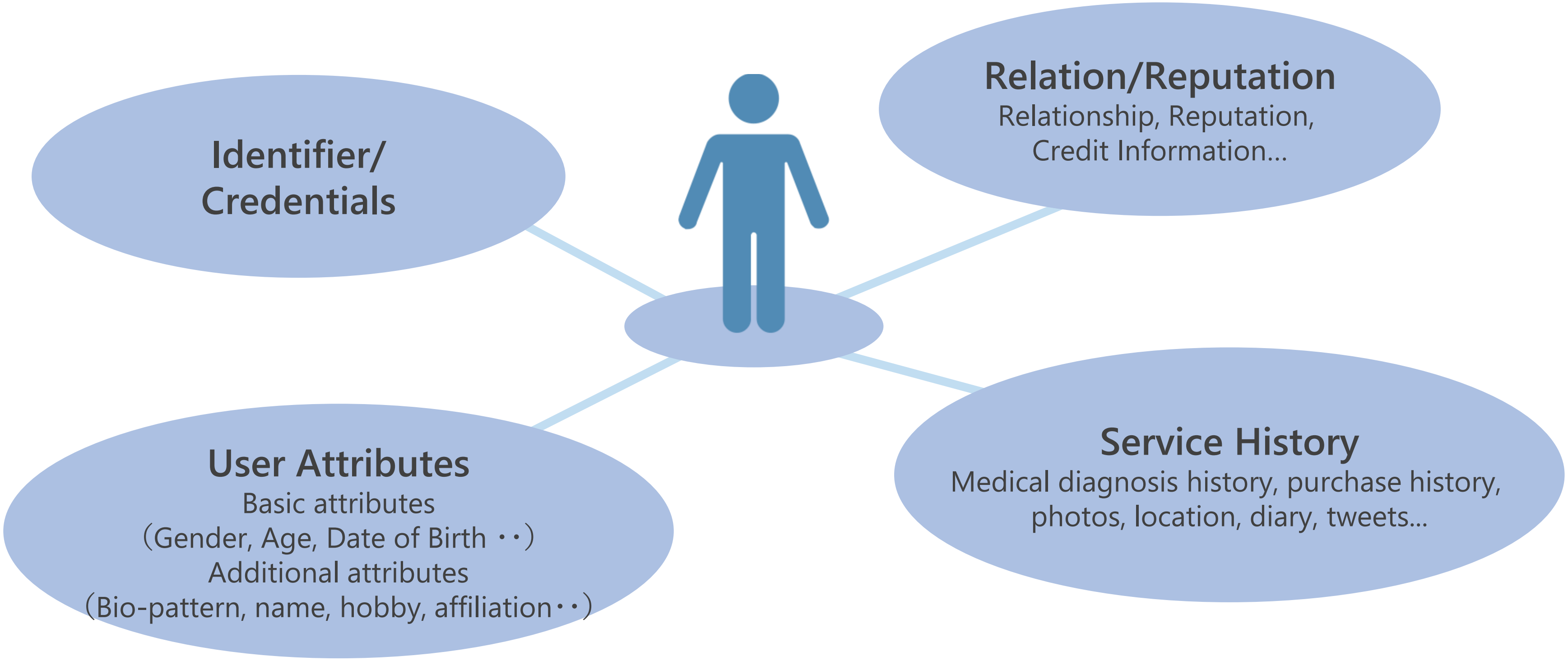
- Existing IMS models have been pointed out to have the risk of account suspension by (malicious) identity providers and the risk of identity tampering by (malicious) identity providers. To address these concerns, the Self-Sovereign Identity (SSI) and Decentralized Identity (DID) models have been proposed.
- The features presented by the SSI model, such as (1) Separation of Authentication and Attributes, (2) Selective Presentation of Claims, (3) Unlinkability, (4) Re-presentation and Verification of Obtained Claims, have the potential to resolve the concerns of existing models.

1-1. Digital Identity and Identity Management Systems (IMS)

What is Identity?

- "Identity" is **"a set of attributes related to an entity"** **(ISO/IEC 24760).** An entity is not only a person, but also an organization or a thing.
- For example, if the entity is a person, the "attributes" include the following information.

Examples of attributes included in a person's identity



Identifier/ Credentials

Relation/Reputation
Relationship, Reputation,
Credit Information...

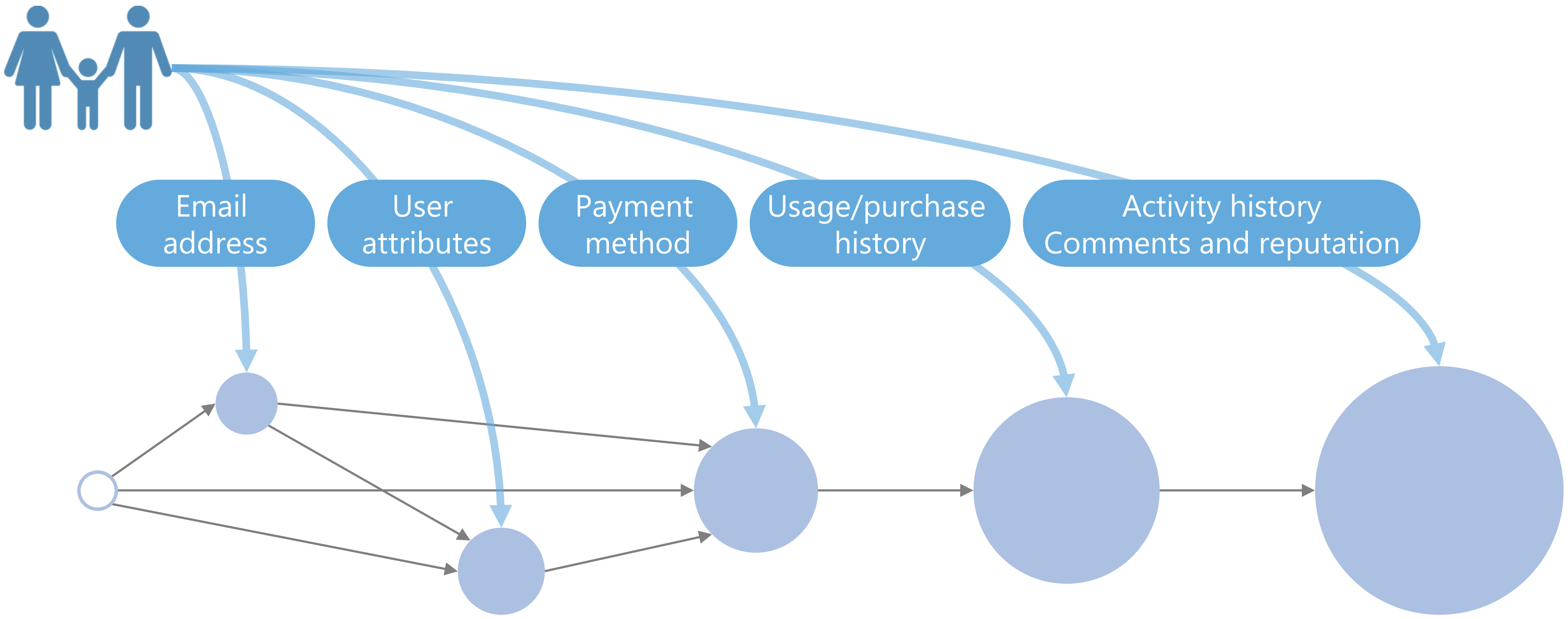
User Attributes
Basic attributes
（Gender, Age, Date of Birth ・・）
Additional attributes
（Bio-pattern, name, hobby, affiliation・・）

Service History
Medical diagnosis history, purchase history,
photos, location, diary, tweets...

Characteristics of Identity

- The attributes increase along with service use and relationships, therefore, **the identity is not a constant, but it is characterized by the fact that it changes and grows as the attributes increase and change.**

Examples of identity change and growth



1-1.Digital Identity and Identity Management Systems (IMS)

What is Digital Identity?

- "Digital identity" has been defined in various ways in various countries and institutions, but it is not globally standardized. Therefore, in this study, it is defined as "an electronic representation of a set of attributes related to an entity," in line with the definition of identity in ISO/IEC 24760.

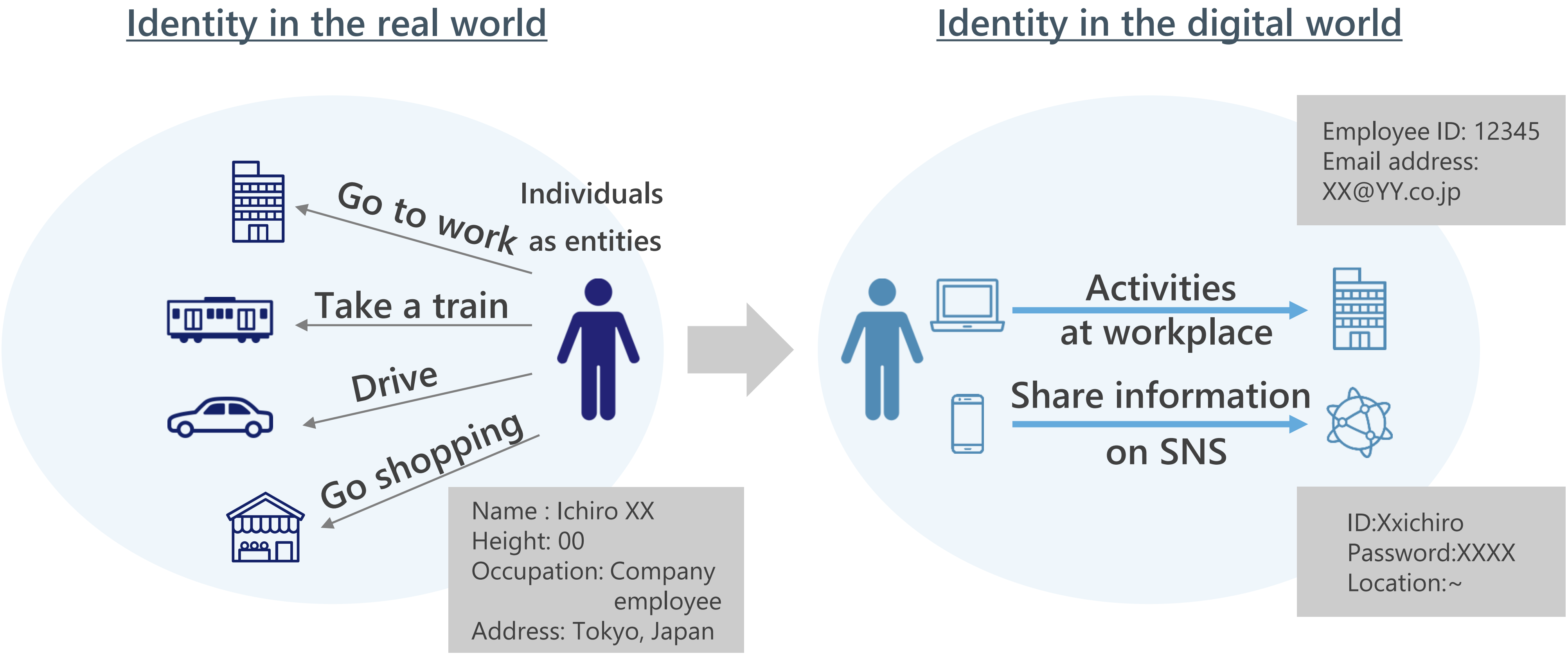
Examples of definitions of digital identity in major organizations

Organizations	Definition
U.S. Government	"Digital identity is the unique representation of a subject engaged in an online transaction." (U.S., "NIST SP 800-63 revision 3")
U.K. Government	"A digital identity is a digital representation of who you are." (U.K., "The UK digital identity and attributes trust framework")
Australian Government	"an electronic representation of an entity which enables that entity to be sufficiently distinguished when interacting online." (Australia, "The Trusted Digital Identity Framework")
ITU	"A digital representation of the information known about a resource, a specific individual, group or organization." (ITU, X.1252 "Baseline identity Management terms and definitions")
World Bank	"a set of electronically captured and stored attributes and credentials that can uniquely identify a person." (ID4D, "Technical Standards for Digital Identification Systems")

Source) Created by NRI based on each website.

Characteristics of Digital Identity

- By being able to easily digitize personal attributes in the real world, individuals can now use a variety of digital identities depending on the digital services they use.
- One of the characteristics of digital identities is that **they are easier to create and use than real-world identities** in comparison with real-world identities.



Name : Ichiro XX
Height: 00
Occupation: Company employee
Address: Tokyo, Japan

Employee ID: 12345
Email address:
XX@YY.co.jp

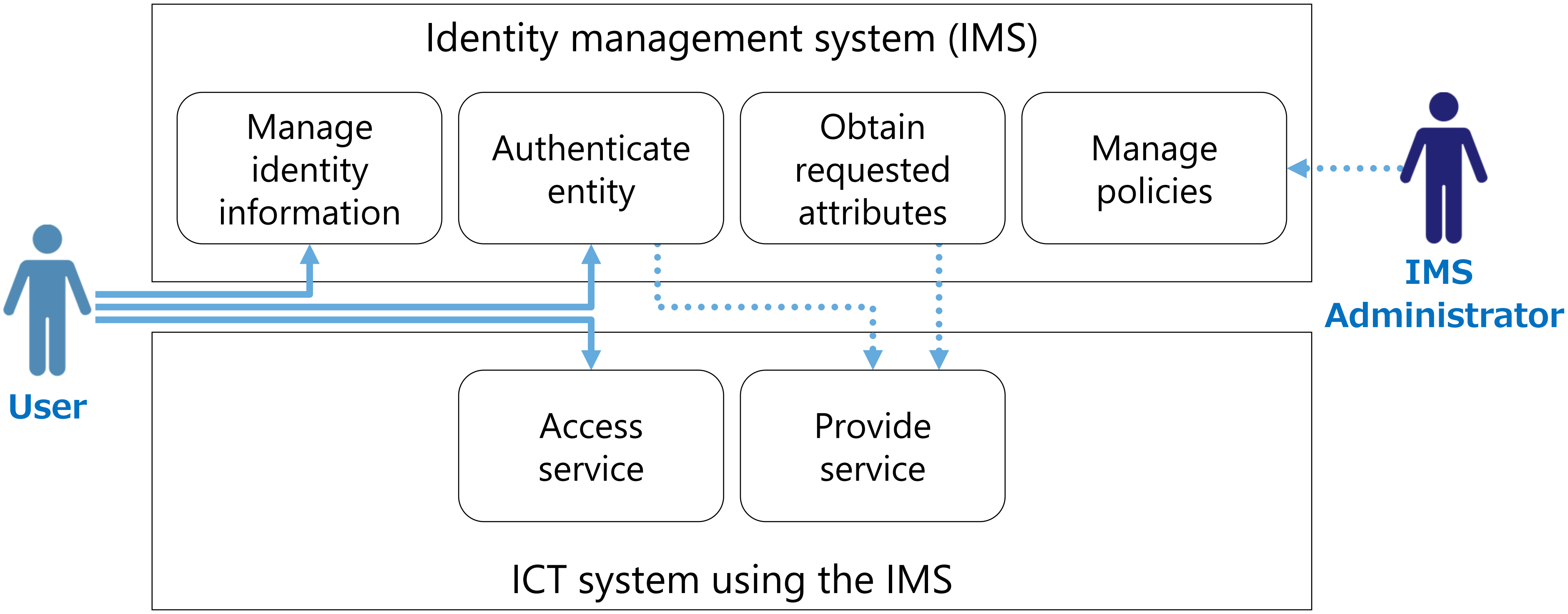
ID:Xxichiro
Password:XXXX
Location:~

Source) Created by NRI

What is Identity Management System (IMS)?

- Identities managed in ICT systems, etc., are managed as identity information. In order to properly manage identity information, a mechanism (i.e., Identity Management System: IMS) consisting of policies, procedures, technologies, and other resources is required to maintain identity information.
- The main roles of IMS are administrative activity (manage identity information, manage policies)and resource access activity(authentication and obtaining identity information)

The main mechanism of IMS



Source) Created by NRI based on ISO/IEC24760-2

1-1.Digital Identity and Identity Management Systems (IMS)

"Seven Laws of Identity”

- Kim Cameron, a former identity architect at Microsoft who has greatly influenced the thinking of the identity industry, has proposed the "Seven Laws of Identity” for digital identity in managing digital identities.
- It is important for IMS to design, develop, and operate based on these principles.

#	Principles	Contents
1	Law of User Control and Consent	• Identity systems must only reveal information identifying a user with the user's consent.
2	Law of Minimal Disclosure For A Constrained Use	• The identity system must disclose the least identifying information possible, as this is the most stable, long-term solution.
3	Justifiable Parties	• Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4	Directed Identity	• A universal identity system must support both "omni-directional" identifiers for use by public entities and "uni-directional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5	Pluralism of Operators and Technologies	• A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
6	Human Integration	• Identity systems must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
7	Consistent Experience Across Contexts	• The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

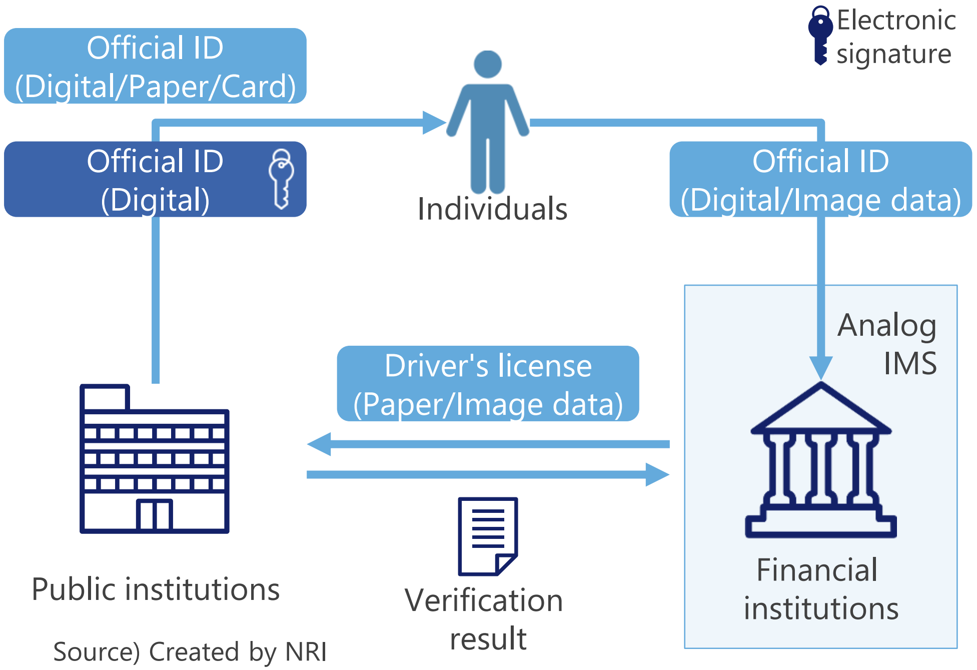
Source) Kim Cameron, “The Laws of Identity” https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Digitization of Identity Management

- For the exchange of identity information between IMS, it is still mostly handled in an analog way by many systems using paper or other media. (e.g., sending a paper copy of a driver's license by mail as a means of identity evidence assertion used for identity proofing)
- In this study, the digitization of identity management systems is considered as the digitization of such interactions. (e.g., assertion of identity evidence in machine-readable formats)

IMS in Analog (example)

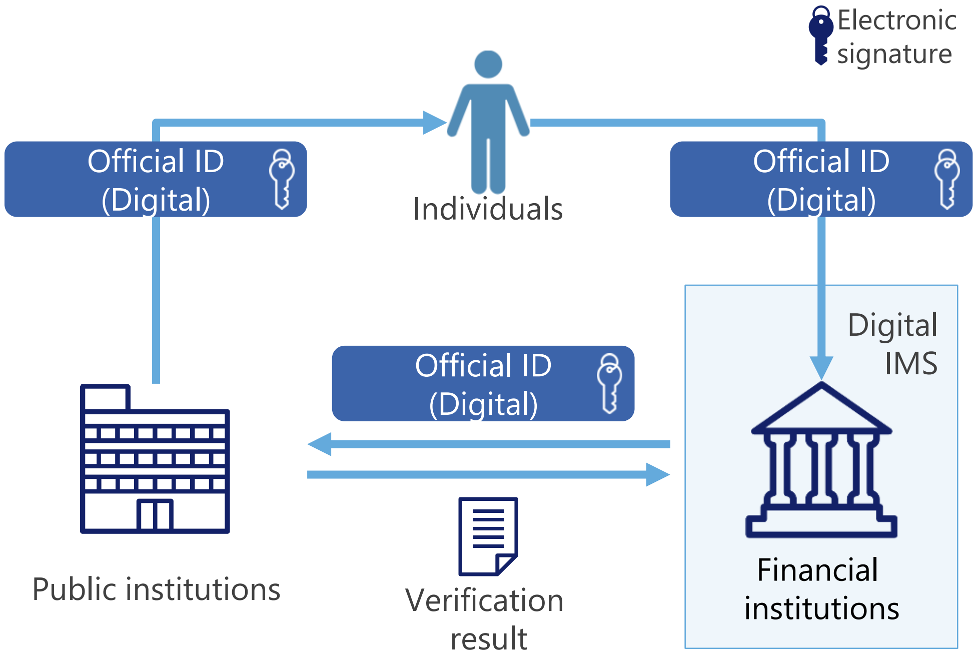
- When opening a new bank account at a financial institution, individuals submits a copy of their official ID (paper) to the financial institution as a form of identification.
- The financial institution verifies the identity based on the analog information.



Source) Created by NRI

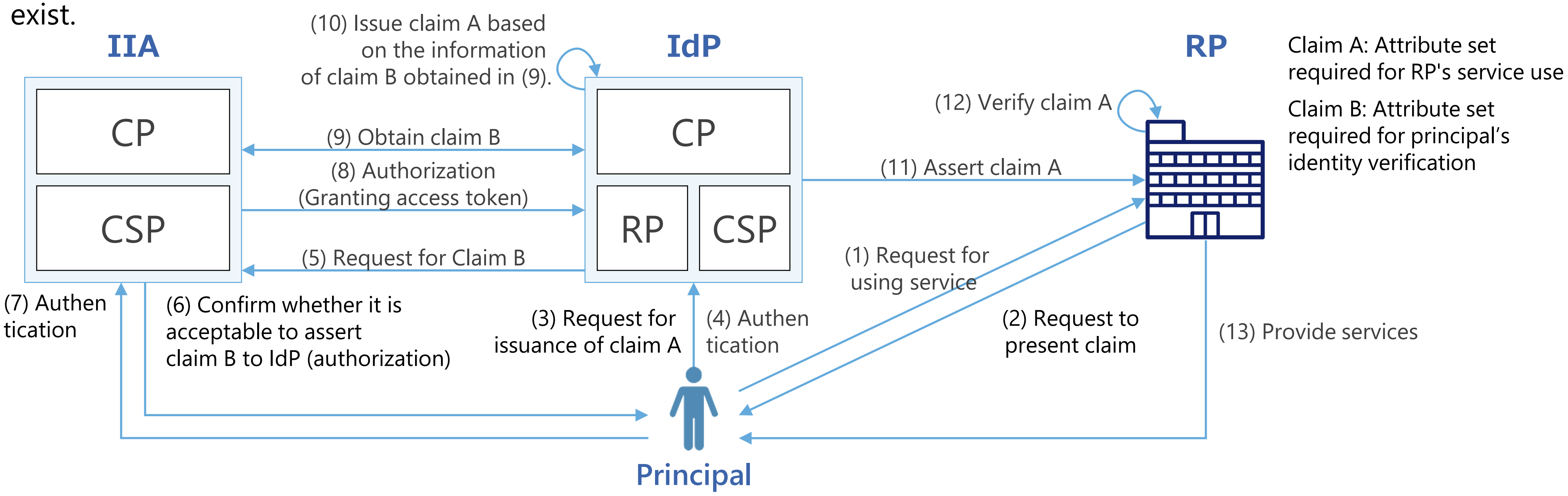
IMS in Digital (example)

- When opening a new bank account at a financial institution, the individual submits a copy of their official ID (digital) to the financial institution as a form of identification.
- The financial institution can verify the asserted official IDs in a machine-readable format.



Main Actors Constituting the IMS

- If taking as an example the time of assertion (= federation model) of claims (some attribute sets of entities that are identities) to a relying party, which is a service provider, as the main actors that constitute IMS, the following actors exist.


IIA
CP
CSP
IdP
CP
RP
CSP
RP
Principal
(10) Issue claim A based on the information of claim B obtained in (9).
(9) Obtain claim B
(8) Authorization (Granting access token)
(5) Request for Claim B
(7) Authen tication
(6) Confirm whether it is acceptable to assert claim B to IdP (authorization)
(3) Request for issuance of claim A
(4) Authen tication
(12) Verify claim A
(11) Assert claim A
(1) Request for using service
(2) Request to present claim
(13) Provide services

Claim A: Attribute set required for RP's service use

Claim B: Attribute set required for principal's identity verification

#	Actors (roles)	Definition
1	Principal	・ Entities that have identity information stored and managed by IMS
2	Identity information authority: IIA	・ Entity related to a particular domain that can make provable statements on the validity and/or correctness of one or more attribute values in an identity
3	Identity provider: IdP	・ Entity that provides available identity information and creates and maintains identity information; IIA may also act as an IdP ・ Also called an Identity information provider (IIP)
4	Credential service provider: CSP	・ Trusted entity that is responsible for managing credentials (a statement of identity used during authentication. For example, user IDs, passwords, etc.)
5	claims provider: CP	・ Entity that provides a claim
6	Relying party: RP	・ Entity that relies on the verification of identity information for a particular entity

Source) Created by NRI based on ISO/IEC24760-1, OpenID Connect Core 1.0

1-2. Main IMS Models and Components

Centralized Model and Third Party IdP/Federation Model

■ IAs for the models/schemes of IMS, the following are the two past/current representative models.

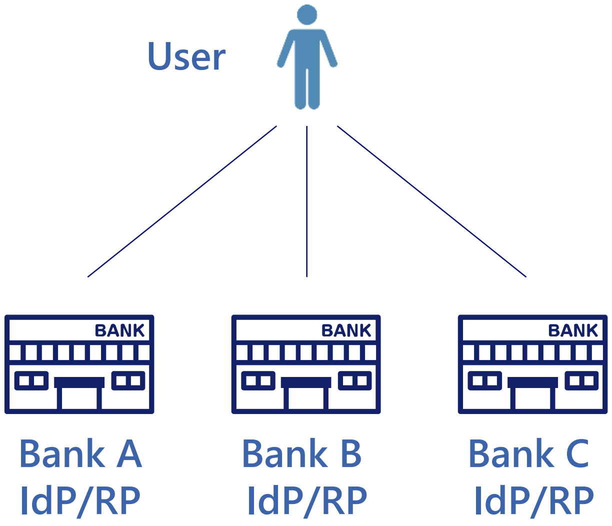
- **Centralized model**
  - The RP acts as the IdP and provides individual identity management and services. Users need to manage their identities for each service.

    Example: A user accesses the online banking accounts of Bank A, Bank B, and Bank C by logging in separately with the online accounts created by each bank.

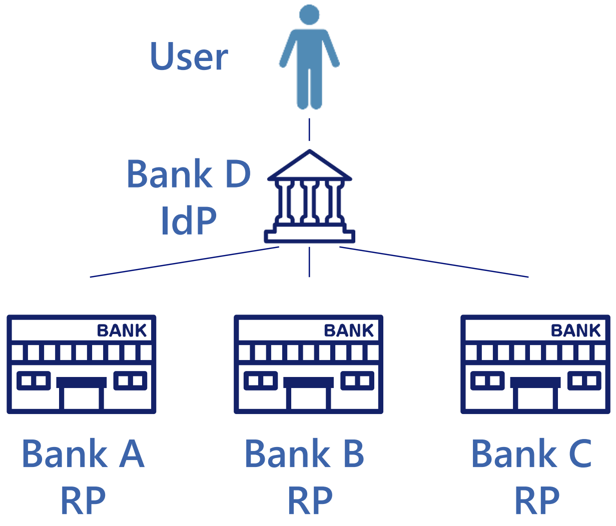
- **Federation model**
  - The RP and the IdP are separate entities, and users use the identity information of the IdP to access the digital services of the RP. A user can access multiple RPs based on the identity information of a particular IdP without the need to log in to each RP.

    Example: A user accesses the online banking accounts of Bank A, Bank B, and Bank C using the account provided by Bank D.

Centralized model

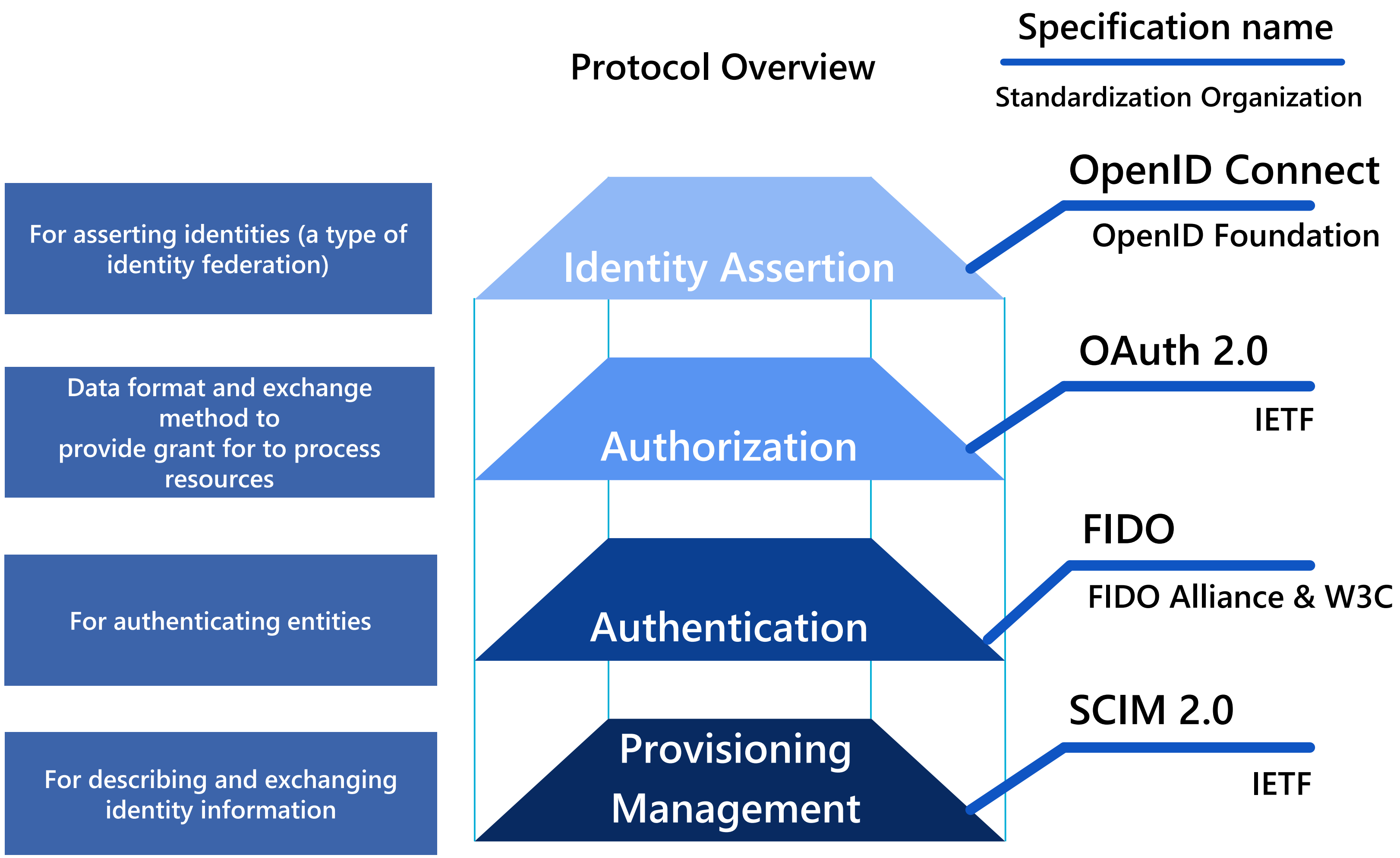


Federation model



Major Technological Elements Used in Main IMS Models

■ Protocols and major specifications used for the digital identity



Protocol Overview

Specification name

Standardization Organization

For asserting identities (a type of identity federation)

Identity Assertion

OpenID Connect

OpenID Foundation

Data format and exchange method to
provide grant for to process resources

Authorization

OAuth 2.0

IETF

For authenticating entities

Authentication

FIDO

FIDO Alliance & W3C

For describing and exchanging identity information

Provisioning Management

SCIM 2.0

IETF

Source) Created by NRI

Provisioning Management: What is SCIM 2.0?

■ SCIM 2.0 (System for Cross-domain Identity Management 2.0)

● A protocol specification for provisioning (management instructions) from a client of a website or application to a service provider of a web application for identity information managed in an identity management system.

Background of Appearance

- With the spread and expansion of the Internet, it has become necessary to provide management instructions (provisioning) for identity information across the board, not just confined to a single domain.
- In order to standardize the provisioning process, a protocol called SPLM (Service Provisioning Markup Language) was developed, but SPLM was not widely used due to its complex specification and poor interoperability. With the development of cloud services and the increase in usage opportunities, a new specification that is easy to use became necessary.

Specification Features

- In SCIM 2.0, released in 2015, identity information is written in JSON format with a common schema, and CRUD-specific processing is performed with a RESTful web API. The use of SCIM as a user-friendly protocol has been expanding.
- As various services became compliant with and supported SCIM, websites and applications could be provisioned from a variety of applications by supporting a single method.

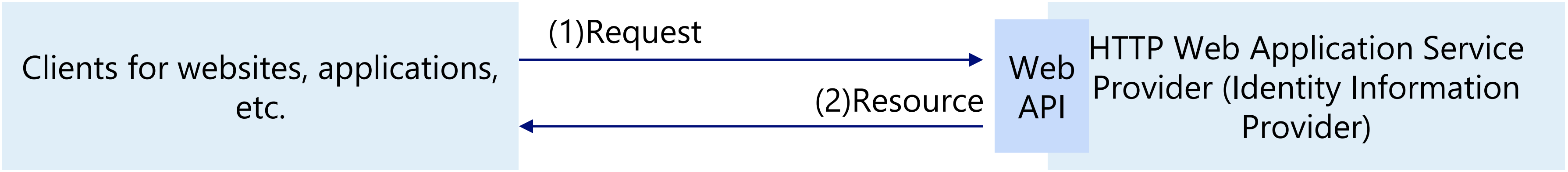
Specification Details

- SCIM 2.0 allows clients of Web sites and applications to perform provisioning (management instructions) using the HTTP REST protocol request method.
- A group of identity information (attributes) managed in JSON format within the IMS of a web application ("resource") is specified as the target of instructions.

Source) Created by NRI based on Information Technology Promotion Agency,
“Survey on Information Security Technology Trends (First Half of 2011) （https://www.ipa.go.jp/security/fy23/reports/tech1-tg/a_08.html),
System for Cross-domain Identity Management （http://www.simplecloud.info/) , IETF RFC:7643 SCIM Core Schema（https://tools.ietf.org/html/rfc7643）

Provisioning Management: What is SCIM 2.0?

Overview of the provisioning process in SCIM 2.0


Clients for websites, applications, etc.
(1)Request
(2)Resource
Web API
HTTP Web Application Service Provider (Identity Information Provider)

(1) Request method in REST protocol

Operation
Create
Read
Replace
Delete
Update

(2) Example of attributes when the type of "resource" is user

Attribute Name		Overview
userName		Username
name	Formatted	Full name ex.“Mr. Kenta Christopher Yamada, II”
	familyName	Gender ex. ”Yamada”
	givenName	Name ex. ”Kenta”
	middleName	Middle name ex. : ”Christopher”
	honorificPrefix	title of honour ex. : ”Mr.”
	honorificSuffix	suffix ex. : ”II”
displayName		Name displayed
nickName		Nick name

Source) Created by NRI based on IETF RFC:7643 SCIM Core Schema (https://tools.ietf.org/html/rfc7643)

Authentication: What is FIDO?

■ FIDO (Fast IDentity Online)

- A protocol specification for multi-factor authentication that verifies that the entity attempting to manipulate an identity is the same entity that was previously registered.

Background of Appearance

- Conventional authentication methods that use a combination of IDs and passwords have risks such as eavesdropping on the network, unauthorized access to verifiers, credential theft by man-in-the-middle attacks such as phishing sites, and list-type attacks.
- In response to this, there was a need for a multi-factor authentication specification that would not degrade the user experience and prevent unauthorized login through credential theft.

Specification Features

- The FIDO protocol enables robust authentication using standard public key cryptography.
- When registering for an online service, a new key pair is generated on the user's client device, the private key is kept on the client device, and only the public key is registered for the online service. The client device uses the private key to sign the challenge, thereby proving to the online service that it holds the private key for authentication.
- The private key held in the client device can be used by the user by unlocking it on the device. User-friendly and secure actions such as fingerprint authentication, face recognition, PIN entry, and two-step authentication device insertion can be adopted for unlocking.

Specification Details

- The FIDO Alliance, which is responsible for FIDO specification development and dissemination activities, initially developed specifications called UAF (Universal Authenticator Framework) and U2F (Universal Second Factor).
- Later, the W3C, which formulates standard technical specifications related to the Internet, formulated WebAuthn (Web Authentication API), which defines API specifications for a Web browser to function as a FIDO client and access a FIDO authenticator. In addition, the CTAP (Client to Authenticator Protocol), which defines communication specifications between FIDO clients and authenticators, was established and is collectively referred to as FIDO2.

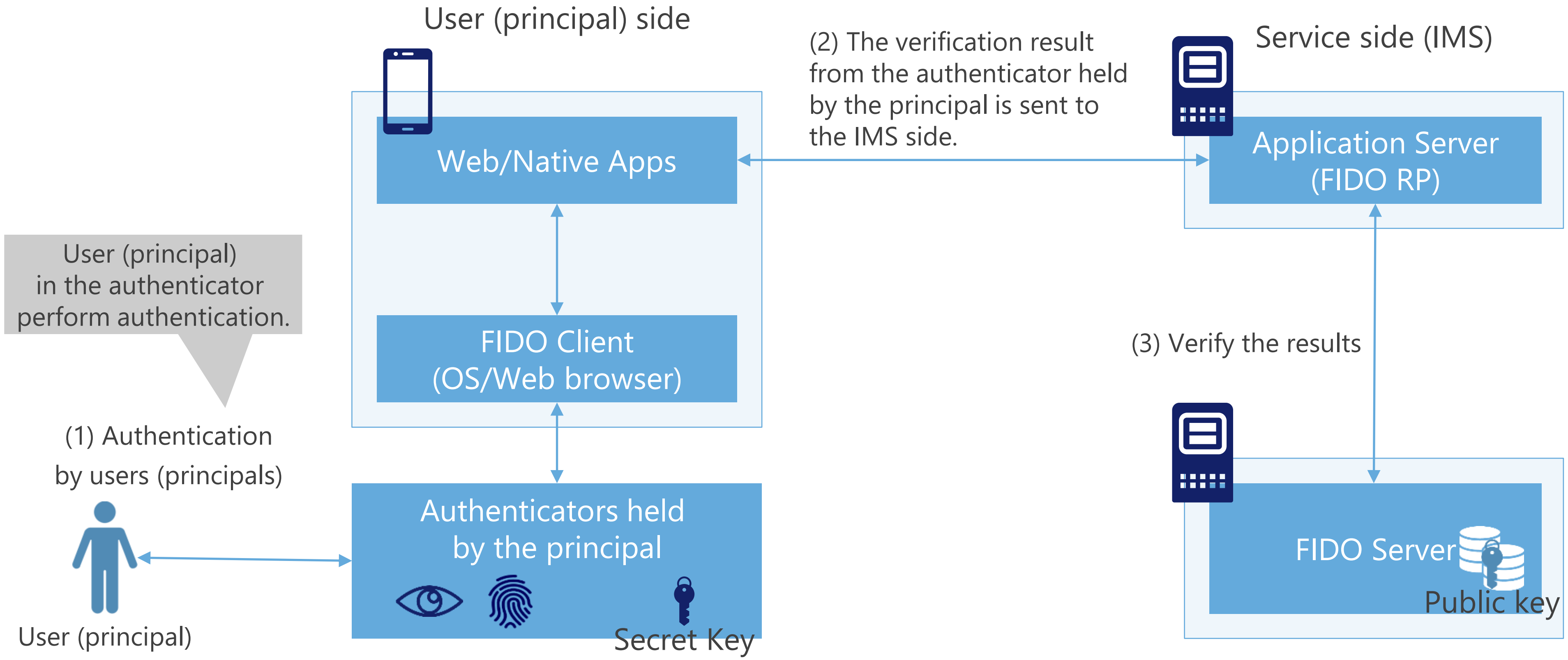
Source) Created by NRI based on FIDO Alliance websites

1-2. Main IMS Models and Components

Authentication: What is FIDO?

- The private key is held in the client device (authenticator) and only the public key is registered with the online service. The client device uses the private key to sign the challenge, thereby proving to the online service that it holds the private key for authentication.

Overview of authentication in FIDO2



Source) Created by NRI based on FIDO Alliance “FIDO2: WebAuthn & CTAP” (https://fidoalliance.org/fido2/)
Ministry of Health, Labour and Welfare, "Report on the Survey and Research Project for Certification and Approval (September 2020). (https://www.mhlw.go.jp/stf/newpage_14525.html)

Authorization: What is OAuth 2.0?

■ OAuth 2.0

- A specification of the format of data that provides authorization to process resources such as data and services, and the protocol for their exchange.

Background of Appearance

- Until the OAuth protocol that defined the concept of authorization was developed, it was necessary to delegate credentials such as IDs and passwords to applications that wanted to process specific resources.
- As a result, there is a risk that credentials (passwords) that allow full access to resources may be leaked in the event of an application information leak, there is a risk of granting access privileges to unnecessary resources, and the method of restricting (stopping) access by applications is limited to changing credentials. In addition, the method to restrict (stop) access by applications is limited to changing credentials.
- For this reason, there was a need for a specification that allows individual credentials with limited privileges to be granted, and access to be restricted at any time by the owner of the resource.

Specification Features

- OAuth 2.0 was developed from OAuth 1.0, which was defined based on the idea of delegating and authorizing access privileges.
- It provides individual credentials (tokens) with limited privileges, and in the event of an application information leak, credentials with full privileges will not be leaked, access to unnecessary resources can be restricted, and credentials can be disabled at any time.

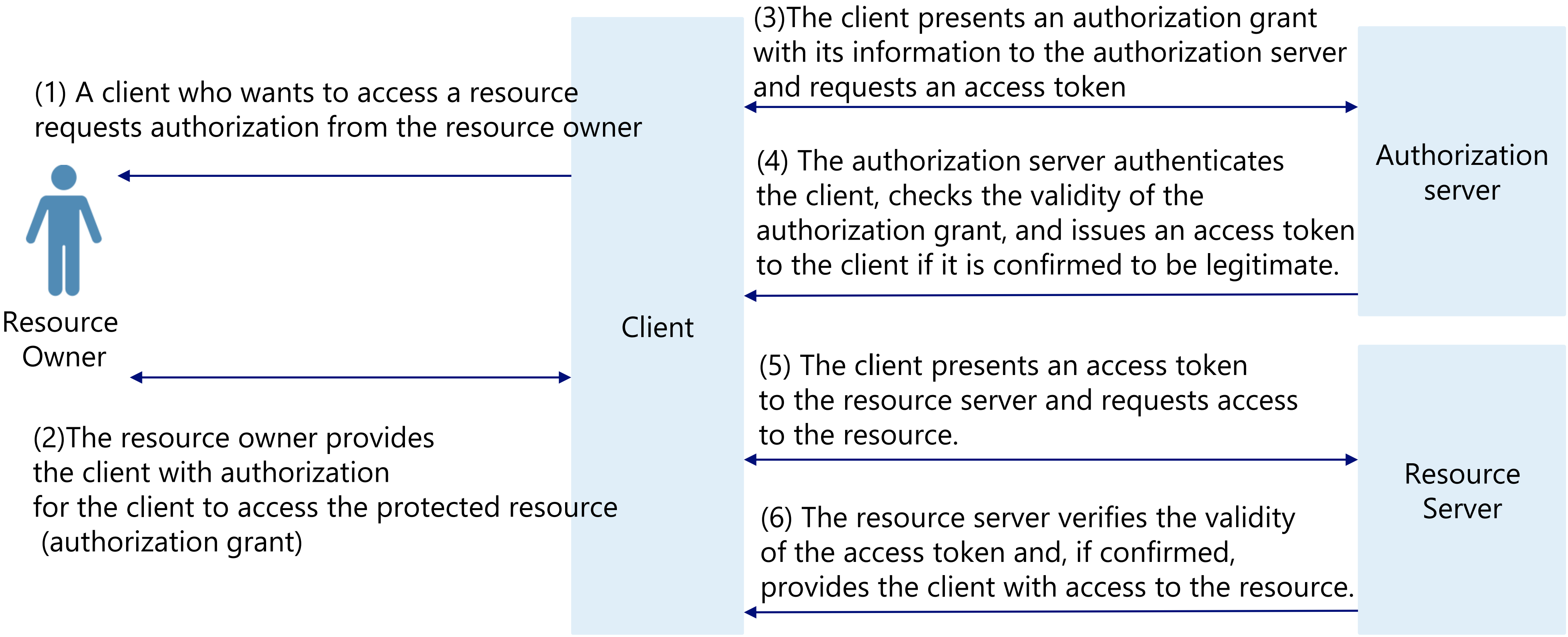
Specification Details

- OAuth 2.0 divides the roles into the entity that has ownership of the resource (resource owner), the server that holds and protects the resource on behalf of the resource owner (resource server), the application that attempts to access the resource after obtaining authorization from the resource owner (client), and the authorization server that provides the authorization exchange feature.

Source) Created by NRI based on OAuth “Introduction” （https://oauth.net/about/introduction/）
IETF RFC:6749 The OAuth 2.0 Authorization Framework（https://tools.ietf.org/html/rfc6749 ）

Authorization: What is OAuth 2.0?

Overview flow of OAuth 2.0



(1) A client who wants to access a resource requests authorization from the resource owner

(2)The resource owner provides the client with authorization for the client to access the protected resource (authorization grant)

(3)The client presents an authorization grant with its information to the authorization server and requests an access token

(4) The authorization server authenticates the client, checks the validity of the authorization grant, and issues an access token to the client if it is confirmed to be legitimate.

(5) The client presents an access token to the resource server and requests access to the resource.

(6) The resource server verifies the validity of the access token and, if confirmed, provides the client with access to the resource.

Source) Created by NRI based on IETF RFC:6749 The OAuth 2.0 Authorization Framework（https://tools.ietf.org/html/rfc6749 ）

Identity Federation: What is OpenID Connect?

■ OpenID Connect

- ● A protocol specification for identity federation, in which IMS passes identity information to other IMS.

Background of Appearance

- In response to the demand for single sign-on for Web services, a protocol called SAML (Security Assertion Markup Language) has been developed as a means to realize federation between IMS.
- Since this protocol requires the exchange of public keys and metadata before federation, and is a markup language that emphasizes XML format, it was expected that a federation protocol using a lighter language would emerge.

Specification Features

- OpenID Connect was released by the OpenID Foundation in 2014 based on OAuth 2.0, and has become widely used due to its adoption of lightweight data description in JSON format instead of XML, and its ability to communicate using RESTful protocols. It has become widely used because it uses lightweight data description in JSON format instead of XML, and because it can be exchanged using RESTful protocols.

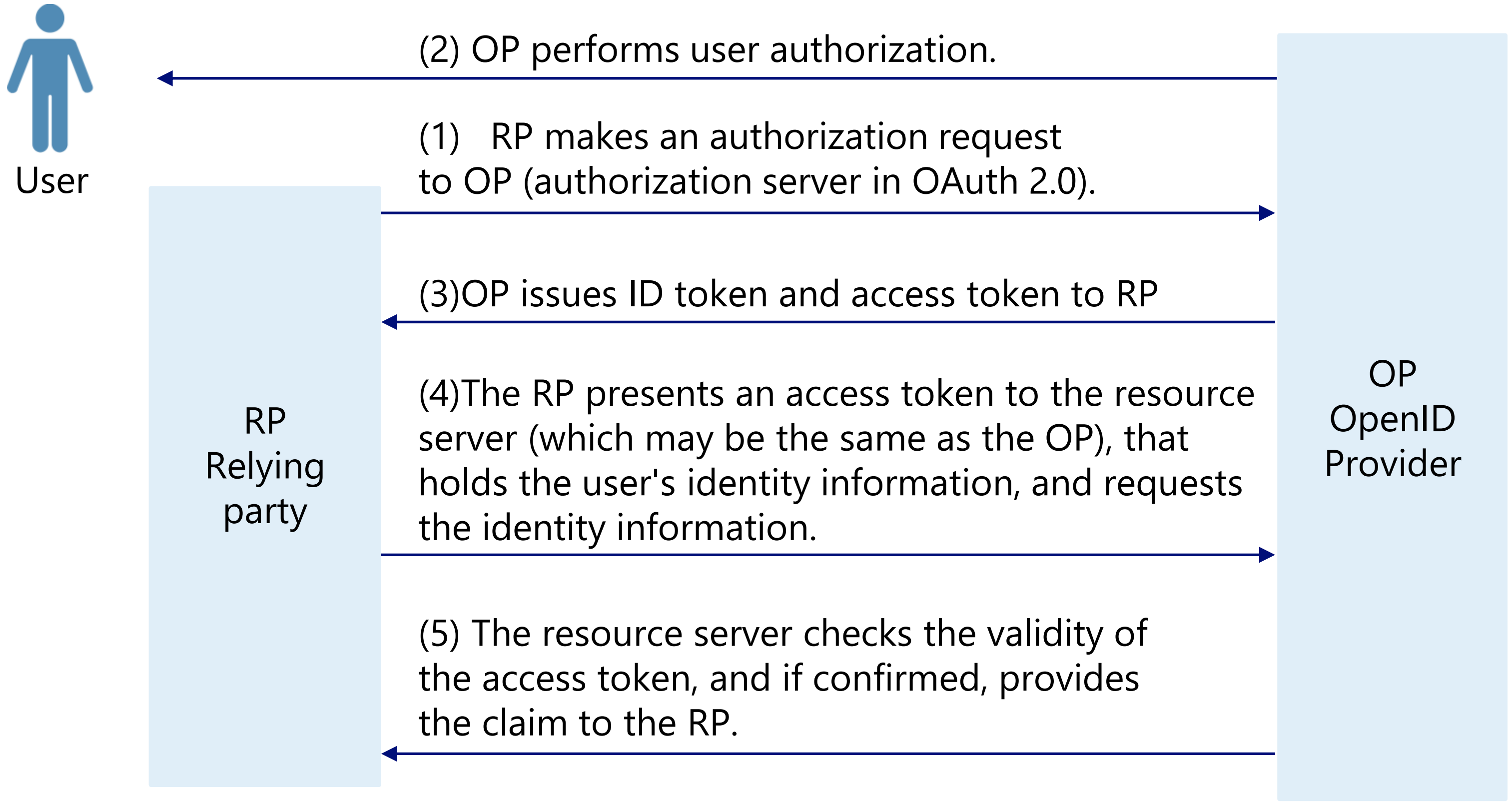
Specification Details

- OpenID Connect extends the concept of authentication to the OAuth 2.0 authorization process, enabling the use of secure identity federation and API federation.
- The relying party (client in OAuth 2.0) receives a JSON Web Token (JWT) called an "ID Token" that contains the user's authorization result and identity information from the OpenID Provider (authorization server in OAuth 2.0). Or it receives identity information from a resource server as a claim, which is a collection of information about the user.

Source) Created by NRI based on Ministry of Internal Affairs and Communications, "Research and Development of Advanced Privacy Protection Functions in an Open ID Collaboration Platform for Information Distribution Collaboration (2012)" (https://www.soumu.go.jp/main_content/000256289.pdf) and OpenID Connect Core 1.0 incorporating errata set 1 (https://openid.net/specs/openid-connect-core-1_0.html)

Identity Federation: What is OpenID Connect?

Overview flow of the OpenID Connect



(2) OP performs user authorization.

(1) RP makes an authorization request to OP (authorization server in OAuth 2.0).

(3)OP issues ID token and access token to RP

(4)The RP presents an access token to the resource server (which may be the same as the OP), that holds the user's identity information, and requests the identity information.

(5) The resource server checks the validity of the access token, and if confirmed, provides the claim to the RP.

Source) Created by NRI based on OpenID Foundation “OpenID Connect Core 1.0 incorporating errata set 1”の1.3 Overview（https://openid.net/specs/openid-connect-core-1_0.html）

Governance Framework for Digital Identity (Trust Framework)

- In order to properly operate IMS, it is important to design and operate it based on not only technical elements such as standard protocols, but also governance elements.
- Many rules for the governance of digital identities have been developed and published in other countries under the name of "trust frameworks". For example, the Open Identity Exchange (OIX), an international non-profit organization, defines a trust framework as "an environment for governed identity transactions based on a set of rules that enable users, organizations, services and devices to trust each other." and has developed and published rules/guides on the following topics

Components specified in the OIX trust framework

Components	Items
Principles	
Trustmark(s) and UX	
Roles and Obligations	
General Rules	Record Keeping and Audit Trail
	Fraud and Cyber Controls
User Services	Choosing a Digital Identity
	Creation and Management of a Digital Identity
	Achieving and Presenting Trust
	Consent
	Help and Support

Components	Items
Relying Party Services	User Access to Identity Service
	Requests and Responses (API)
	Relying party Based Identity Assurance
	Liability
	Service Levels
	Help & Support
Trust Rules	Proofing
	Identity Assurance
	Authentication
	Eligibility Assurance

Components	Items
Security and Technical Requirements	Security Rules
	Trust Registry of eco-system participants
	Recording and Presentation of evidence Proofs
	Request and Response Schemas
Interoperability Requirements	Internal Interoperability
	External Interoperability
Governance of the Trust Framework	Creation and Management of a Trust Framework
	Enforceability of a Trust Framework
	Certification to a Trust Framework
	Operation of a Trust Framework

Source) OIX,” OIX Guide to Trust Frameworks(version 0.1 Beta)”

Major Governance Frameworks for Digital Identity in Other Countries

- Many countries have formulated and issued governance frameworks (trust frameworks) for the appropriate operation of IMS by government agencies, private sector, and other entities, and each IMS operator is required to build a governance framework based on these frameworks.
- In Japan, the Act on Prevention of Transfer of Criminal Proceeds, the Act on Prevention of Improper Use of Mobile Phones, the Electronic Signature Act, and other laws stipulate requirements for identity verification, but there is no governance framework for digital identity in general.

Major governance frameworks for digital identity in other countries

Country		Publishing Organization	Governance Framework
U.S.A	NIST	NIST SP 800-63 Series (2017)	• The U.S. National Institute of Standards and Technology (NIST) has formulated the SP800-63 series of "Guidelines for Electronic Authentication," which are widely referenced guidelines not only by government agencies but also by the private sector.
EU	European Commission	eIDAS	• Provided for eID (electronic identification) and eTrust services (electronic signatures, electronic seals, time stamps, electronic distribution, website authentication, etc..) And applies as law to EU member states. (Ratified on 23 July 2014)
Australia	Digital Transformation Agency	Trusted Digital Identity Framework	• The Digital Transformation Agency (Australia) published the Trusted Digital Identity Framework (TDIF) in February 2018. It sets out standards and rules for the authentication of providers of digital identity services.
UK	Department for Digital, Culture, Media & Sport	UK Digital Identity and Attributes Trust Framework	• Guidelines (alpha version) for operators (identity service providers, attribute service providers, orchestration service providers and relining parties) using digital identities published February 2021. It specifies the requirements that will be needed to authenticate providers in the future.
Canada	DIACC *Non-profit organization	Pan-Canadian Trust Framework (PCTF) 1.0	• DIACC is a not-for-profit organization established in 2012 in response to the recommendations of the Treasury Board of Canada Task Force. • The PCTF was developed as a framework for the use of digital identities by government agencies and private sector businesses in Canada.
-	OIX *Non-profit organization	OIX Guide to Trust Frameworks	• OIX is a non-profit organization founded in 2010. It was established at the request of the U.S. government, with funding from the OpenID Foundation and the Information Card Foundation. • The Trust Framework sets out specific principles, content and responsibilities for businesses that use digital identities.

Source) Created by NRI based on each website

1-3. Self-Sovereign Identity (SSI)

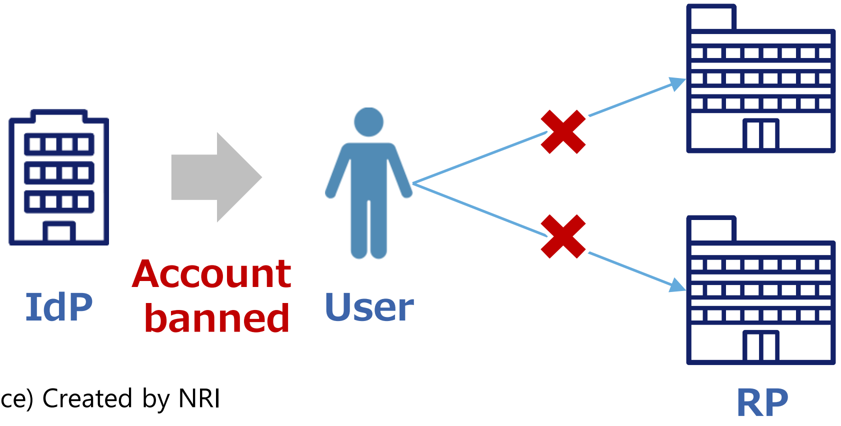
1-3. Self-Sovereign Identity (SSI)

Concerns about Federation Model

- The federation model is now the mainstream, and reliance on identity providers is increasing.
- However, there are some concerns about relying on a specific identity provider. For example, if the following risks were to materialize, the impact on users would be enormous.
  ① Risk of account suspension by an identity provider (intentional suspension by a malicious IdP, suspension due to bankruptcy, etc.)
  ② Risk of identity tampering by (malicious) identity providers
- As ideas for identity management that can resolve these concerns, Self Sovereign Identity (SSI) and Decentralized Identity (DID) have been proposed.

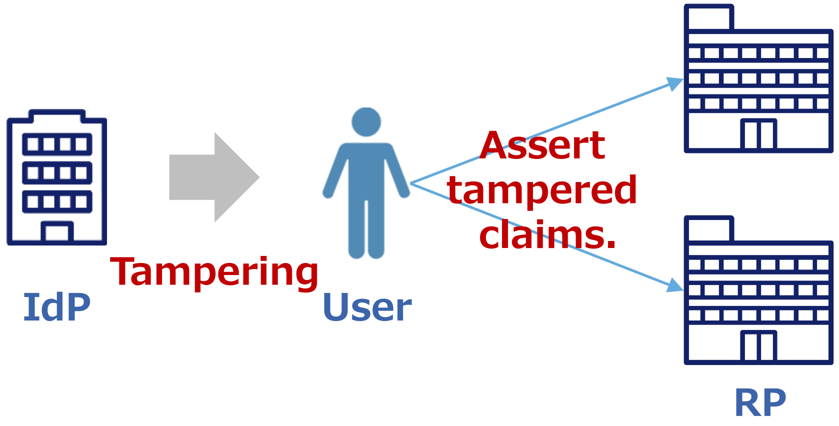
Example: Risk of having an account suspended by an IdP

- When an IdP suspends a user's account, other services that are utilized for ID assertion will also become unavailable.



Example: Risk of tampering by an IdP

- There is a risk that the IdP will intentionally tamper with the identity of the user and the tampered claims will be shared to the RP.



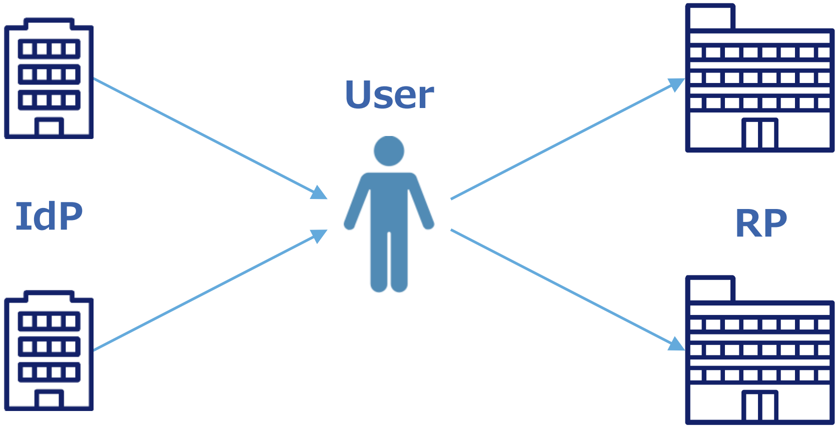
Source) Created by NRI

What is Self-Sovereign Identity/Decentralized Identity?

■ Self-Sovereign Identity：SSI

- A concept that aims to allow individuals to control their own identities without the intervention of an identity management entity (*1).
- After ensuring that the user has control over their own the information, the user can obtain the information issued by a trusted organization and assert it to RPs, etc. to the scope permitted by the user.

Conceptual diagram of SSI

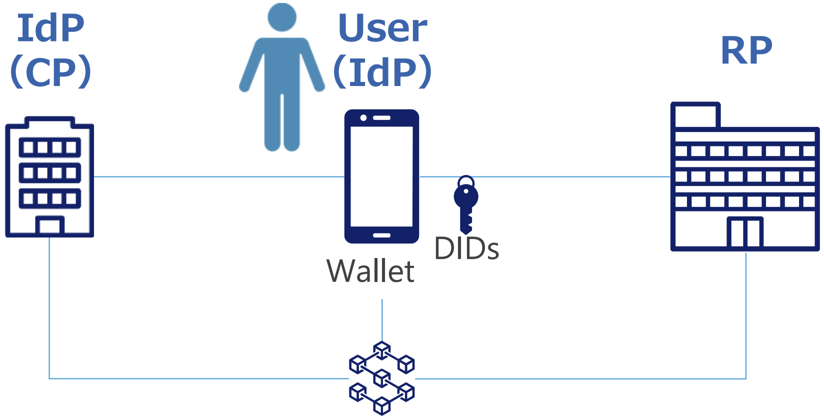


■ Decentralized Identity：DID

- In contrast to SSI, which aims to allow users to self-control their own digital identity, decentralized identity aims to reduce the dependency of a user's digital identity on a specific IdP. To realize this, the use of distributed repositories such as blockchain is often advocated.
- For example, Microsoft, which has published a white paper on decentralized identity, defines it as follows(*2).

  "Decentralized identity replaces identifiers such as usernames with self-owned, independent identities, and enables data exchange using blockchain and distributed ledger technologies."(Microsoft)

Conceptual diagram of DID



Distributed repositories (e.g., blockchain)

*1 : Sovrin Foundation, https://sovrin.org/faq/what-is-self-sovereign-identity/

*2 : Microsoft, https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain

Seven Laws of Identity

- Kim Cameron, who proposed the "Seven Laws of Identity", has presented the "Seven Laws of Identity in SSI", which are based on the "Seven Laws of Identity".
- From the "Seven Laws of Identity", **mainly principles 5 and 6 are updated in the SSI version.** The details of this update are described in Chapter 3.

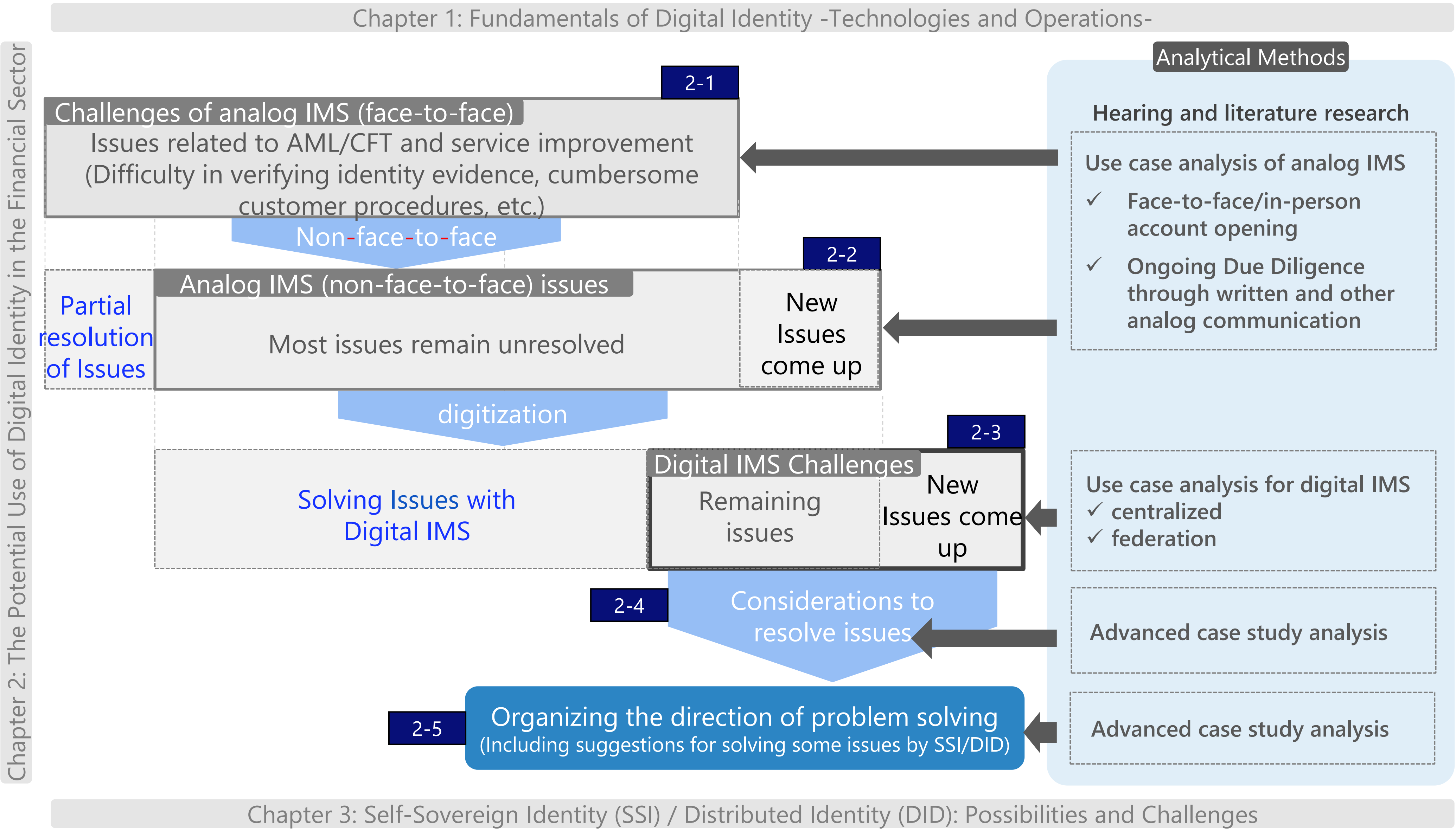
#	Principles	Contents
1	Law of User Control and Consent	• Identity systems must only reveal information identifying a user with the user's consent.
2	Law of Minimal Disclosure For A Constrained Use	• The identity system must disclose the least identifying information possible, as this is the most stable, long-term solution.
3	Justifiable Parties	• Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4	Directed Identity	• A universal identity system must support both "omni-directional" identifiers for use by public entities and "uni-directional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5	Standardized identity hub	• User can represent him/herself and use identity in a consistent manner across providers, with identity being separated across the context at the same time
6	Standardized DID for long-terms identity stability	• After storing personal data in a way that it is not dependent on the operators, survive the identity operators and retain relationships with service
7	Human Integration	• Identity systems must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

Source) Created by NRI based on Natsuhiko Sakimura, “The Law of Identity in SSI Era by Kim Cameron”
https://nat.sakimura.org/2020/06/23/the-law-of-identity-in-ssi-era-by-kim-cameron/

Chapter 2: The Potential Use of Digital Identity in the Financial Sector

Overview of this chapter

Flow of this chapter



Chapter 1: Fundamentals of Digital Identity -Technologies and Operations-

Chapter 2: The Potential Use of Digital Identity in the Financial Sector

2-1

Challenges of analog IMS (face-to-face)

Issues related to AML/CFT and service improvement (Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)

Non-face-to-face

2-2

Partial resolution of Issues

Analog IMS (non-face-to-face) issues

Most issues remain unresolved

New Issues come up

digitization

2-3

Solving Issues with Digital IMS

Digital IMS Challenges

Remaining issues

New Issues come up

2-4

Considerations to resolve issues

2-5

Organizing the direction of problem solving

(Including suggestions for solving some issues by SSI/DID)

Analytical Methods

Hearing and literature research

Use case analysis of analog IMS

- ✓ Face-to-face/in-person account opening
- ✓ Ongoing Due Diligence through written and other analog communication

Use case analysis for digital IMS

- ✓ centralized
- ✓ federation

Advanced case study analysis

Advanced case study analysis

Chapter 3: Self-Sovereign Identity (SSI) / Distributed Identity (DID): Possibilities and Challenges

Research Method

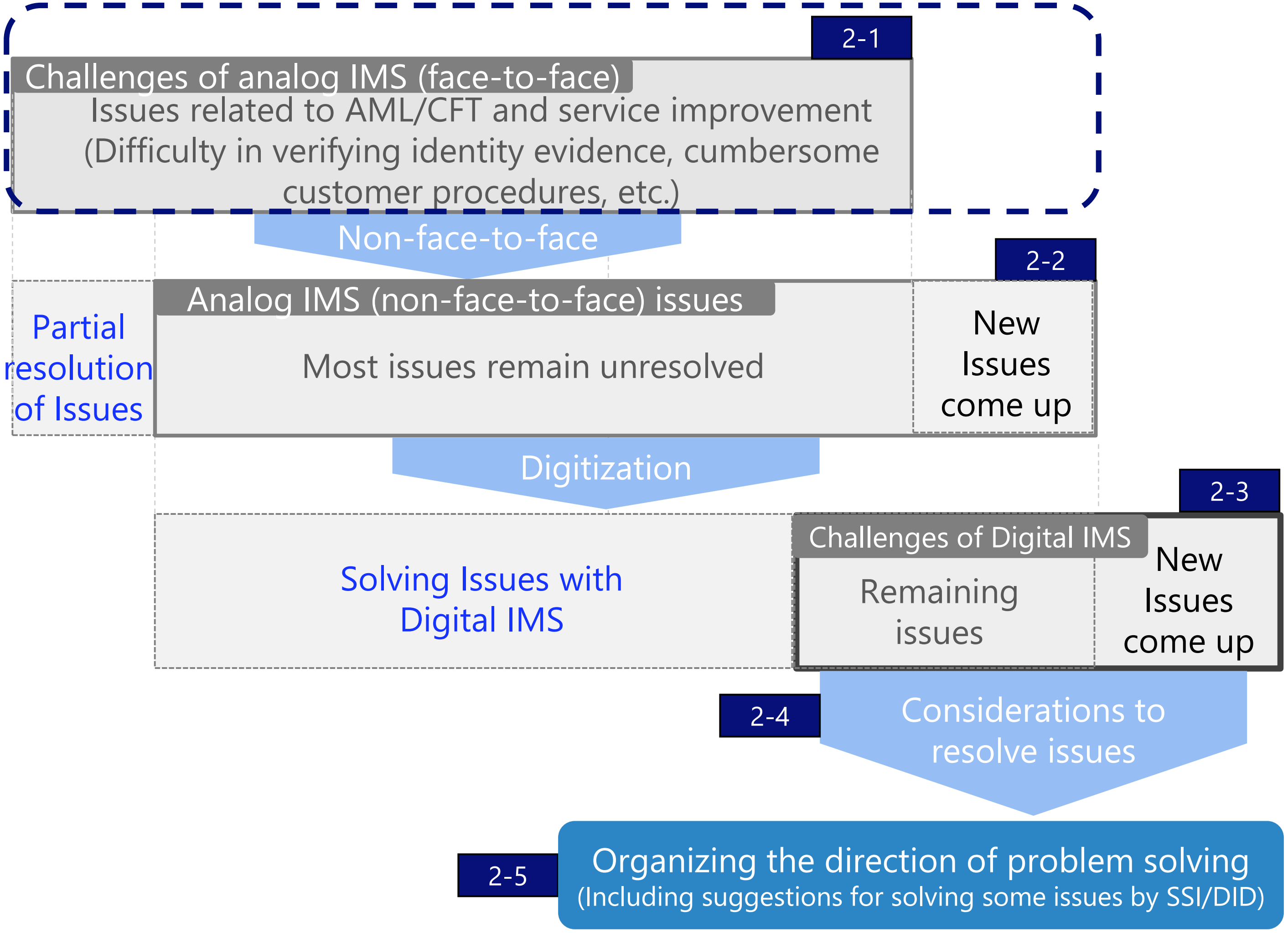
- The following methods were mainly used to identify various issues and investigate the direction of problem solving, as described in the next section.
  - Hearing research with experts in Japan and overseas
  - document survey
  - Analysis of leading examples of using digital identity
- Objectives and perspectives of the survey
  - Conducted interviews with various stakeholders related to the use of digital identities in the financial sector and surveyed the literature published by each stakeholder.
  - Analyzed the business operations of a bank (deposit-taking financial institution), which is one of the most important financial institutions.

Survey targets and perspectives

Destination of survey		Perspectives on problem identification/problem-solving direction research
Domestic	Financial institutions legal personnel Solution Vendors	• Issues in current operations of identity management, focusing on AML/CFT operations • Current efforts, challenges, and future prospects for the use of digital identity • Legal and technical issues when using digital identity
Overseas	Financial institutions Regulators/associations international organization industry group standards body Solution Vendors	• Current initiatives, issues, and future perspectives on the use of digital identity • Specific examples of applications that contribute to improved customer convenience and their challenges • Implications for the advancement of risk-based approaches and financial inclusion • Status and future prospects of regulatory development and compliance • Technology Standardization Trends

2-1. Current Status and Issues of Identity Management in Financial Institutions

Subject of discussion in this section


2-1
Challenges of analog IMS (face-to-face)
Issues related to AML/CFT and service improvement
(Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)
Non-face-to-face
2-2
Partial resolution of Issues
Analog IMS (non-face-to-face) issues
Most issues remain unresolved
New Issues come up
Digitization
2-3
Solving Issues with Digital IMS
Challenges of Digital IMS
Remaining issues
New Issues come up
2-4
Considerations to resolve issues
2-5
Organizing the direction of problem solving
(Including suggestions for solving some issues by SSI/DID)

Overview of Identity Management Operations

■ Target Areas to be investigated in this chapter

- In this chapter, identity information refers to identities (set of attributes related to a certain entity) managed in ICT systems, etc., as in Chapter 1. Specifically, it refers to user attributes such as name, address, date of birth, user identifier, transaction history, etc.
- In this chapter, identity management refers to activities related to identity management system (IMS) defined in Chapter 1. Specifically, it refers to the management of identity information and the provision, etc. of attributes requested by each service
- In this chapter, we selected the fields that are considered to be closely related to identity management as the main topic of survey.
- Discussions centered on AML / CFT regulatory compliance, where strict identity management is required, such as identity verification being stipulated by law.
- We will focus on operations related to identity verification which is a part of AML/ CFT regulatory compliance. The compliance requires stringent management of identity such as identity verification, etc. as stipulated by law.
- In addition, mention about improving customer service by utilizing multifaceted identity information, which aims to provide products and services in the best interests of users.

Policy Goal	Items	Relationship with identity management
Balance stability of the financial system and the performance of financial intermediary functions	AML/CFT regulatory compliance	Verification at the time of transaction, customer filtering, analysis / evaluation, judgment / response
User protection and user convenience	Effort to provide products and services in the best interests of users	Improvement in customer service using identity information

Source: Created by NRI based on "Financial Inspection / Supervision and Procedure (Basic Inspection / Supervision Policy" of Financial Services Agency
https://www.fsa.go.jp/news/30/wp/supervisory_approaches_revised.pdf

2-1-1. Current Status and Issues of Identity Management in Financial Institutions

Overview of Identity Management Operations

■ Classification of operations to be considered in this chapter

- Regarding the subject areas described in the previous page, the types of work to be considered in this chapter are classified into three categories based on the purpose of the work and the timing of the implementation of the work.
- The terms “onboarding” and “ongoing” in this section refer to the classification based on the timing of operations, and the same applies to the following pages.
  - Onboarding: Refers to operations at the time of account opening, and in this survey, refers to (1) in the figure below.
    (In this survey, regarding operations for the purpose of improving customer service, there is no operation at the time of opening an account. So, here it means onboarding due diligence as described in the glossary).
  - Ongoing: This term refers to operations after the completion of account opening, and in this study refers to (2) and (3) in the figure below.
    The term "ongoing due diligence" refers to (2) in the glossary.

		Timing of Operations	
		Onboarding	Ongoing
Purpose of Operations	AML/CFT regulatory compliance	(1) Account Opening (verification at the time of transaction)	(2) Ongoing Due Diligence
	Improve customer service	(No work before identity registration)	(3) Provide services using Identity information inside and outside the company

Outline of Identity management operation for each business category

Classification of operations			Overview of Operations
Onboarding	(1) Account Opening (verification at the time of transaction)		Application for account opening for customer - Examination and decision by financial institution to open account
Ongoing	(2) Ongoing Due Diligence	Periodic Customer Information Collection	Periodic verification of attribute changes for account-holding customers
		Verification upon receipt of transaction	Transaction application from customer - Risk confirmation and decision by financial institution
		Transaction Monitoring (after)	Financial institutions‘ analysis of trading trends of customer and reassessment of customer risk
	3) Provide services using identity information inside and outside the company		Collection and analysis of customer identity information by financial institutions and efforts to improve customer service (tailor-made service proposals, etc.)

Details of Identity Management Operations
(1) Account Opening (verification at the time of transaction)

Operation Process for Account Opening (verification at the time of transaction)

Operation Process	Process details	
Receipt of application	Receipt of application form for account opening, etc.	• Receive account opening application and identity evidence (see next page for definition) from customer.
Verification at the time of transaction	Verification of identity/ objective of transactions	• Verify the authenticity (that the information is correct for the applicant) and validity (that the identity evidence is valid) of the identity evidence. Also verify objective of transaction and ultimate beneficial owner (in the case of a corporation).
Customer Filtering	Customer Filtering	• Prevent antisocial forces and sanctioned persons from holding accounts by checking against the list of antisocial forces and sanctioned persons, and by verifying consistency with transaction purposes, attributes, and ultimate beneficial owners.
Analysis and evaluation	Assessing customer risk	• Analyze AML risk, etc., based on transaction type, customer attributes, product and service characteristics, etc., and conduct additional verification if necessary.
Judgment and response	Account Opening Notification or Suspicious Activity Report	• Approve the opening of an account and notify the customer, or decline the opening of an account and file a suspicious activity report, if necessary.

Appendix: Definitions and Examples of Identity Evidence

- In this chapter, identity evidence is defined as "identification documents/corporate identification documents recognized in each jurisdiction.

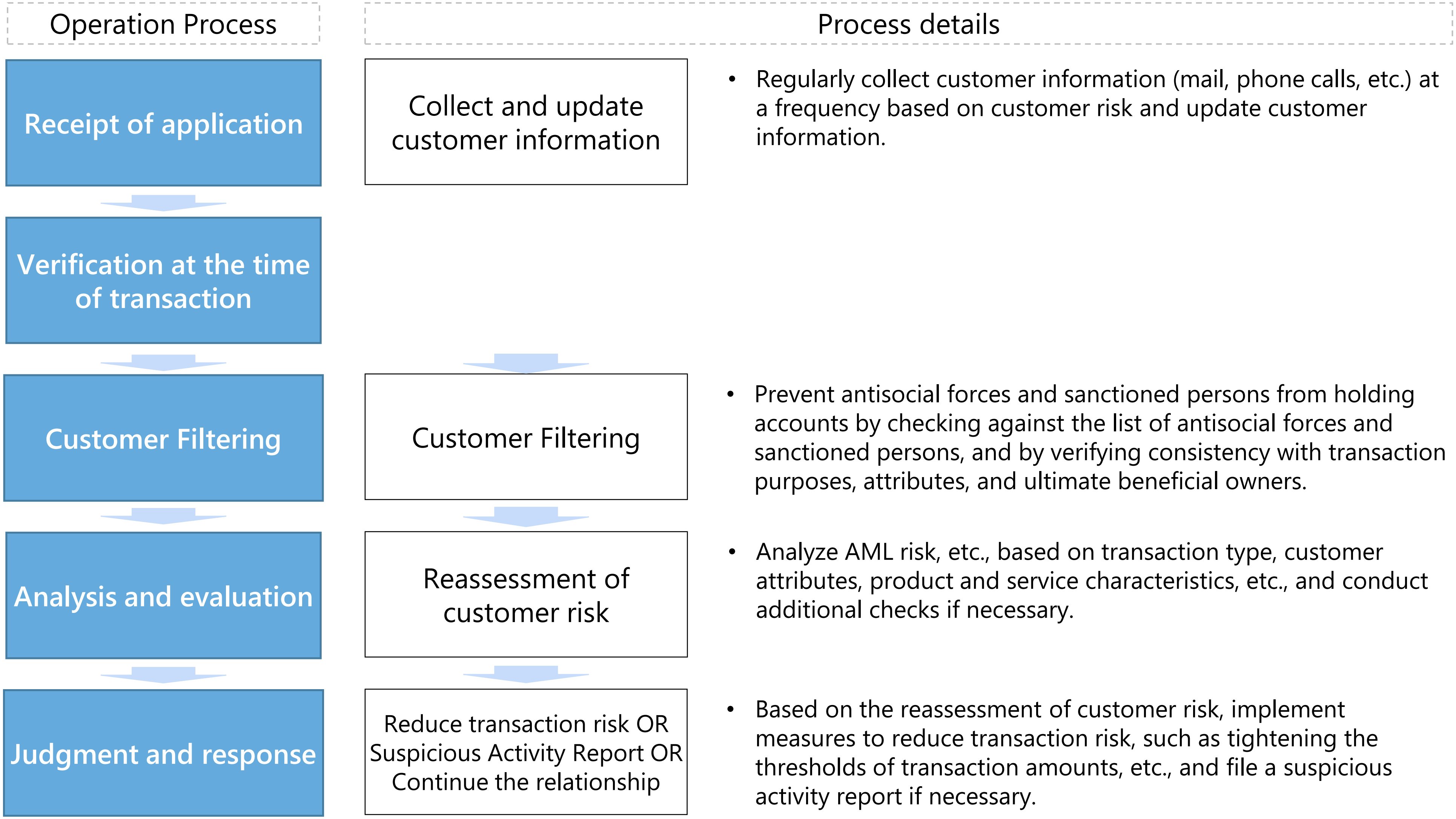
An example of identity evidence

Individual/ Corporate	Overview
Individual	• Personal Identification Documents ✓ Driver's license ✓ Passport ✓ National ID card (e.g., My Number Card in Japan) ✓ Residence card, special permanent resident certificate (e.g., U.S. green card), etc.
Corporate	• Corporate Identification Documents ✓ Certificate of registration ✓ Certificate of stamp registration ✓ Documents, etc. issued by public offices other than those listed above that contain the name of the corporation and the location of its head office or principal office. • Identity verification documents of the person in charge, representative, or ultimate beneficial owner ✓ Same as individuals

2-1-1. Current Status and Issues of Identity Management in Financial Institutions

Details of Identity Management Operations
(2) Ongoing Due Diligence (2)-1 Periodic Customer Information Collection

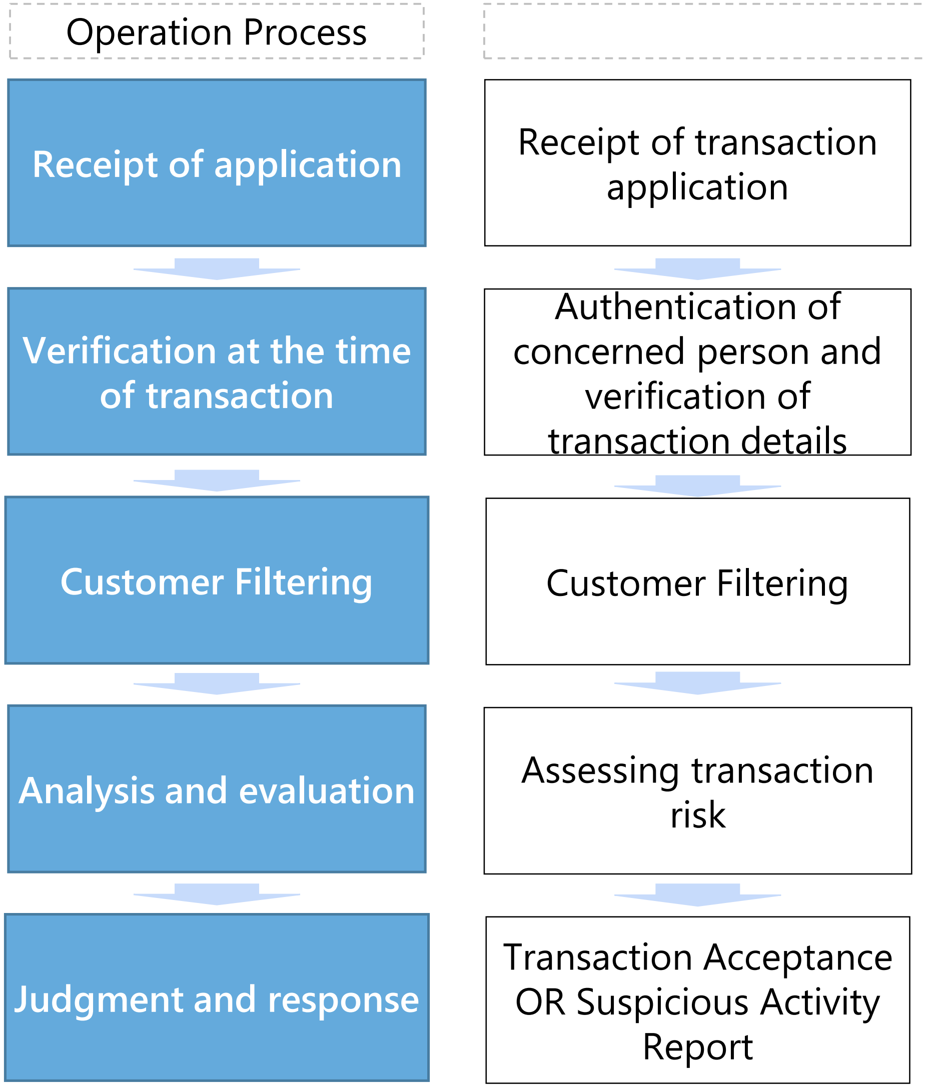
Operation Process for Periodic Customer Information Collection



Operation Process	Process details	
Receipt of application	Collect and update customer information	• Regularly collect customer information (mail, phone calls, etc.) at a frequency based on customer risk and update customer information.
Verification at the time of transaction		
Customer Filtering	Customer Filtering	• Prevent antisocial forces and sanctioned persons from holding accounts by checking against the list of antisocial forces and sanctioned persons, and by verifying consistency with transaction purposes, attributes, and ultimate beneficial owners.
Analysis and evaluation	Reassessment of customer risk	• Analyze AML risk, etc., based on transaction type, customer attributes, product and service characteristics, etc., and conduct additional checks if necessary.
Judgment and response	Reduce transaction risk OR Suspicious Activity Report OR Continue the relationship	• Based on the reassessment of customer risk, implement measures to reduce transaction risk, such as tightening the thresholds of transaction amounts, etc., and file a suspicious activity report if necessary.

Details of Identity Management Operations
(2) Ongoing Due Diligence (2)-2 Verification upon Receipt of Transaction

Operation Process for Verification upon Receipt of Transaction

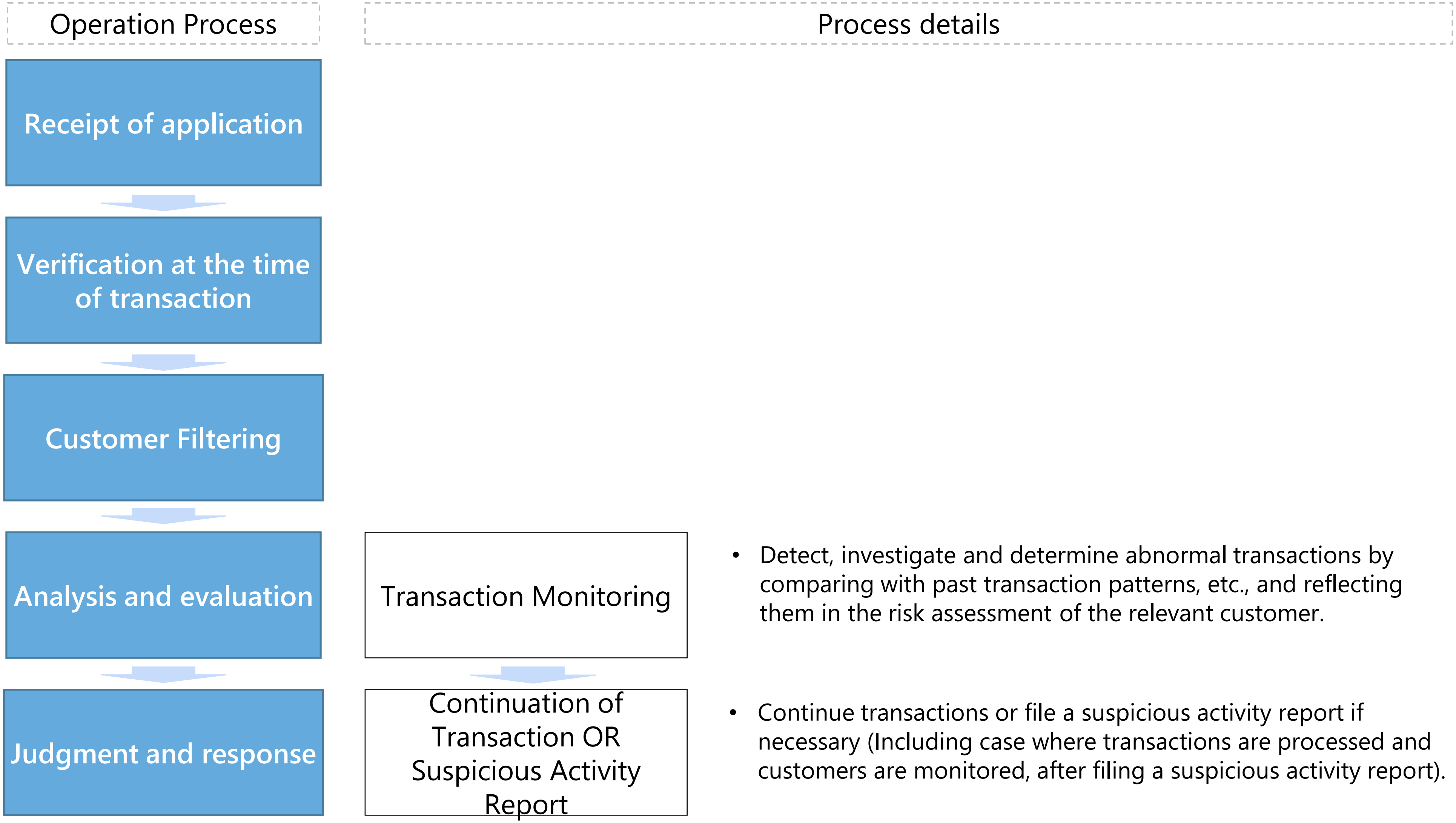


Operation Process	Process details	
Receipt of application	Receipt of transaction application	• Receive transaction application documents from customers.
Verification at the time of transaction	Authentication of concerned person and verification of transaction details	• Verify the authenticity (that the information is correct for the applicant) and validity (that the identity evidence is valid) of the identity evidence. • Authenticate the applicant who is conducting the transaction and verify the transaction details such as the purpose and amount of the transaction.
Customer Filtering	Customer Filtering	• Prevent antisocial forces and sanctioned persons from holding accounts by checking against the list of antisocial forces and sanctioned persons, and by verifying consistency with transaction purposes, attributes, and ultimate beneficial owners.
Analysis and evaluation	Assessing transaction risk	• Analyze AML risk, etc., based on transaction type, customer attributes, product and service characteristics, etc., and conduct additional checks if necessary.
Judgment and response	Transaction Acceptance OR Suspicious Activity Report	• Accept or reject transactions and, if necessary, file a suspicious activity report.

2-1-1. Current Status and Issues of Identity Management in Financial Institutions

Details of Identity Management Operations
(2) Ongoing Due Diligence (2)-3 Transaction Monitoring (after)

Operation Process for Transaction Monitoring (after)


Operation Process

Process details

Receipt of application

Verification at the time of transaction

Customer Filtering

Analysis and evaluation

Judgment and response

Transaction Monitoring

Continuation of Transaction OR Suspicious Activity Report

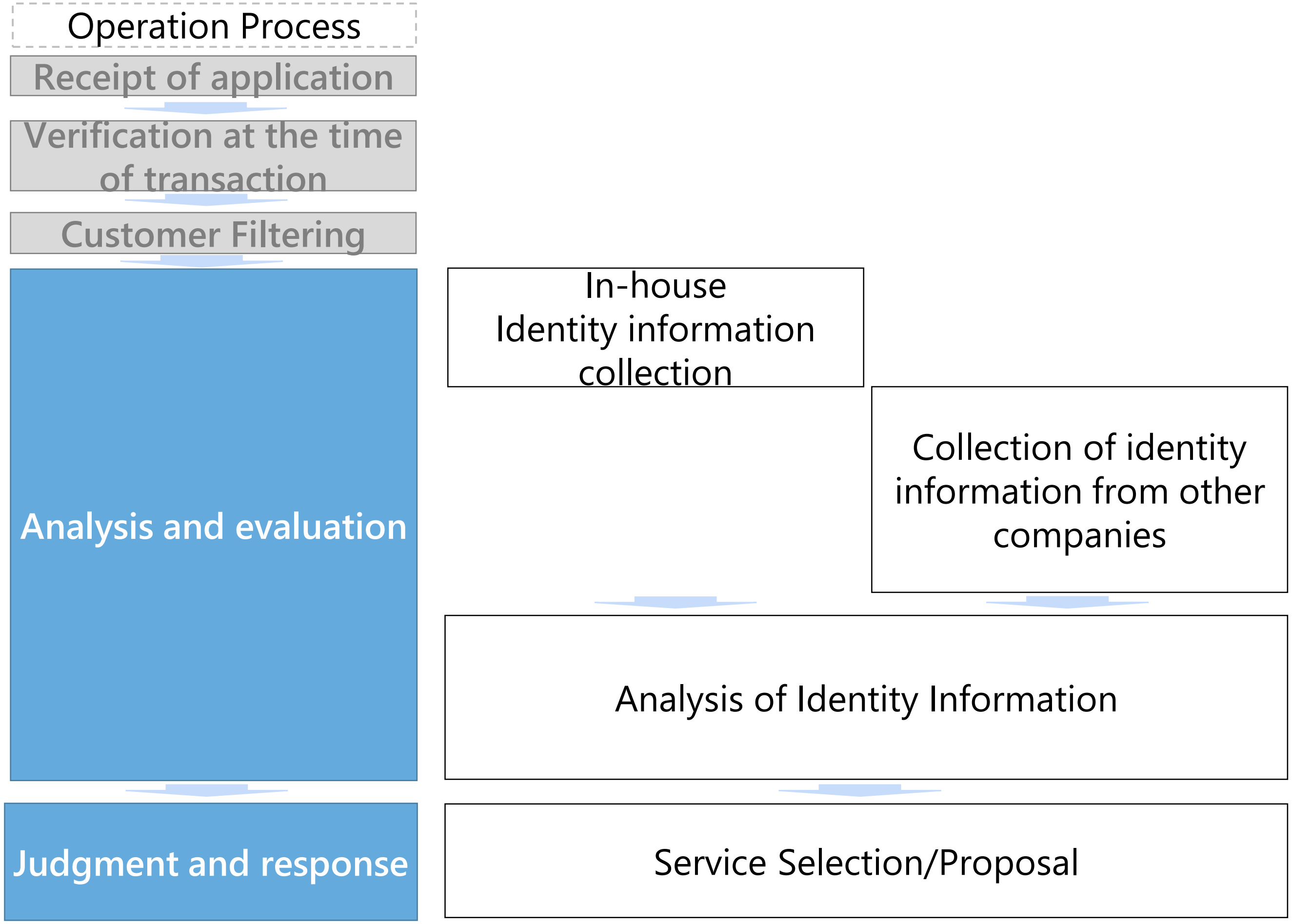
- Detect, investigate and determine abnormal transactions by comparing with past transaction patterns, etc., and reflecting them in the risk assessment of the relevant customer.
- Continue transactions or file a suspicious activity report if necessary (Including case where transactions are processed and customers are monitored, after filing a suspicious activity report).

Details of Identity Management Operations

(3) Improve customer service by utilizing identity information inside and outside the company

- Take initiatives to improve customer service, such as proposing tailor-made services, etc. by collecting and analyzing a variety of internal and external identity information related to customers.

Operation Process for Improving Customer Service by utilizing identity information inside and outside the company



Operation Process
Receipt of application
Verification at the time of transaction
Customer Filtering
Analysis and evaluation
Judgment and response
In-house Identity information collection
Collection of identity information from other companies
Analysis of Identity Information
Service Selection/Proposal

- Collect information related to customers such as transaction information within the company.
- Collect customer-related information from other companies, including financial and non-financial transaction information, non-traditional information (customer site access and location information, social networking sites), etc.
- Analyze customer's financial needs, etc. from the collected information (e.g., analyze the timing when educational loan might be needed from a customer's EC site purchase history, etc.).
- Based on the analysis results, select the most suitable service for the customer and propose it to the customer.

2-1-1. Identity Management Operations in Financial Institutions

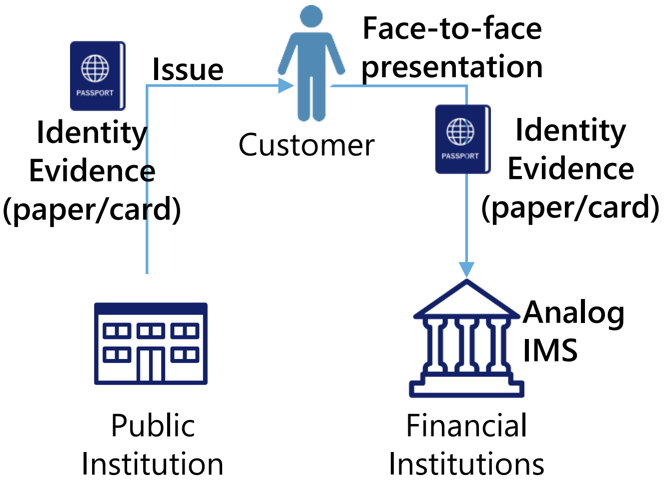
Identity management operations are still analog centric

■ Conduct analog-centric operations such as usage of face-to-face analog identity evidence* and mail documents by post, etc.

* Analog identity evidence: Refer to Identity evidence that cannot be read as data, such as paper, cards, images, etc.

Identity verification for Account Opening

- Customers submit analog identity evidence to financial institutions in person.
- The financial institution verifies the identity of the customer based on the evidence.

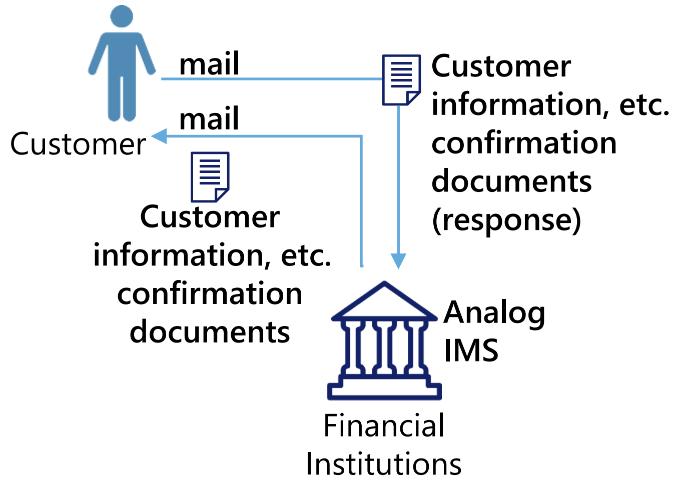


Issue
Face-to-face presentation
Identity Evidence (paper/card)
Customer
Identity Evidence (paper/card)
Analog IMS
Public Institution
Financial Institutions

*Authenticity and validity of identity evidence to public authorities are not conducted for analog identity evidence.

Ongoing Due Diligence (Periodic Customer Information Collection)

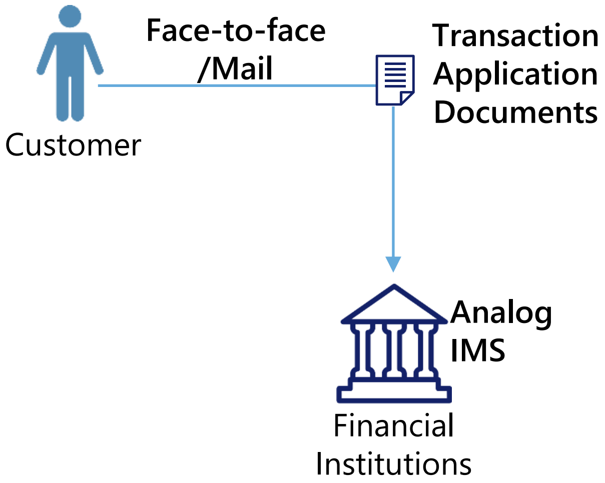
- Financial institutions mail customer information,etc. related confirmation document to the customer.
- Customer mails the customer information confirmation document (response) and analog identity evidence (only when the address change, etc. is required) to the financial institution.
- Financial institutions carry out identity verification and modification of attributes.



mail
Customer information, etc. confirmation documents (response)
mail
Customer
Customer information, etc. confirmation documents
Analog IMS
Financial Institutions

Ongoing Due Diligence (Verification at the time of transaction)

- Customers apply for transactions with financial institutions face-to-face or by mail.
- Financial institutions carry out identity verification based on the evidence.



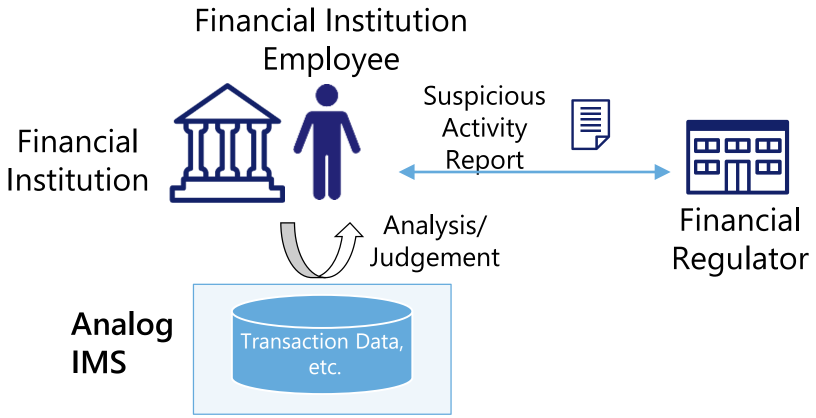
2-1-1. Current Status of Identity Management Operations in Financial Institutions

Identity management operations are still analog centric

■ Carry out analysis and evaluation using own transaction data

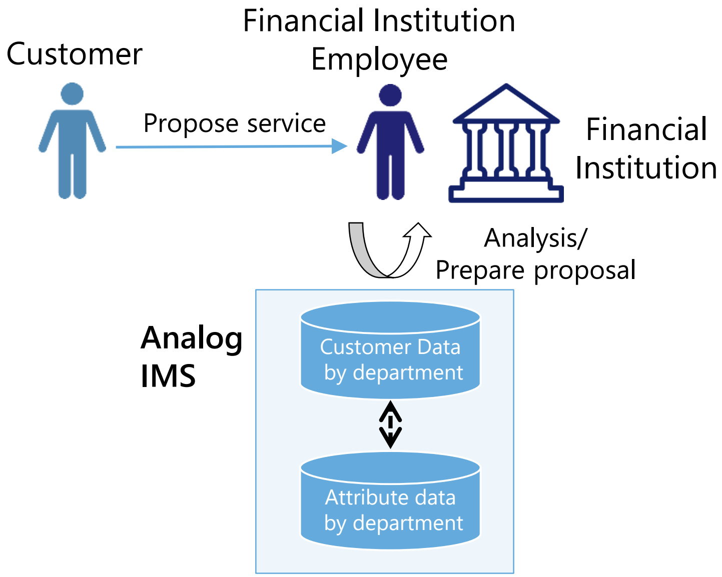
Ongoing Due Diligence (Transaction Monitoring(after))

- Financial institutions detect abnormal transactions from thresholds such as amount, etc. and sanction lists along with tendency of customers to conduct transactions
- Financial institutions scrutinize the details of abnormal transactions detected and re-evaluate customer risk according to the scrutiny results.
- If the detected abnormal transaction is suspected to be a suspicious transaction, the financial institution files a suspicious activity report.



Improve customer service using in-house identity information

- Financial institutions analyze customer attributes and transaction trends and select/ design services suitable for customers.
- Financial institutions propose services to customers.



Customer
Financial Institution Employee
Propose service
Financial Institution
Analysis/ Prepare proposal
Analog IMS
Customer Data by department
Attribute data by department

(1) Account Opening (verification at the time of transaction)
Outline of the issue

- ■ Difficulty of identity verification at financial institutions and administrative burden on customers are main issues.
- ■ The main issues (highlighted in the table below) are described in detail on the following pages (for other issues, please refer to the supplementary document).

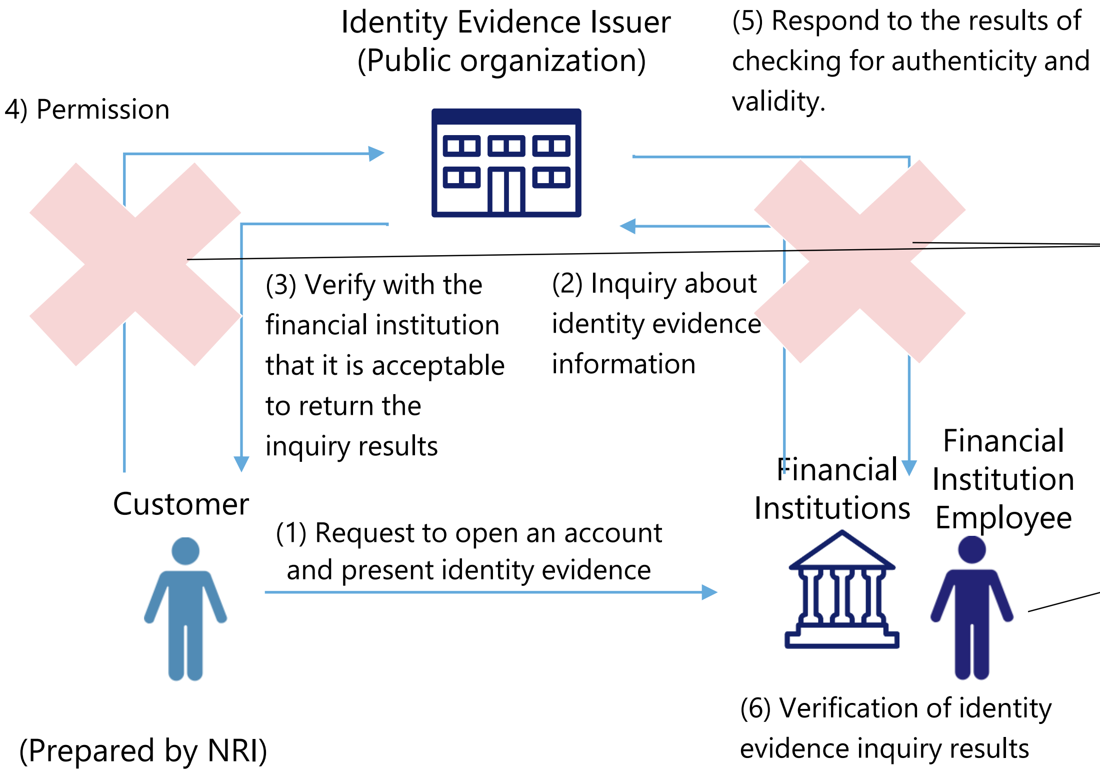
		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of application	• Burden of converting application and evidence information into data	• Financial Inclusion of remote residents in emerging markets • Customer visit burden • Burden of filling out paperwork for customers • Waiting time for customer paperwork • Burden of applying for a similar account at each financial institution.
	Verification at the time of transaction	• Difficulty in verifying the identity evidence of analogs • Operational costs (document storage costs) • Burden of verifying customers who have already been verified by other companies from scratch	
	Customer Filtering	• Burden of verifying customers who have already been verified by other companies from scratch	
	Analysis and evaluation		
	Judgment and response		

2-1-2. Major issues of face-to-face and analog IMS (1) Account Opening (verification at the time of transaction)

[AML/CFT] Difficulty in verifying analog identity evidence

- In practice, financial institutions face two issues: (1) they do not have a mechanism to check and verify the authenticity and validity of identity evidence, and (2) there is a possibility of human errors.
- The mechanism in (1) has not yet been established in Japan. (refer next page)

Flow for verifying the authenticity and validity of identity evidence
(at the time of account opening)



Identity Evidence Issuer
(Public organization)
4) Permission
(5) Respond to the results of checking for authenticity and validity.
(3) Verify with the financial institution that it is acceptable to return the inquiry results
(2) Inquiry about identity evidence information
Customer
(1) Request to open an account and present identity evidence
Financial Institutions
Financial Institution Employee
(6) Verification of identity evidence inquiry results

(1) There is no mechanism to inquire and verify the authenticity and validity of identity evidence.

- There is no mechanism to verify with the identity evidence issuer (public institution) that the content of the identity evidence is correct and that the identity evidence is valid.

(2) Possibility of human errors

- Since falsification of evidence is verified by visual inspection, etc., the possibility of misjudgment due to subjective judgment or insufficient experience of the person in charge cannot be eliminated.

(Prepared by NRI)

2-1-2. Major issues of face-to-face and analog IMS (1) Account Opening (verification at the time of transaction)

Reference: Status of Authenticity and Validity verification of major Japanese Identity Evidence

- Authenticity and validity verification mainly needs to be done manually.
- Although it is functionally possible to verify the authenticity and validity of driver's licenses and My Number cards by using digital evidence (IC chip information, etc.), cost and operational issues have been pointed out in terms of expanding their use in practice.
  - The authenticity of a driver's license can be verified using information stored in the IC chip, and the authenticity and validity of a My Number card can be verified using the public personal authentication system.
  - Regarding practical use of the system, in interviews with domestic financial institutions and experts, opinions were expressed about the challenges in terms of wider use, such as the cost of preparing IC readers and forgetting PINs for reference, etc.

Authenticity and verifiability of identity evidence in Japan

Face-to-face /Non-face-to-face	Evidence	Status of verification of authenticity and validity	
		Authenticity	Effectiveness
Face-to-face	Driver’s license	○*1)	×
	MyNumber card	○	○
	Other certificates	×	×
Non-face-to-face	Paper copy of certificate	×	×
	certificate image	×	×
	Certificate Image + Personal Appearance Photo	○*2)	×
	Driver's license (IC chip readable)	○*1)	×
	MyNumber card (IC chip readable)	○	○*3)

0: Can be referred based on data stored in IC, etc. ×: Judged manually

*1) Article 6, Paragraph 1, Item 1 of the Act on Prevention of Transfer of Criminal Proceeds, etc.

*2) Article 6, Paragraph 1, Item 1 of the Act on Prevention of Transfer of Criminal Proceeds, etc.

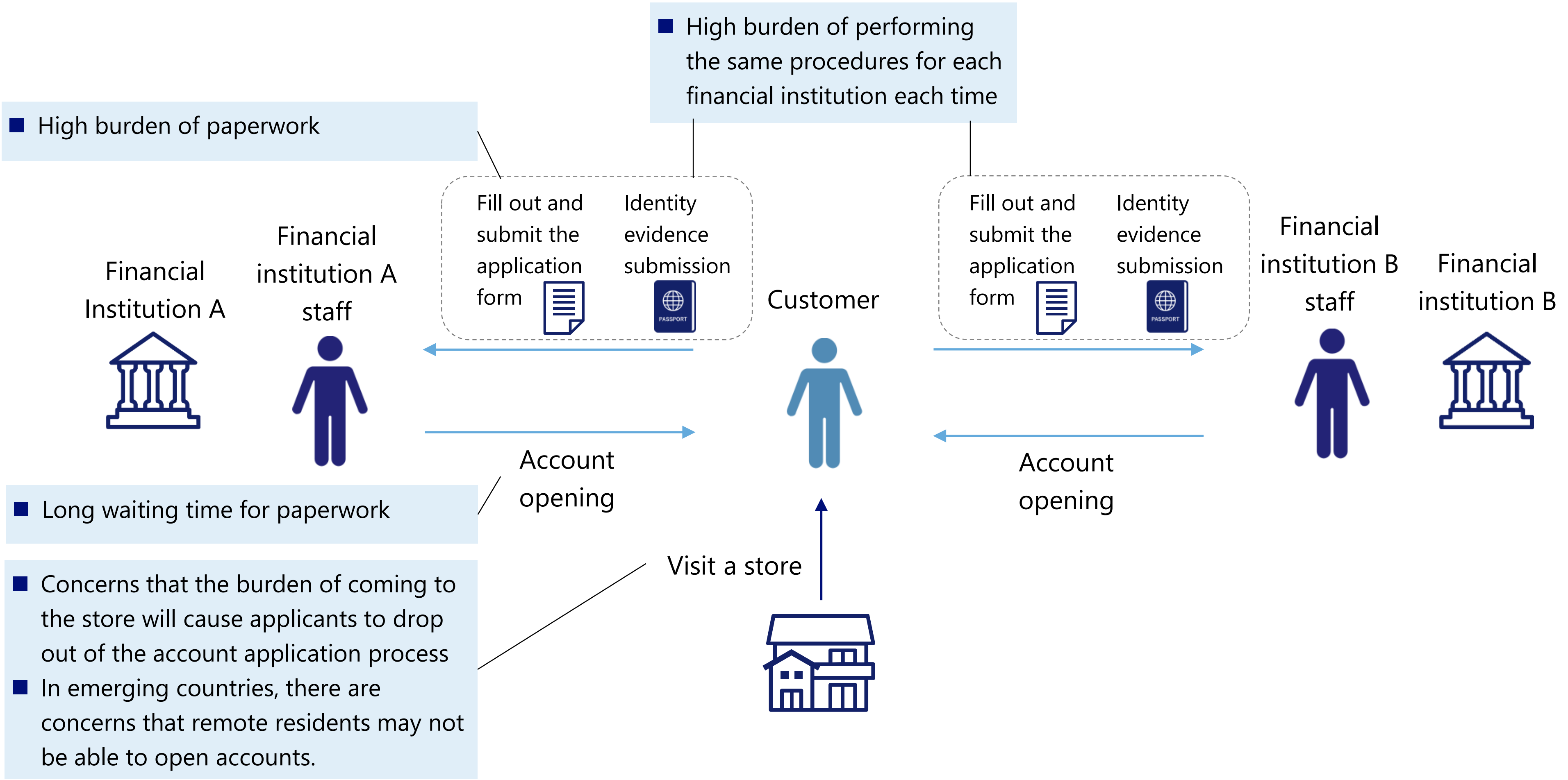
*3) Within identity verification using the My Number Card, the electronic certificate for signature for public personal authentication recorded on the IC chip is used.

2-1-2. Major issues of face-to-face and analog IMS (1)Account Opening (verification at the time of transaction)

[Service Improvement] Various issues in customer related procedures caused by analog exchange of information

- There are various procedural burdens for customers, such as visiting stores and filling out forms, etc.

<u>Main challenges for customers in opening accounts face-to-face and analog IMS</u>



- High burden of performing the same procedures for each financial institution each time

- High burden of paperwork

- Long waiting time for paperwork

- Concerns that the burden of coming to the store will cause applicants to drop out of the account application process
- In emerging countries, there are concerns that remote residents may not be able to open accounts.

Financial Institution A
Financial institution A staff
Fill out and submit the application form
Identity evidence submission
PASSPORT
Customer
Fill out and submit the application form
Identity evidence submission
PASSPORT
Financial institution B staff
Financial institution B
Account opening
Account opening
Visit a store

	onboarding	ongoing
AML	①Account Opening	②Ongoing Due Diligence
Service		③Provide service

2-1-3. Major issues of face-to-face and analog IMS (2) Ongoing Due Diligence

Ongoing Due Diligence
Overview of Issues

- ■ Administrative burden of AML/CFT on financial institutions and customers.
- ■ Main issues (highlighted in the table below) are described in detail on the following pages (for other issues, please refer to the supplementary document).

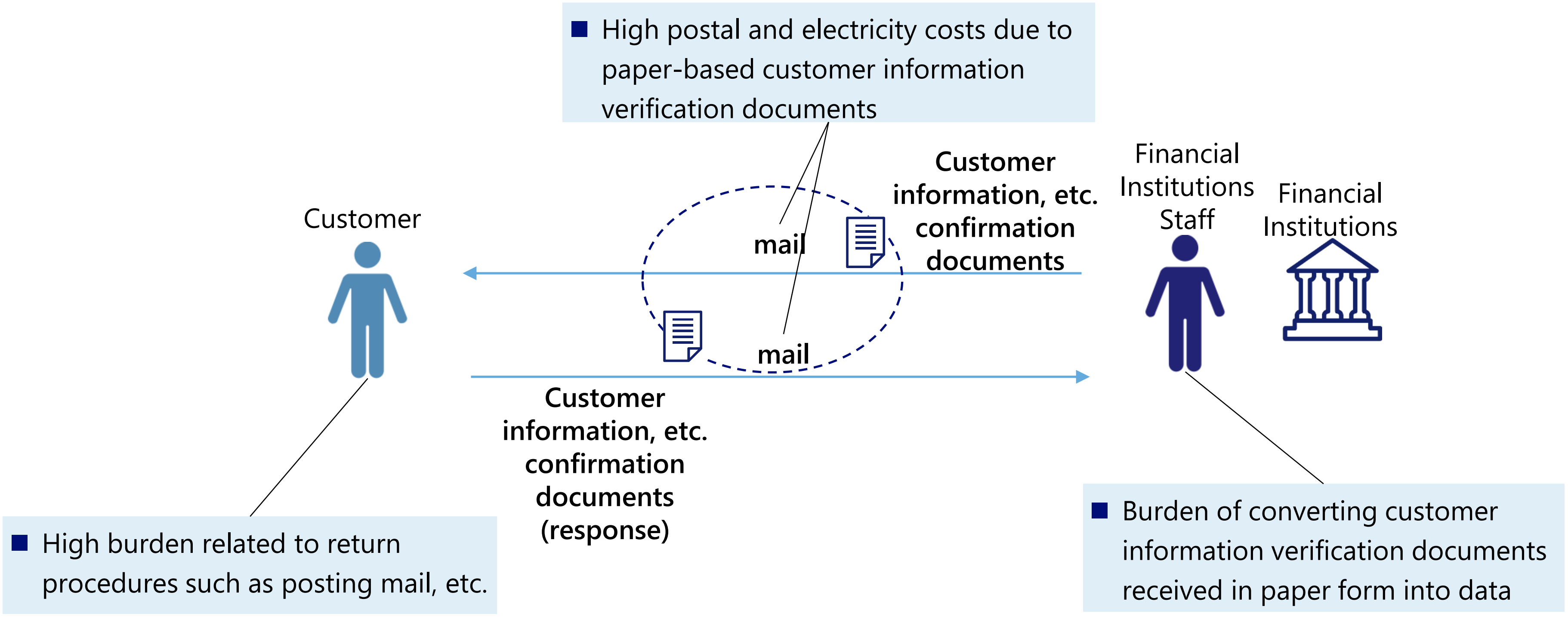
		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of Application	• Burden of converting transaction applicati document into data. B	• Burden of return postage A
	Verification at the time of transaction	• Administrative verification burden for a lar number of customers A	• Security risks during transactions B (e.g. password theft during non-face-to-face access,etc.)
	Customer Filtering		
	Analysis and evaluation	• Burden of analog customer information collection postal and electric costs and data conversion A	Legend A Periodic Customer Information Collection B Verification upon receipt of transaction
	Judgment and response		

2-1-3. Major issues of face-to-face and analog IMS (2) Ongoing Due Diligence

Issues coming up from analog IMS in Periodic Customer Information Collection

- In Periodic Customer Information Collection, there are issues of administrative and cost burden due to written exchanges between customers and financial institutions.

Issues in Periodic Customer Information Collection



- High postal and electricity costs due to paper-based customer information verification documents

- High burden related to return procedures such as posting mail, etc.

- Burden of converting customer information verification documents received in paper form into data

Customer
mail
Customer information, etc. confirmation documents
Financial Institutions Staff
Financial Institutions
mail
Customer information, etc. confirmation documents (response)

(3) Provide services using identity information
Overview of the issue

- There are issues related to aggregation of data for data utilization. This will be discussed in detail on the next page.

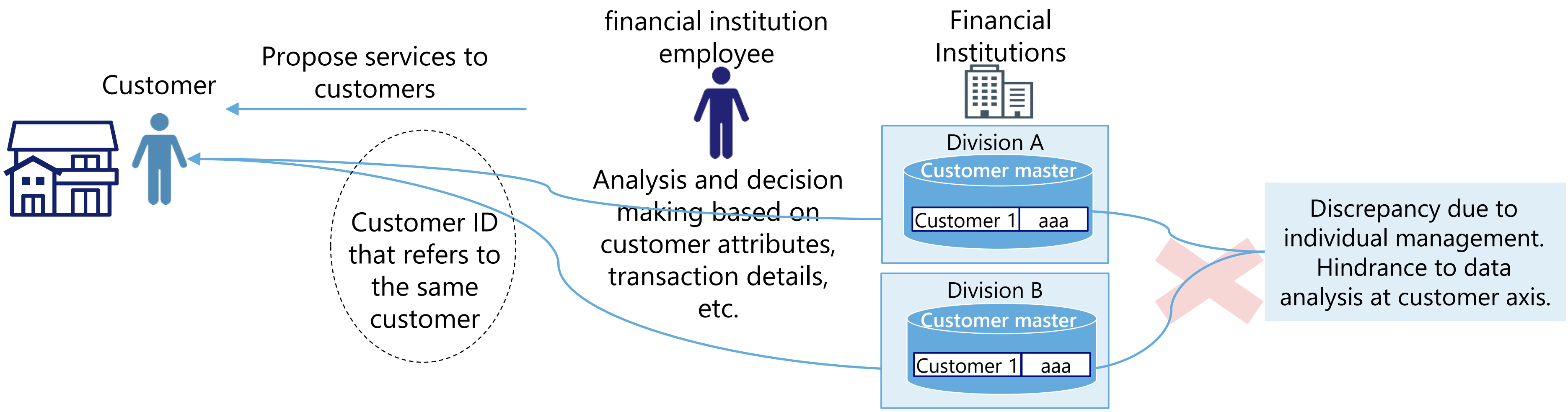
		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of Application		
	Verification at the time of transaction		
	Customer Filtering		
	Analysis and evaluation	• Burden of data consent management in order to utilize customer data across multiple services	• Data aggregation is difficult due to identifier mismatch – Customer identifier mismatch due to management by department/organization – Customer identifier mismatch with data of other companies • Data aggregation is difficult due to inconsistent data formats inside and outside the company • Increased risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization
	Judgment and response		

2-1-4. Major issues of face-to-face and analog IMS (3) Provide services using identity information

Service improvement: Difficulty in utilizing data due to inconsistent customer identifiers and data format within the company

- Regarding information analysis operations in financial institutions, several literatures have pointed out issues related to partial optimization of data.
  - Since the accounting management of banks was based on a vertical divisional axis, huge number of operations managed by each business division and product led to the partial optimization of master data, making it difficult to manage the data horizontally. This has been pointed out by practitioners of domestic financial institution[*1)].
  - There are no rules for data design, and each system has a different code structure and granularity, making it burdensome and costly to ensure uniformity in the data structure, and thus unable to provide useful data for analysis. This has been pointed out by experts. [*2)]
- When internal data is partially optimized, customer identifiers and data format may differ from department to department or system to system. Issue occurs where analysis of cross-sectional data on the customer axis for service improvement cannot be done sufficiently
- Permission of data usage of customers need to be taken based on each service such as when explaining the purpose of usage each time a contract is made. In such cases, it may be required to verify the data usage permissions for cross-sectional analysis on the customer axis. Moreover, due to insufficient explanation to the customer at that time, the customer may be concerned about data utilization which the customer might not want.

Inconsistency of customer identifiers in data management



Customer

Propose services to customers

financial institution employee

Analysis and decision making based on customer attributes, transaction details, etc.

Financial Institutions

Division A

Customer master

Customer 1 | aaa

Division B

Customer master

Customer 1 | aaa

Customer ID that refers to the same customer

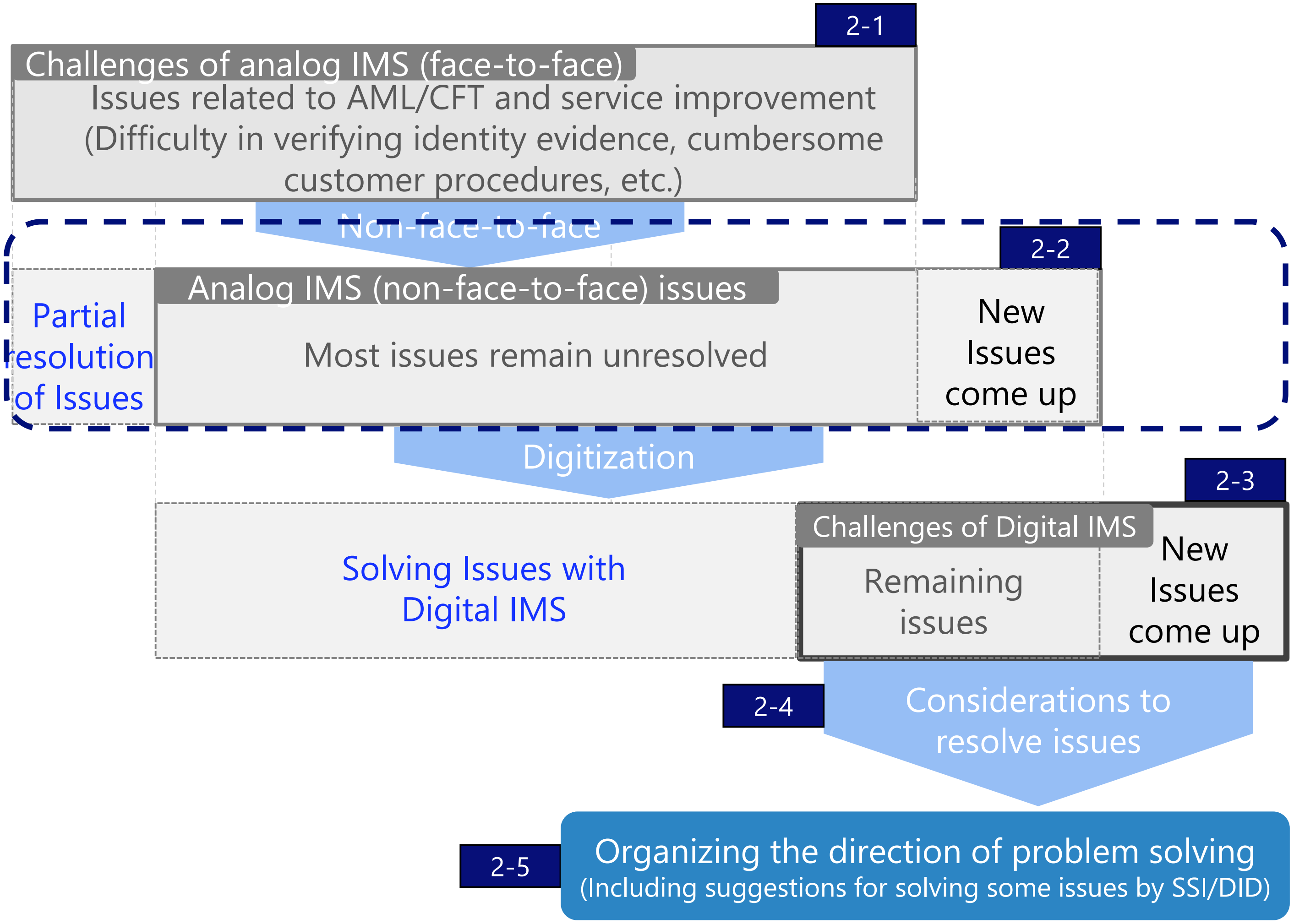
Discrepancy due to individual management. Hindrance to data analysis at customer axis.

*1) Excerpts from FINANCE FORUM, Data Utilization Practices Required for Financial Institutions https://thefinance.jp/event/finance-forum-200528

*2) Advanced Data-Based Decision Making in Financial Institutions, 2016 https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/jp-fi-data-utilization.pdf

2-2. Progress of non-face-to-face Onboarding Process

Subject of discussion in this section



2-1

Challenges of analog IMS (face-to-face)

Issues related to AML/CFT and service improvement (Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)

Non-face-to-face

2-2

Partial resolution of Issues

Analog IMS (non-face-to-face) issues

Most issues remain unresolved

New Issues come up

Digitization

2-3

Solving Issues with Digital IMS

Challenges of Digital IMS

Remaining issues

New Issues come up

2-4

Considerations to resolve issues

2-5

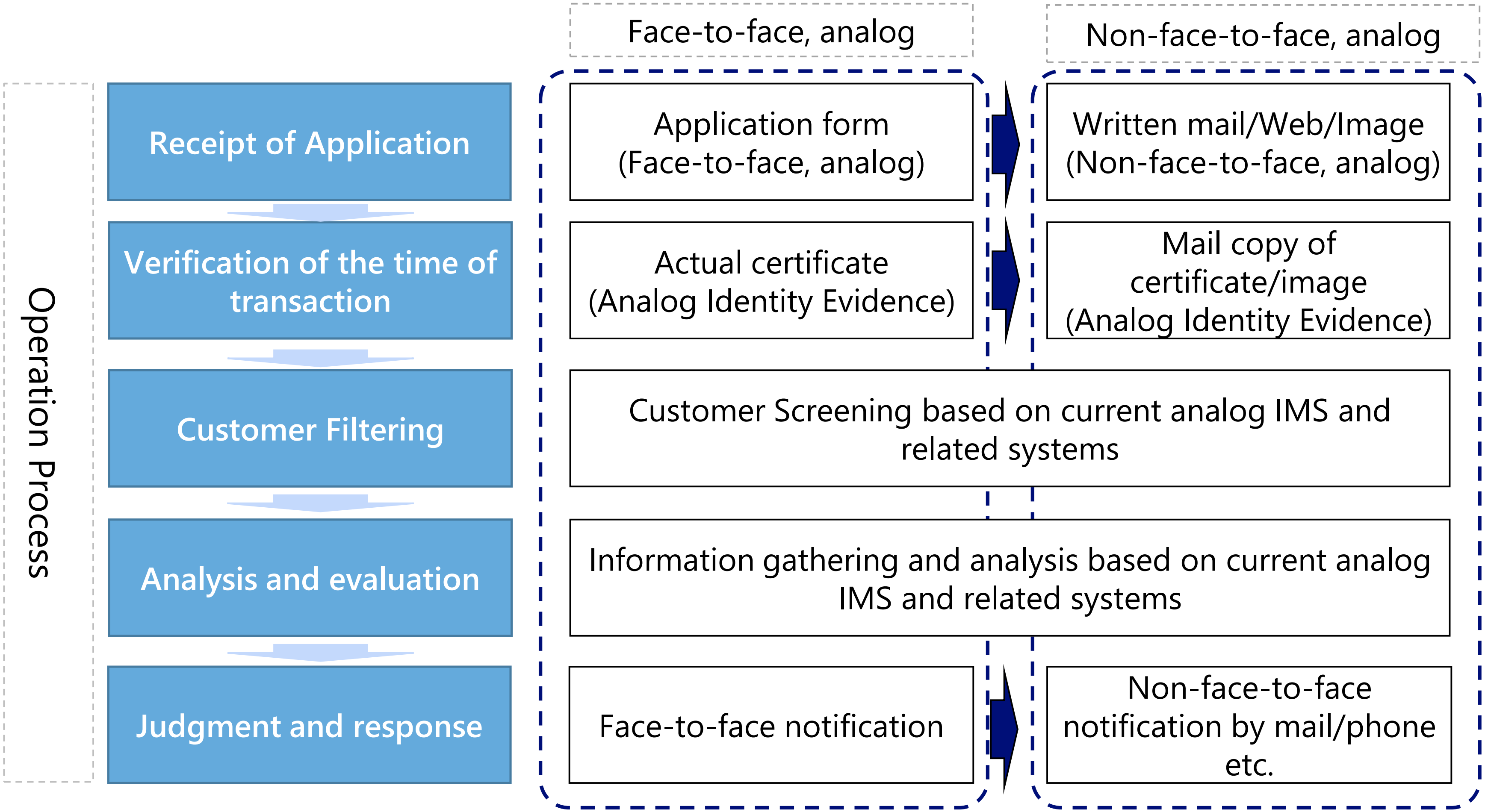
Organizing the direction of problem solving (Including suggestions for solving some issues by SSI/DID)

2-2-1. Progress of non-face-to-face Onboarding Process

Progress of non-face-to-face Onboarding Process

- With the development of identity verification regulations for remote onboarding such as eKYC,etc. and the expansion of solutions provided by private vendors, non-face-to-face transactions issues are getting resolved

Change in Operation Process due to non-face-to-face transactions



Operation Process	Face-to-face, analog	Non-face-to-face, analog
Receipt of Application	Application form (Face-to-face, analog)	Written mail/Web/Image (Non-face-to-face, analog)
Verification of the time of transaction	Actual certificate (Analog Identity Evidence)	Mail copy of certificate/image (Analog Identity Evidence)
Customer Filtering	Customer Screening based on current analog IMS and related systems	
Analysis and evaluation	Information gathering and analysis based on current analog IMS and related systems	
Judgment and response	Face-to-face notification	Non-face-to-face notification by mail/phone etc.

2-2-2. Partial resolution of issues through non-face-to-face interaction

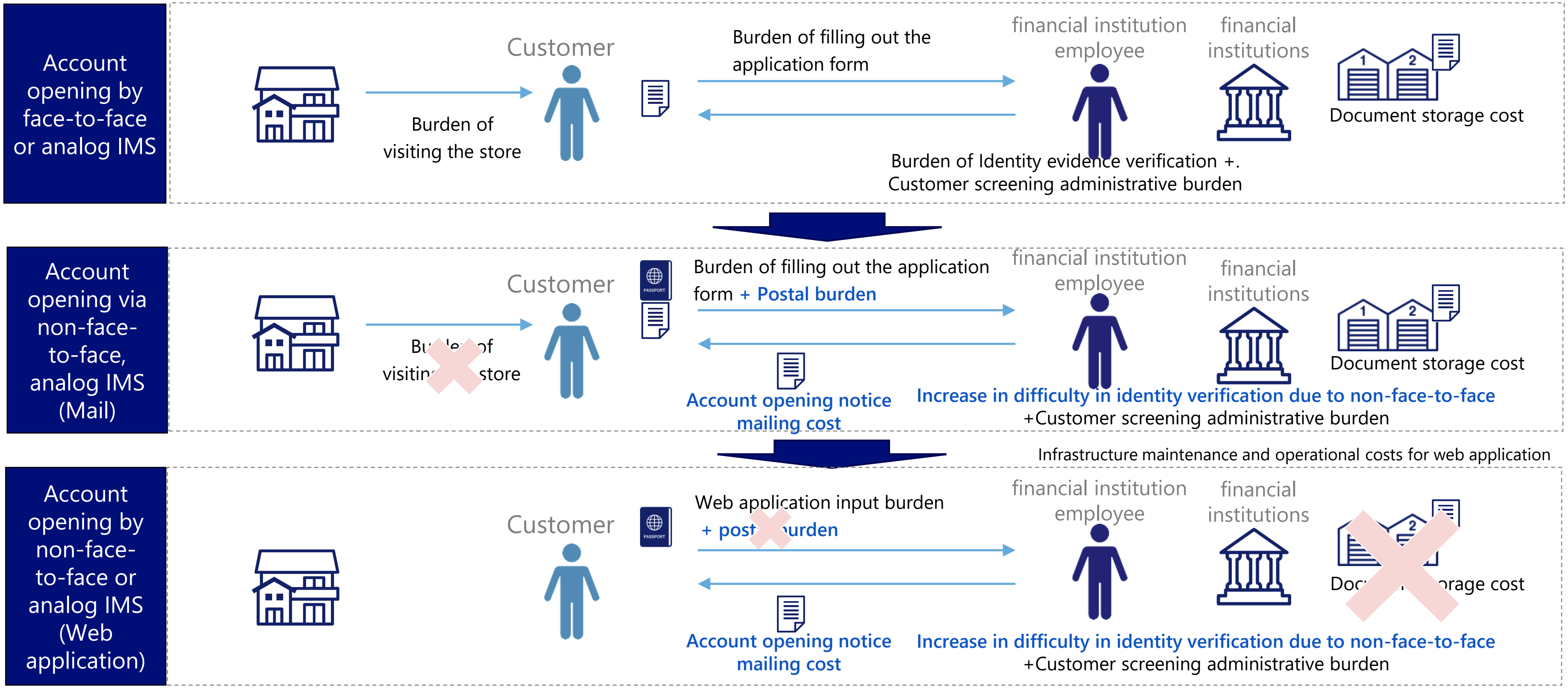
Partial resolution of face-to-face and analog IMS issues through non-face-to-face interaction

- Some administrative burdens for customers and financial institutions will get reduced, however, new issues will come up such as increase in difficulty level of verifying the identity of customers will increase due to the shift to non-face-to-face interaction and new costs will get incurred for mail notification of account opening to verify the location of the customer along with infrastructure maintenance and operational costs for web application (only when providing web application)

✕ : Issues to be resolved

Blue : New issues that come up with the shift to non-face-to-face

Partial resolution of issues of face-to-face and Analog IMS due to non-face-to-face interaction



Account opening by face-to-face or analog IMS
Customer
Burden of visiting the store
Burden of filling out the application form
financial institution employee
financial institutions
Document storage cost
1
2
Burden of Identity evidence verification +. Customer screening administrative burden
Account opening via non-face-to-face, analog IMS (Mail)
Customer
Bu le of visitin store
Burden of filling out the application form + Postal burden
PASSPORT
financial institution employee
financial institutions
Document storage cost
Account opening notice mailing cost
Increase in difficulty in identity verification due to non-face-to-face
+Customer screening administrative burden
Infrastructure maintenance and operational costs for web application
Account opening by non-face-to-face or analog IMS (Web application)
Customer
Web application input burden
+ post urden
PASSPORT
financial institution employee
financial institutions
Doc orage cost
Account opening notice mailing cost
Increase in difficulty in identity verification due to non-face-to-face
+Customer screening administrative burden

2-2-3. issues that remain even after shifting to non-face-to-face interaction

Issues that remain even after shifting to non-face-to-face interaction

- Even after the shift to non-face-to-face transactions, issues other than the administrative burden on customers and document storage costs for financial institutions will remain unresolved. In addition, new issues come up, such as increase in difficulty in verifying the identity of customers.
- The main issues (highlighted parts in the table below) will be described in detail in the following pages (refer to supplementary document for other issues).

Remarks
~~Character~~: Face-to-face and analog IMS issues eliminated by non-face-to-face interaction
Blue letters: New issues coming up due to non-face-to-face interaction

Operation Process	Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Receipt of Application	• Burden of converting ~~application information and~~ evidence information into data. • Infrastructure maintenance and operational costs for web application	~~• Financial Inclusion of Remote Residents in Emerging Markets~~ ~~• Burden to customers to visit shops~~ ~~• Burden to customers to fill out forms~~ → Burden to apply on Web ~~• Waiting time while administrative work gets completed~~ • Burden of applying for a similar account at each financial institution.
Verification at the time of transaction	• Difficulty in verifying analog identity evidence ~~• Operational costs (document storage costs)~~ • Burden of verifying customers who have already been verified by other companies from scratch • Increasing difficulty in verifying identity with the shift to non-face-to-face interaction	
Customer Filtering	• Burden of verifying customers who have already been verified by other companies from scratch	
Analysis and Evaluation		
Judgment and response	• Mailing cost to notify opening of an account to verify location	

2-2-4. New issues coming up due to non-face-to-face interaction

[AML/CFT] Increasing difficulty of identity verification due to non-face-to-face interaction

- Compared to face-to-face transactions, non-face-to-face transactions carry the risk that the accuracy of identity verification will decrease because the means by which financial institutions detect impersonation of others is limited.
  - By not facing the other party of the transaction directly, identity verification will be conducted without verifying gender, age, appearance, behavior, etc. that gets easily verified in case of face-to-face interaction. As a result, it becomes difficult to determine whether the person's identification is false or impersonated by another person.
  - In addition, it tends to be difficult to recognize forgery of evidence, authenticity of customer, etc. When verifying the identity by copying the evidence, touch and quality cannot be detected.

- In non-face-to-face onboarding operation, it is difficult to reduce the risk as long as analog IMS is used, which cannot sufficiently verify the authenticity and validity of identity evidence. It should be noted that there are risks posed and it might get expanded due to non-face-to-face interaction.

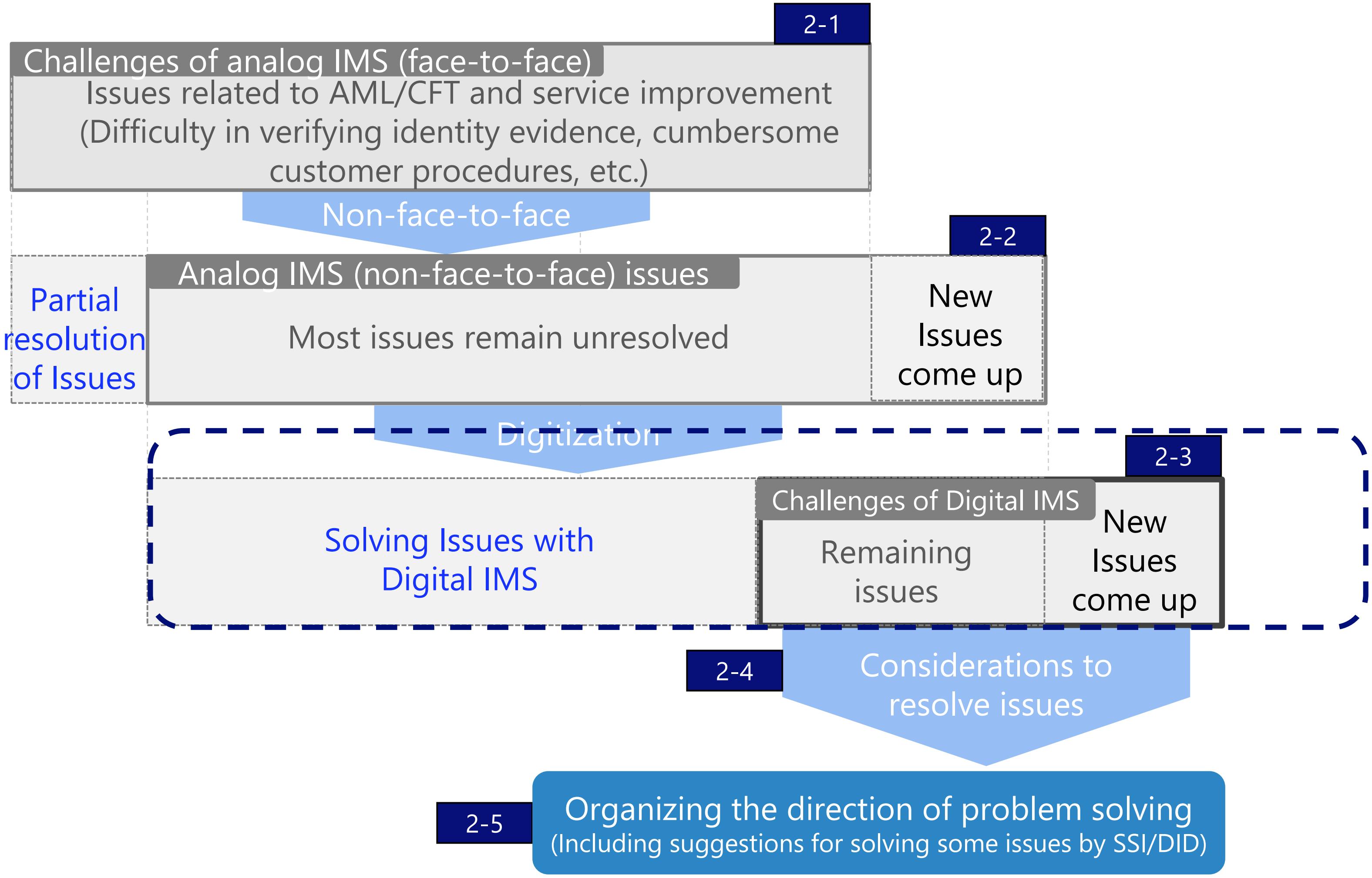
- For this reason, financial institutions generally tend to recognize that non-face-to-face transactions are more risky than face-to-face transactions. Risk Assessment of Money Laundering and Terrorist Financing *1) also mentions non-face-to-face transactions as one of the high-risk transactions.

*1) National Risk Assessment of Money Laundering and Terrorist Financing, Nov 2020 https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk021105.pdf

2-3. Possibility of using digital IMS

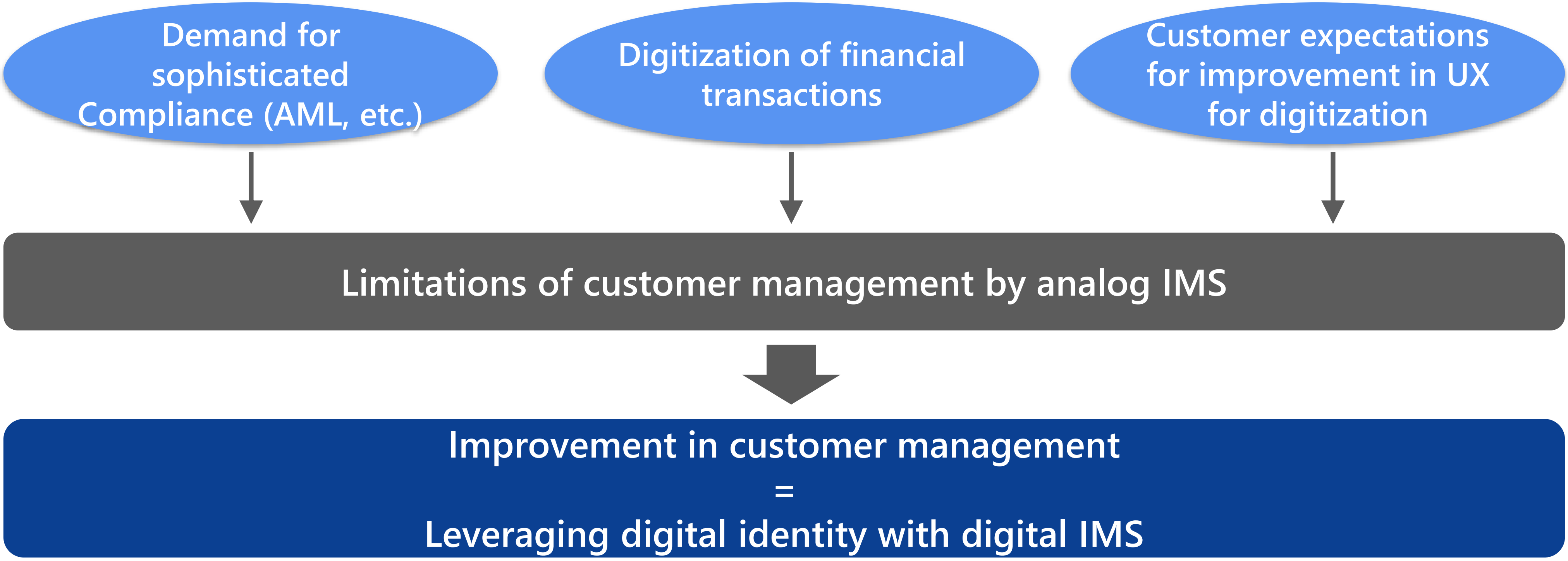
2-3. Possibility of using digital IMS

Subject of discussion in this section


2-1
Challenges of analog IMS (face-to-face)
Issues related to AML/CFT and service improvement (Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)
Non-face-to-face
2-2
Analog IMS (non-face-to-face) issues
Partial resolution of Issues
Most issues remain unresolved
New Issues come up
Digitization
2-3
Solving Issues with Digital IMS
Challenges of Digital IMS
Remaining issues
New Issues come up
2-4
Considerations to resolve issues
2-5
Organizing the direction of problem solving
(Including suggestions for solving some issues by SSI/DID)

Importance of Using Digital Identity in Financial Institutions

- In the backdrop of corona, shift in digitization has accelerated in the society along with acceleration in digitization of financial transactions. It is becoming more and more important to verify identity in the digital space from the perspective of AML and other compliances.
- In order to conduct various procedures digitally, UX is gradually gaining popularity in the financial sector and customer expectations towards digitization are increasing.
- The use of digital IMS is expected to solve the analog IMS issues faced by financial institutions, as summarized in the previous section.



Demand for sophisticated Compliance (AML, etc.)

Digitization of financial transactions

Customer expectations for improvement in UX for digitization

Limitations of customer management by analog IMS

Improvement in customer management
=
Leveraging digital identity with digital IMS

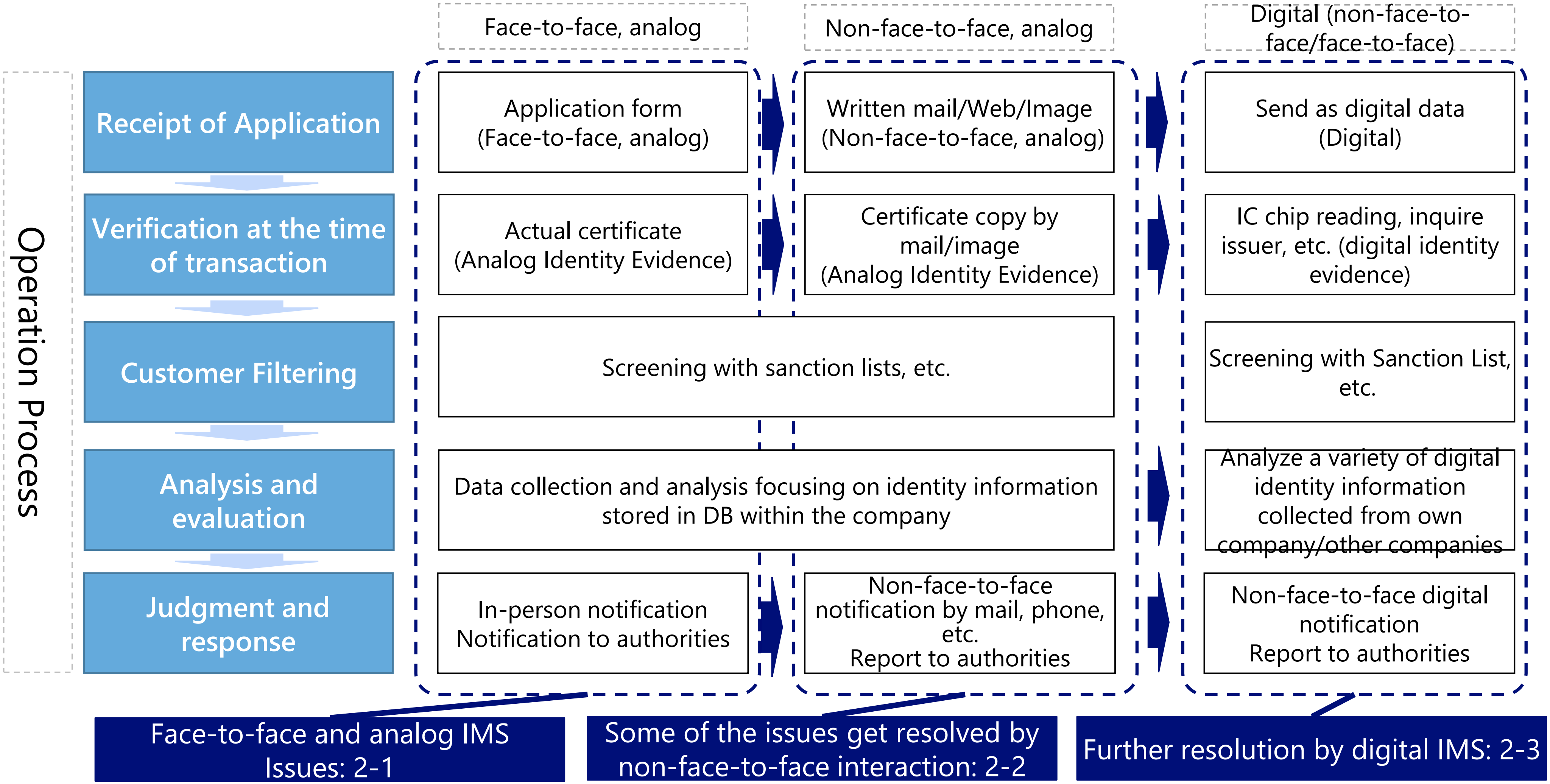
	onboarding	ongoing
AML	①Account Opening	②Ongoing Due Diligence
Service		③Provide service

2-3-1. Importance of Using Digital Identity in Financial Institutions

Digitization of IMS

- Digitization of IMS: Digitizing the interaction of identity information (e.g., linking identity evidence in machine-readable format).

Changes in IMS operation process due to digitization



Operation Process	Face-to-face, analog	Non-face-to-face, analog	Digital (non-face-to-face/face-to-face)
Receipt of Application	Application form (Face-to-face, analog)	Written mail/Web/Image (Non-face-to-face, analog)	Send as digital data (Digital)
Verification at the time of transaction	Actual certificate (Analog Identity Evidence)	Certificate copy by mail/image (Analog Identity Evidence)	IC chip reading, inquire issuer, etc. (digital identity evidence)
Customer Filtering	Screening with sanction lists, etc.		Screening with Sanction List, etc.
Analysis and evaluation	Data collection and analysis focusing on identity information stored in DB within the company		Analyze a variety of digital identity information collected from own company/other companies
Judgment and response	In-person notification Notification to authorities	Non-face-to-face notification by mail, phone, etc. Report to authorities	Non-face-to-face digital notification Report to authorities

Face-to-face and analog IMS Issues: 2-1

Some of the issues get resolved by non-face-to-face interaction: 2-2

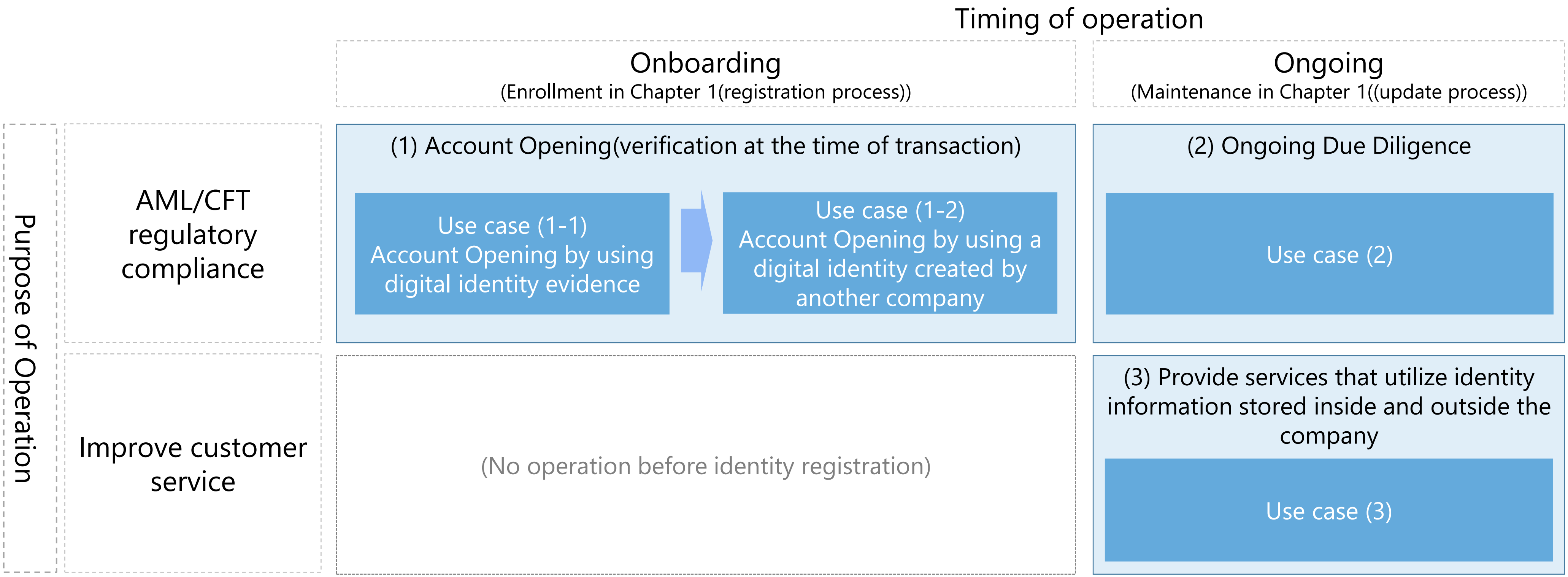
Further resolution by digital IMS: 2-3

2-3-2. Use cases to be analyzed

Use cases to be analyzed

- Set use cases as per classification in 2-1-1 and conduct analysis.
- Assuming that there will be progress in ID linkage at the time of account opening, onboarding process will be analyzed in two patterns: (1-1) using digital evidence and (1-2) not using evidence but using digital identities already created by other companies,.

Positioning of use cases for analysis



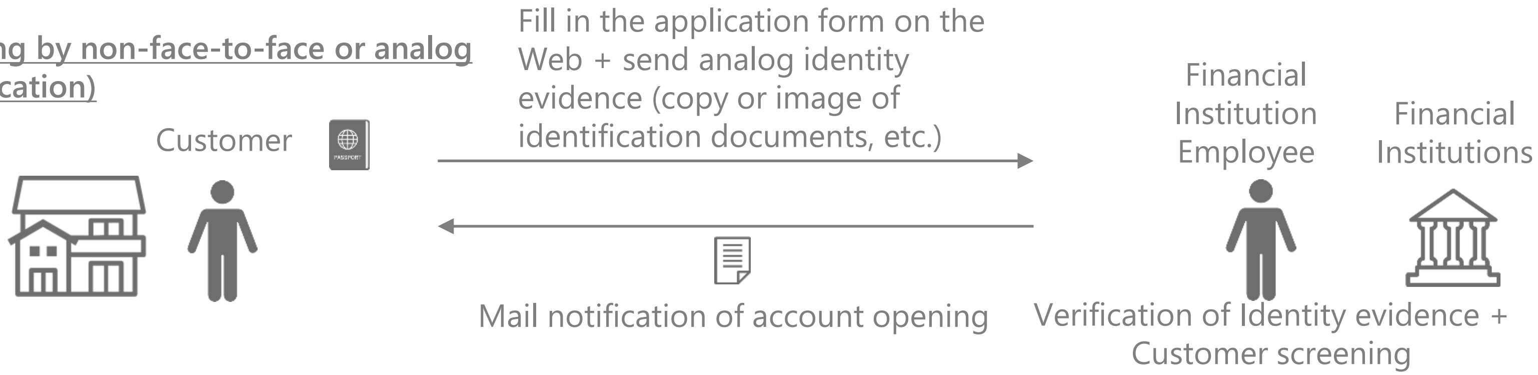
Timing of operation
Onboarding
(Enrollment in Chapter 1(registration process))
Ongoing
(Maintenance in Chapter 1((update process))
Purpose of Operation
AML/CFT regulatory compliance
(1) Account Opening(verification at the time of transaction)
Use case (1-1) Account Opening by using digital identity evidence
Use case (1-2) Account Opening by using a digital identity created by another company
(2) Ongoing Due Diligence
Use case (2)
Improve customer service
(No operation before identity registration)
(3) Provide services that utilize identity information stored inside and outside the company
Use case (3)

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Use Case Overview

- Open an account by verifying your identity using machine-readable and digitally verifiable identity evidence.

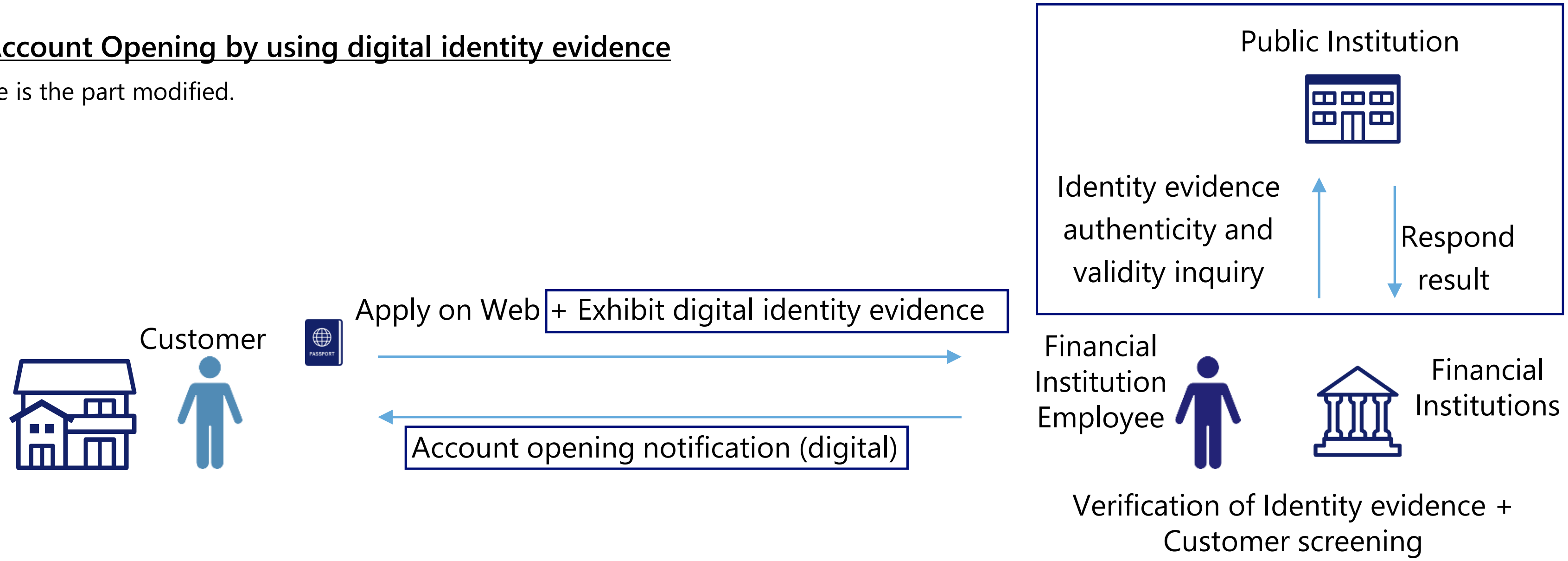
Account Opening by non-face-to-face or analog IMS (Web application)



Customer
Fill in the application form on the Web + send analog identity evidence (copy or image of identification documents, etc.)
Financial Institution Employee
Financial Institutions
Mail notification of account opening
Verification of Identity evidence + Customer screening

Use Case (1-1) Account Opening by using digital identity evidence

*The blue frame is the part modified.



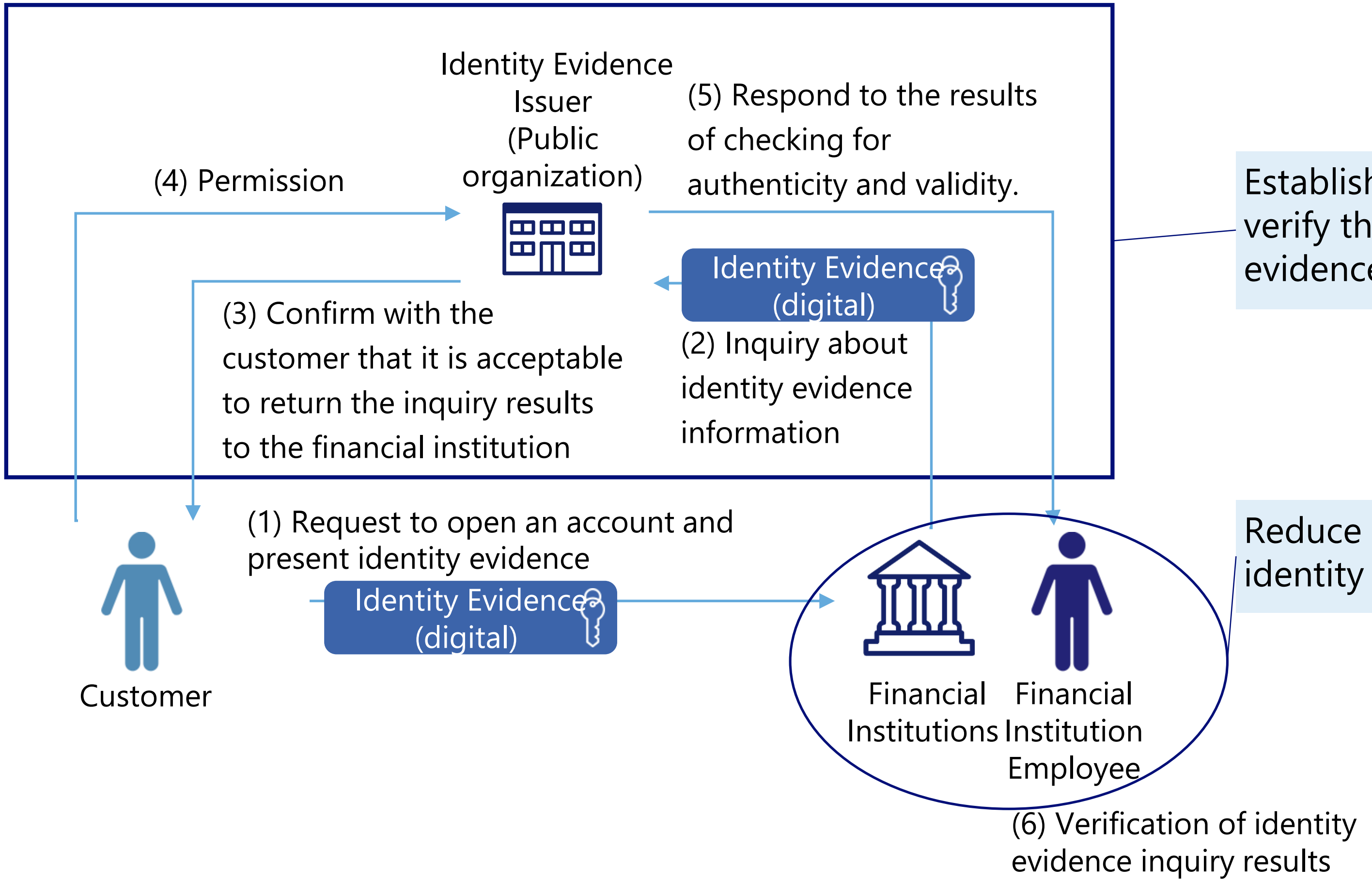
Public Institution
Identity evidence authenticity and validity inquiry
Respond result
Customer
Apply on Web
+ Exhibit digital identity evidence
Account opening notification (digital)
Financial Institution Employee
Financial Institutions
Verification of Identity evidence + Customer screening

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Solving issues with digital IMS: Eliminating the difficulty of verifying analog identity evidence

- The use of machine-readable, digitally verifiable identity evidence can eliminate the difficulty of verifying identity evidence and other issues related to analog IMS.

Flow of verifying authenticity and validity of identity evidence in digital IMS (When opening an account)



Identity Evidence Issuer (Public organization)
(4) Permission
(5) Respond to the results of checking for authenticity and validity.
Identity Evidence (digital)
(3) Confirm with the customer that it is acceptable to return the inquiry results to the financial institution
(2) Inquiry about identity evidence information
(1) Request to open an account and present identity evidence
Identity Evidence (digital)
Customer
Financial Institutions
Financial Institution Employee
(6) Verification of identity evidence inquiry results

Establish a mechanism to query and verify the accuracy of identity evidence.

Reduce human error by digitizing identity evidence inquiry operation

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Solving problems with digital IMS: Solving other problems with analog IMS

Challenges in opening accounts in analog IMS	Solutions by Digital IMS
Increasing difficulty in identity verification due to non-face-to-face interaction Compared to face-to-face transactions, non-face-to-face transactions have limited means of detecting impersonation of others, and there is a risk of reduction in accuracy of identity verification	• Authentication and validation by Digital IMS can reduce the risk of spoofing due to evidence tampering. • By combining biometric information, accuracy of verifying that the identity evidence presented is that of the person who applied to open an account can get improved, reducing the risk of identity theft.
Mailing cost of notification of opening an account for verification of address At the time of opening a non-face-to-face account, a mail which cannot be re-send, is sent to verify the address of the account applicant, which results in high mailing cost	• When using national IDs as digital identity evidence, eliminate the need for postal verification by establishing a system to promptly capture updates to national IDs assuming the address of national ID to be correct. • Eliminate the need for postal confirmation by establishing a system that verifies the reported address by referring to the customer's location information at the time of transaction.

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Issues that will be eliminated by shifting to digital IMS for account opening and new issues that will come up

- Sophistication of regulatory compliance such as AML and labor saving for financial institutions in account opening applications
- On the other hand, new issues will come up, such as development of identification methods using digital IMS. The main issues (highlighted in the table below) are described in detail on the following pages (for other issues, please refer to the supplementary document).

Summary of issues that will be eliminated by shifting to digital IMS for account opening and new issues that will come up

Remarks
~~Black:~~ Analog IMS issues to be solved by digital IMS
Black: Identity management issues difficult to solve even with digital IMS
Blue letters: New issues coming up from the use of digital IMS

		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of Application	• ~~Burden of converting evidence information into data~~ • Infrastructure maintenance and operational costs for web application	• Burden to apply on Web • Burden of applying for a similar account at each financial institution. • Financial exclusion of people who are not digitally compatible
	Verification at time of transaction	• ~~Difficulty in verifying analog identity evidence~~ • Burden of verifying customers who have already been verified by other companies from scratch • ~~Increasing difficulty in verifying identity due to non-face-to-face interaction~~ • Develop a regulatory framework to promote appropriate use of digital IMS • Difficult to make investment decision with regards to the change in existing optimized operations to use digital IMS	• Respond to new security risks, such as the opening of accounts in a chain.
	Customer Filtering	• Burden of checking customers who have already been verified by other companies from scratch	
	Analysis and evaluation		
	Judgment and response	• ~~Mailing cost to notify opening of an account to verify location~~	

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Issue Development of a regulatory framework that encourages the appropriate use of digital IMS (1/2)

- In order to ensure that the IAL (Identity Assurance Level) is suitable for regulatory purposes, the FATF has proposed the following as criteria for adopting or rejecting a digital IMS.

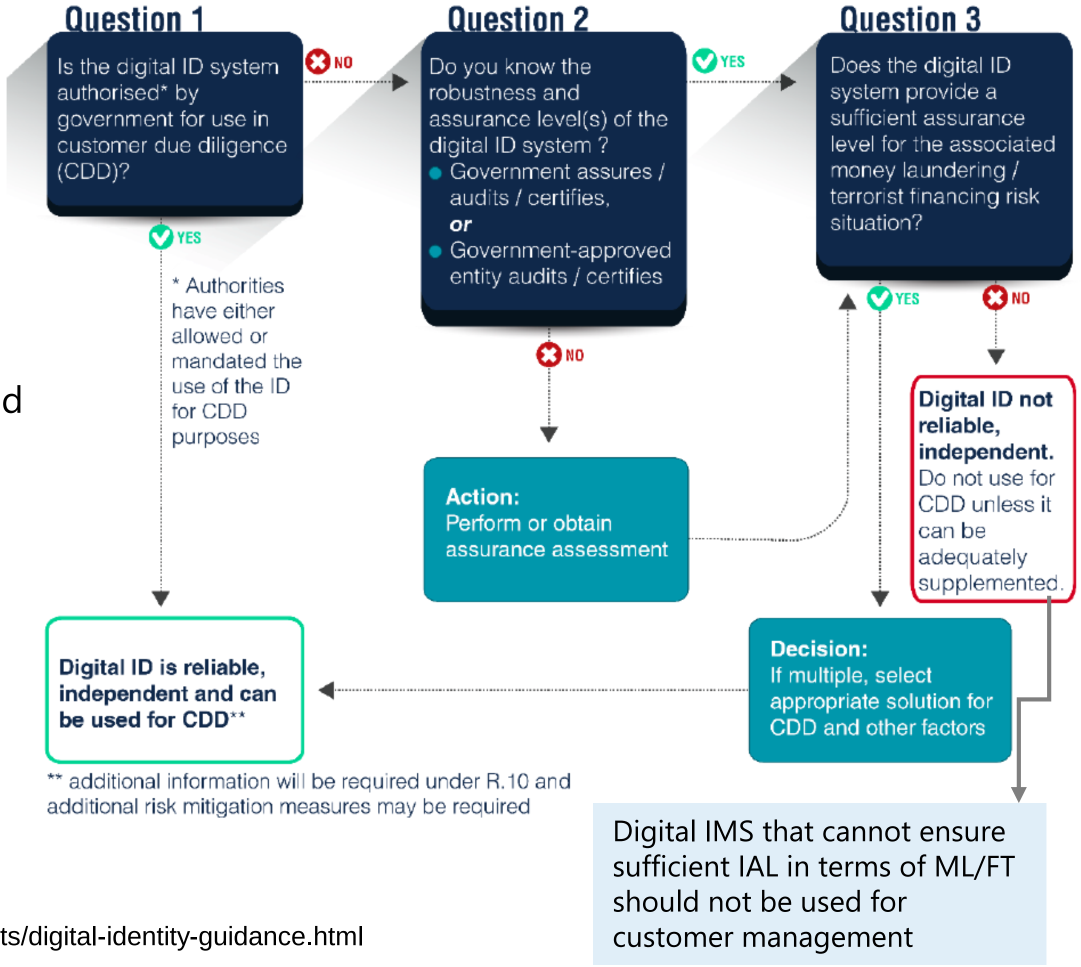
  (1) Those authorized by the government for use in customer management.

  or

  (2) Those whose robustness and IAL are guaranteed or audited by the government or a government-approved body, and which provide sufficient IAL from an AML/CFT perspective.

- In addition, FATF highlights the benefits of a risk-based approach under digital IMS where appropriate IAL is secured, which will contribute to the advancement of AML/CFT and financial inclusion.
  - Even non-face-to-face transactions, which are generally classified as high-risk, may have a standard or low-risk level of risk if they rely on an appropriate digital IMS[*1] .

Decision-making process[*1] for adopting or rejecting digital IMS for AML/CFT purpose as advocated by FATF



Question 1
Is the digital ID system authorised* by government for use in customer due diligence (CDD)?
NO
YES
* Authorities have either allowed or mandated the use of the ID for CDD purposes
Question 2
Do you know the robustness and assurance level(s) of the digital ID system ?
Government assures / audits / certifies,
or
Government-approved entity audits / certifies
YES
NO
Action:
Perform or obtain assurance assessment
Question 3
Does the digital ID system provide a sufficient assurance level for the associated money laundering / terrorist financing risk situation?
YES
NO
Digital ID not reliable, independent.
Do not use for CDD unless it can be adequately supplemented.
Decision:
If multiple, select appropriate solution for CDD and other factors
Digital ID is reliable, independent and can be used for CDD**
** additional information will be required under R.10 and additional risk mitigation measures may be required
Digital IMS that cannot ensure sufficient IAL in terms of ML/FT should not be used for customer management

[*1] GUIDANCE ON DIGITAL IDENTITY(Mar 2020)
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

Issue Development of a regulatory framework that encourages the appropriate use of digital IMS (2/2)

- It is important to integrate IAL and identity verification rules for the proper maintenance of the IAL. But currently, except in the EU (Germany) where eID is recommended, there is no linkage between identity verification rules and identity assurance frameworks.
- Singapore has essentially standardized the level of identity assurance by unifying the use of government IDs.
- In EU, the use of eID for on boarding is being considered, and discussions are underway on the assumption that both technology and governance in the financial sector will comply with eIDAS regulations

	Japan	America	The United Kingdom	Germany	Singapore	New Zealand
Basis of Regulations	The Act on Prevention of Transfer of Criminal Proceeds stipulates the method of identification.	Patriot Act specifies how to verify identity at the federal level; state laws follow it	POCA overview will be the basic law and it will be mentioned in detail in Government Digital Services Guidance, etc..	Money Laundering Act (GwG) provides general principles, details are provided in separate law.	Defined in the Money Laundering and Antiterrorism Act	Specified in Identification Management Standards
Face-to-face verification of identity	In principle, use official certificate with a photograph					Standard specified for each type of business, and if any combination meets the standard, it is okay
Non-face-to-face Identity verification Special example	Video call and verification with official certificates are also possible.	Requested to be determined by the financial institution	No provision for non-face-to-face verification	Detailed regulations on how to verify on the video call	List alternatives for non-face-to-face situations	No need for additional measures even for non-face-to-face in business categories where the required standard is low.
Linkage with Identity Assurance Framework (IAL)	nil	nil	nil (Good Practice Guide 45 links eIDAS, but no guideline yet)	GwG interpretation note stipulates eIDAS compliance	nil	nil
(Reference) National identification number system	Yes (my number※)	Partially available (SSN)	None (ID card law was repealed in 2010)	exist	exist	Partially available (IRD)

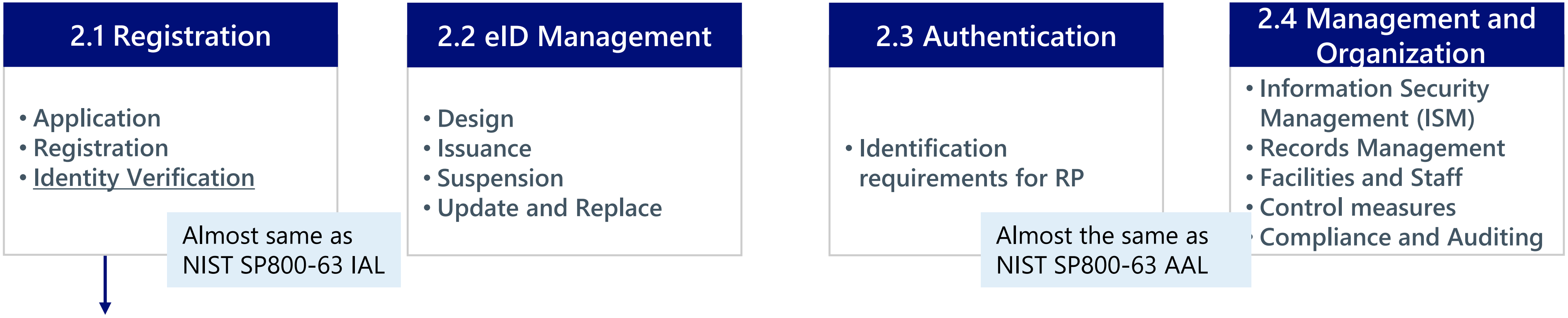
※Use of My Number is currently strictly limited to social security, taxes, and disaster countermeasures, and cannot be used for identity verification.

2-3-3. Use Case Analysis Use Case (1-1) Account Opening by using digital identity evidence

(Reference) Identity assurance frameworks in the US and EU

- U.S.: NIST (National Institute of Standards and Technology) has defined IAL and AAL in SP-800-63A [*1].
- EU: LoA (Levels of Assurance) has been defined in eIDAS.
- The number of jurisdictions with identity assurance frameworks, such as the US and EU, is limited.

LoA during eIDAS identity verification



2.1 Registration
- Application
- Registration
- Identity Verification

Almost same as NIST SP800-63 IAL

2.2 eID Management
- Design
- Issuance
- Suspension
- Update and Replace

2.3 Authentication
- Identification requirements for RP

Almost the same as NIST SP800-63 AAL

2.4 Management and Organization
- Information Security Management (ISM)
- Records Management
- Facilities and Staff
- Control measures
- Compliance and Auditing

● Example of LoA: Identity Verification

LoA	Low	Substantial	High
In-person application at the time of registration	Not necessary	Not necessary	Necessary
Checking Identity Trails	Valid IDs are not checked in-person.	Verification of identity based on an accepted trail	Verify possession of valid ID

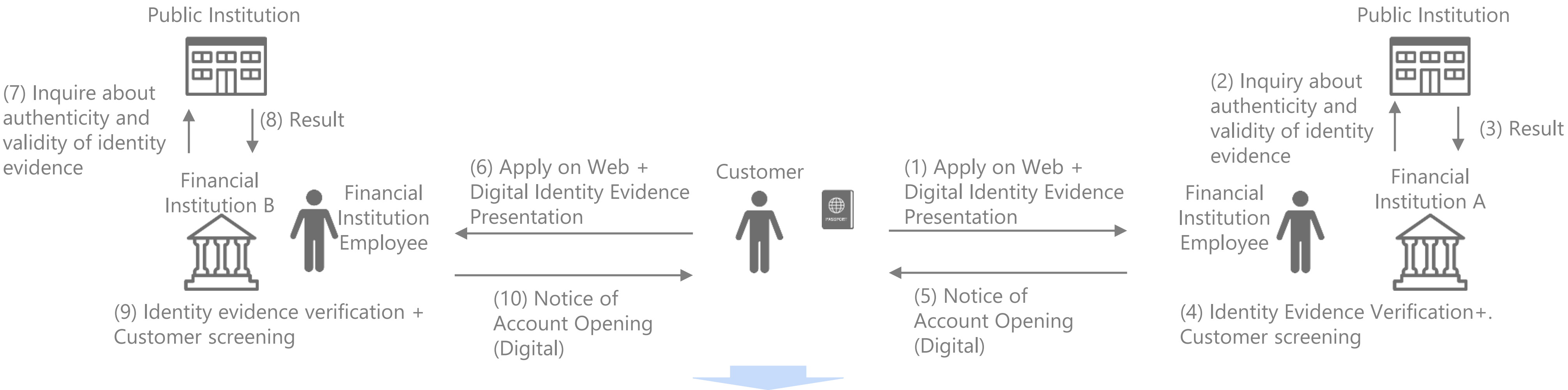
[*1] CONFORMANCE CRITERIA for NIST SP 800-63A ENROLLMENT AND IDENTITY PROOFING and NIST SP 800-63B AUTHENTICATION AND LIFECYCLE
https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf

2-3-3. Use Case Analysis Use Case (1-2) Account Opening by using a digital identity created by another company

Use Case Overview

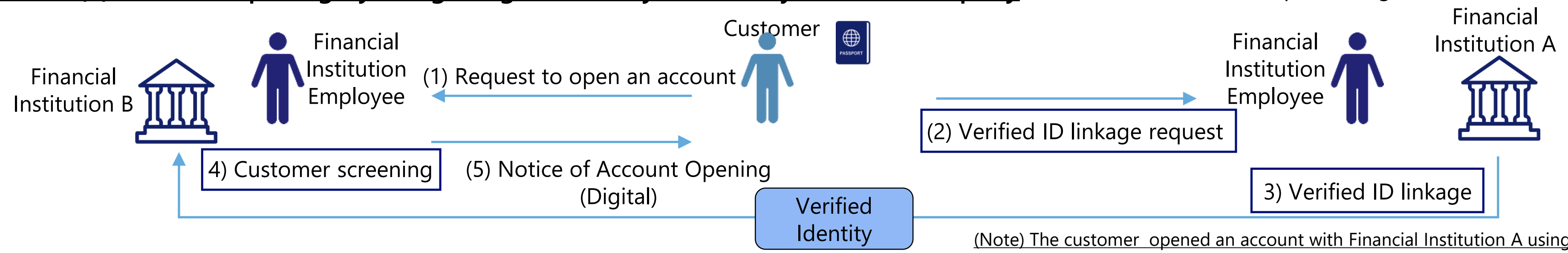
- Open a new account at a different financial institution using the digital identity of an existing financial institution account
- Expected to reduce the burden of opening accounts for customers, and reduce the burden of verifying identity evidence for financial institutions,etc

Administrative flow to open an account with each financial institution individually



Public Institution
(7) Inquire about authenticity and validity of identity evidence
(8) Result
Financial Institution B
Financial Institution Employee
(9) Identity evidence verification + Customer screening
(6) Apply on Web + Digital Identity Evidence Presentation
(10) Notice of Account Opening (Digital)
Customer
(1) Apply on Web + Digital Identity Evidence Presentation
(5) Notice of Account Opening (Digital)
Public Institution
(2) Inquiry about authenticity and validity of identity evidence
(3) Result
Financial Institution Employee
Financial Institution A
(4) Identity Evidence Verification+. Customer screening

Use Case (2) Account Opening by using a digital identity created by another company ＊ The blue frame is the part changed.



Financial Institution B
Financial Institution Employee
Customer
(1) Request to open an account
4) Customer screening
(5) Notice of Account Opening (Digital)
Verified Identity
(2) Verified ID linkage request
Financial Institution Employee
Financial Institution A
3) Verified ID linkage

(Note) The customer opened an account with Financial Institution A using the same administrative flow as when opening an account with each financial institution individually.

2-3-3. Use Case Analysis Use Case (1-2) Account Opening by using a digital identity created by another company

Issues that will be resolved and new issues that will come up by shifting from use case (1-1) (in-house only) to use case (1-2) (using digital IDs created by other companies)

- Further labor saving will occur for both financial institutions and customers in opening accounts, but issues such as the division of responsibilities between the parties will come up
- The main issues (highlighted in the table below) are described in detail on the following pages (for other issues, please refer to the supplementary document).

Remarks

~~Black:~~ Issues in use case (1) to be solved by moving to use cases (1-2)
Black: Issues in use case (1) that are difficult to resolve with transition to use cases (1-2)
Blue letters: New issues coming up from use cases (1-2)

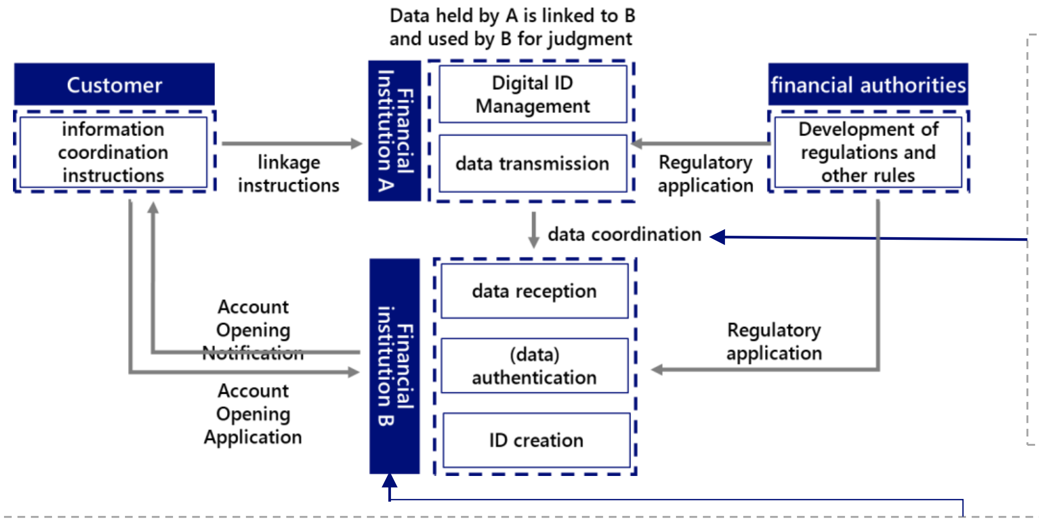
Issues that will be resolved and new issues that will come up by shifting from use case (1-1) (in-house only) to use case (1-2) (using digital IDs created by other companies)

Operation Process	Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Receipt of Application	• Infrastructure maintenance and operational costs for web application • Inadequate business model and division of responsibilities among ID linking parties	• Burden of applying on Web • ~~Burden of applying for a similar account at each financial institution.~~ • Financial exclusion of people who are not digitally compatible • Burden of dealing with complicated ID linkage
Verification at the time of transaction	• ~~Burden of verifying customers who have already been verified by other companies from scratch~~ • Develop a regulatory framework to promote appropriate use of digital IMS. • Difficult to make investment decisions with regards to changing existing optimized operations for the use of digital IMS	• Respond to new security risks, such as the opening of accounts in a chain. • Increased risk of dependence on specific financial institutions (IdP)
Customer Filtering	• ~~Burden of verifying customers who have already been verified by other companies from scratch~~	
Analysis and evaluation		
Judgment and response		

2-3-3. Use Case Analysis Use Case (1-2) Account Opening by using a digital identity created by another company

AML/CFT: Issues related to deciding business models and responsibility among ID federated parties

- Roles and responsibilities of the parties involved in ID linkage need to be clarified, and the two main issues that need to be considered are listed in the table below.
- In either case, the scope of responsibility will be considered after considering the value exchanged between the parties.



[Point 2] What to do when there is an error in the data of financial institution A (sender of ID), which causes a problem on the side of financial institution B (receiver of ID)?

- It is necessary to consider the liability for damages, etc., in case where there is an error in the data of the ID provider, causing damage to the recipient of the ID.
- The amount of damages varies depending on the scope of responsibility mentioned in point 1 and the reason for the error (inadequate management by the ID provider, cyber terrorism, error in the information provided by the customer, etc.).

[Point 1] Responsibility of KYC and identity verification of customer linked from financial institution A (ID sender) to financial institution B (ID receiver)

The following two patterns are possible, and the scope of responsibility should be examined in consideration of the exchanges between the parties.

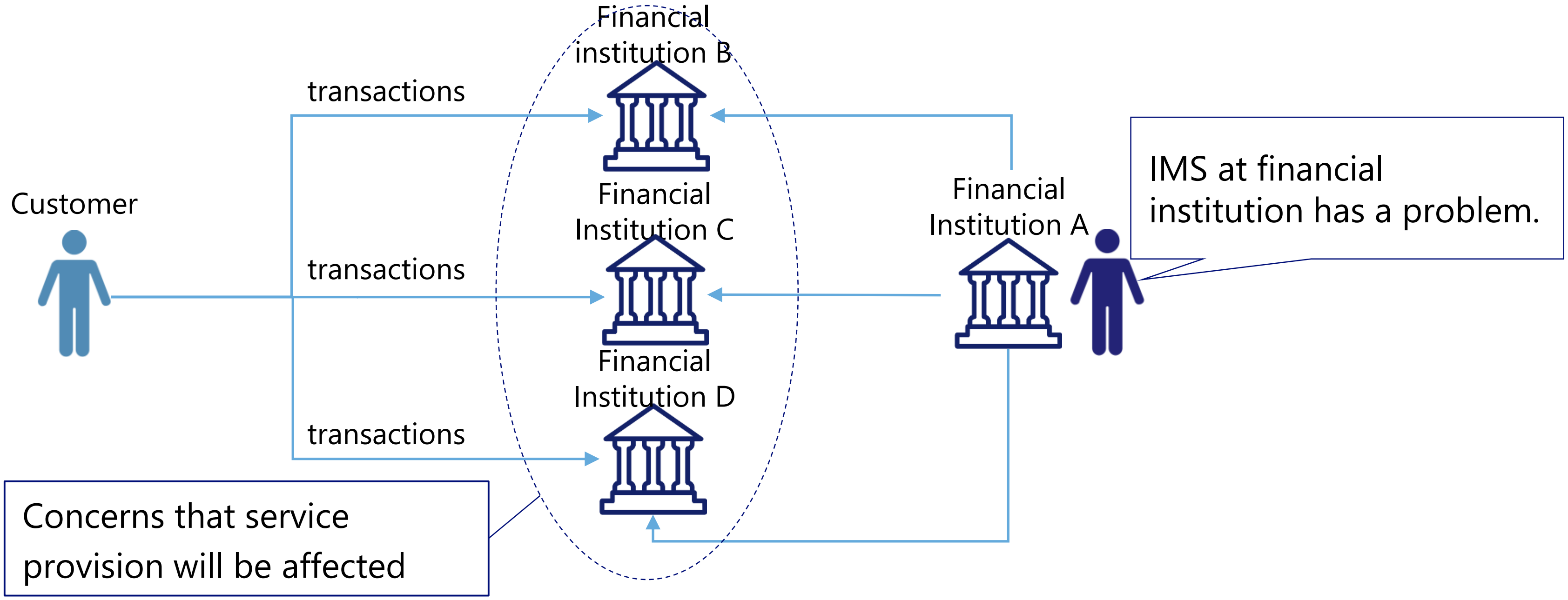
#	Pattern	Possible tasks for each participant
1	Financial institution A (ID sender) is responsible	• Financial institution B uses the linked information as identity-verified information (less responsibility) • The scope of financial institution A's responsibility is expected to increase, such as updating customer data and linking it after Verification, etc. (high responsibility). Also, there are concerns that over-reliance on financial institution A will weaken the KYC capabilities of financial institution B, which in turn will weaken KYC in the industry as a whole.
2	Financial institution B (recipient of ID) is responsible	• Financial institution B uses the information it receives as a reference and conducts its own identity verification again (high responsibility). • Financial institution A links ID information as reference information (less responsibility)

2-3-3. Use Case Analysis Use Case (1-2) Account Opening by using a digital identity created by another company

[Service Improvement] Increased risk of dependence on specific financial institution (IdP)

- When a customer opens an account with multiple financial institutions using an identity created by another company, the risk from the dependency on the identity provider (financial institution A in the figure below) may increase.
- If A problem occurs with verification at financial institution A, then the services of the financial institution to which the ID is linked will be affected

The impact if a problem occurs at a financial institution as an IdP



IMS at financial institution has a problem.

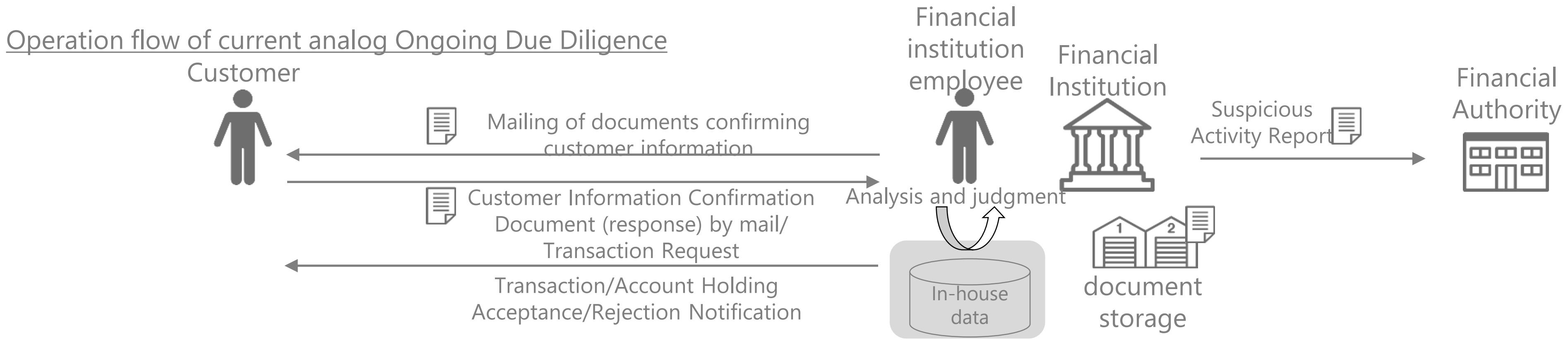
Concerns that service provision will be affected

2-3-3. Use Case Analysis Use Case (2) Ongoing Due Diligence

Use Case Overview

- Digital IMS will digitize interactions between financial institutions and customers, reducing the administrative burden on both financial institutions and customers.
- Analysis using data from other companies because of digital IMS, is expected to become easier than how it is currently.

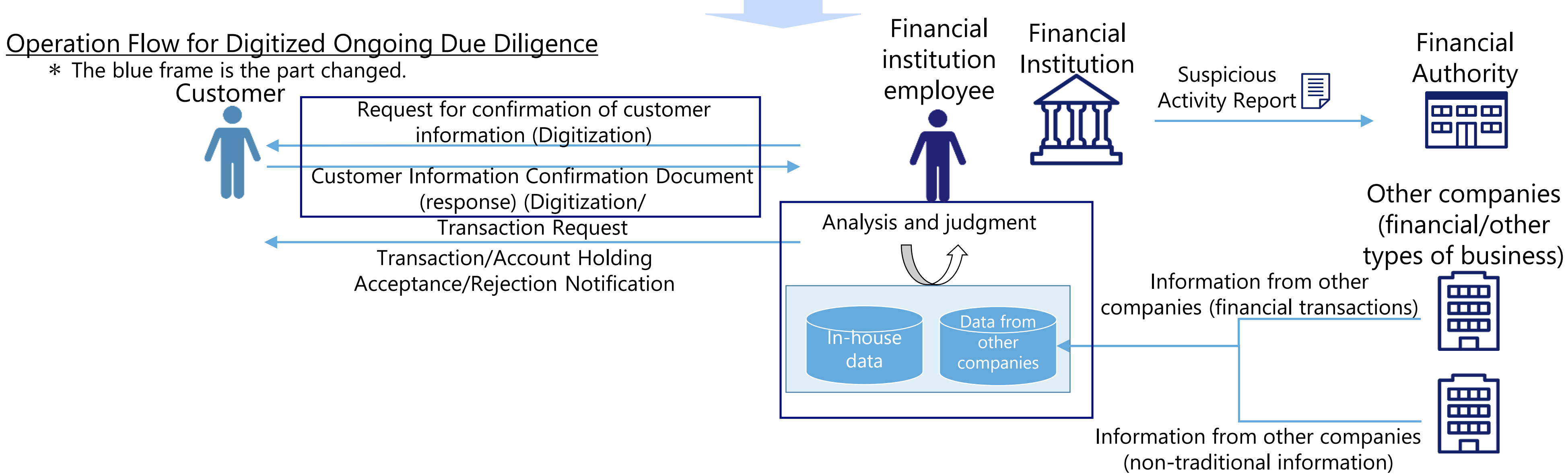
Operation flow of current analog Ongoing Due Diligence



Customer
Financial institution employee
Financial Institution
Financial Authority
Mailing of documents confirming customer information
Customer Information Confirmation Document (response) by mail/ Transaction Request
Transaction/Account Holding Acceptance/Rejection Notification
Analysis and judgment
In-house data
1
2
document storage
Suspicious Activity Report

Operation Flow for Digitized Ongoing Due Diligence

＊ The blue frame is the part changed.



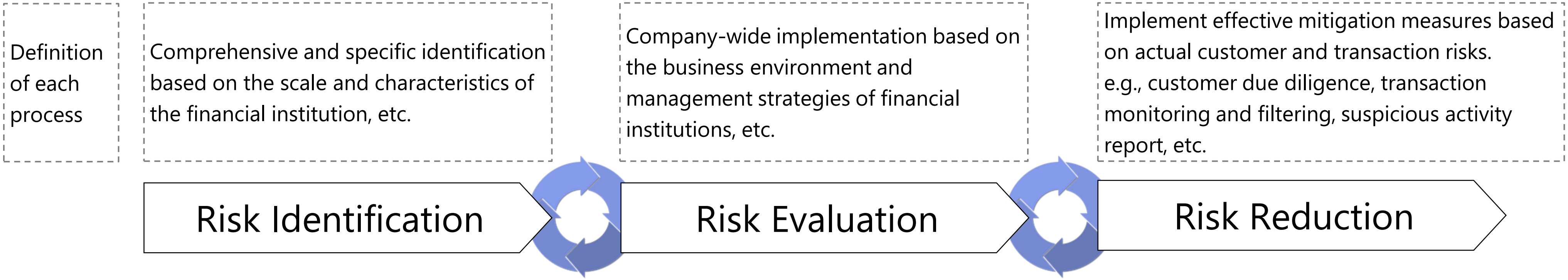
Customer
Request for confirmation of customer information (Digitization)
Customer Information Confirmation Document (response) (Digitization/ Transaction Request
Transaction/Account Holding Acceptance/Rejection Notification
Financial institution employee
Financial Institution
Financial Authority
Suspicious Activity Report
Analysis and judgment
In-house data
Data from other companies
Other companies (financial/other types of business)
Information from other companies (financial transactions)
Information from other companies (non-traditional information)

2-3-3. Use Case Analysis Use Case (2) Ongoing Due Diligence

Improvement in risk-based approach through digital IMS

- In FATF's guidance on digital identities, it mentions the possibility of enhancement of risk mitigation measures by using new technologies based on digital identity[*1)].
  - Facilitate customer identification and verification at onboarding
    - Geolocation, IP addresses, digital device identifiers used for the transaction, etc.
    - Additional information available through various channels such as the Internet and smart ~~cell~~ phones
  - Support ongoing due diligence and scrutiny of transactions throughout the course of the business relationship
    - Strengthen authentication of people accessing the site.
    - Enhanced detection of unusual or suspicious transactions
  - Contribution to financial Inclusion
    - Alternatives to traditional official documents (passport, driver's license, etc.) in emerging countries
    - Provide financial services according to the level of digital identity assurance in emerging economies

Process Overview of Risk-Based Approach



Definition of each process

Comprehensive and specific identification based on the scale and characteristics of the financial institution, etc.

Company-wide implementation based on the business environment and management strategies of financial institutions, etc.

Implement effective mitigation measures based on actual customer and transaction risks. e.g., customer due diligence, transaction monitoring and filtering, suspicious activity report, etc.

*1) FATF Guidance on Digital Identity (March 2020)
http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

	onboarding	ongoing
AML	①Account Opening	②Ongoing Due Diligence
Service		③Provide service

2-3-3. Use Case Analysis Use Case (2) Ongoing Due Diligence

Issues eliminated by usage of Digital IMS for Ongoing Due Diligence and new challenges

- While the risk-based approach has become more sophisticated and cost reduction has been achieved, new challenges related to utilization of other companies' data have come up.

Summary of Issues eliminated by usage of Digital IMS for Continuous Customer Management and new challenges

Remarks

~~Black:~~ Analog IMS issues to be solved by digital IMS
Black: Identity management issues difficult to resolve even with digital IMS
Blue letters: New issues coming up due to usage of digital IMS

Operation Process	Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Receipt of Application	~~• Burden of converting application and evidence information into data.~~ B	~~• Postage burden of mails~~ A • UX degradation due to excessive security measures to prevent information leaks in Ongoing Due Diligence A B
Verification of the identity of the applicant	~~• Burden of verification of a large number of customers~~ A	~~• Security risks during transactions (e.g., password theft during non-face-to-face access)~~ B
Transaction Filtering		
Analysis and evaluation	~~• Burden of collection of analog customer information, postal and electric costs and data conversion~~ A	
	• Regarding the provision of information to a third party, the burden of managing customer consent is high as a data provider(see use case (3) for details). A B • Burden of explaining data provider and confirming regarding the provision of information to third parties, is high for the data recipient (see use case (3) for details). A B	
Judgment and response		

Legend

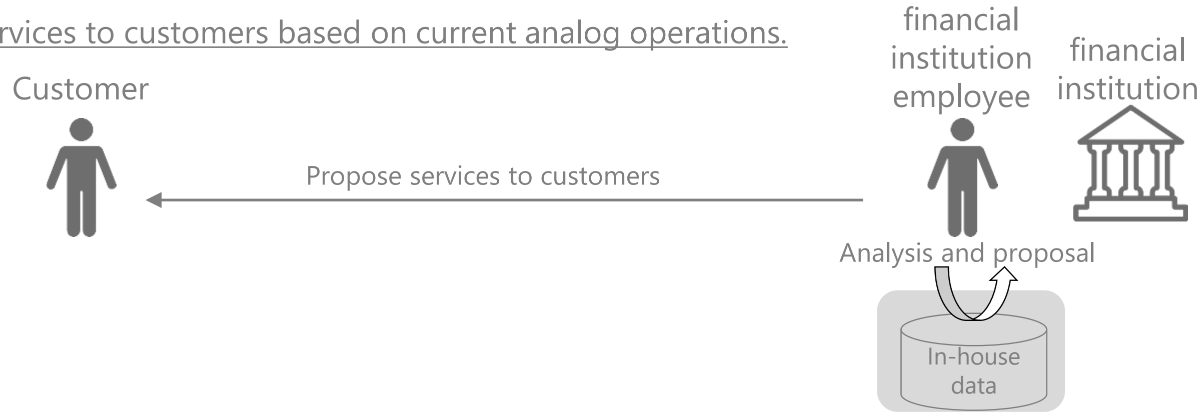
A	Periodic Customer Information Collection
B	Verification upon receipt of transaction

	onboarding	ongoing
AML	①Account Opening	②Ongoing Due Diligence
Service		③Provide service

Use Case Overview

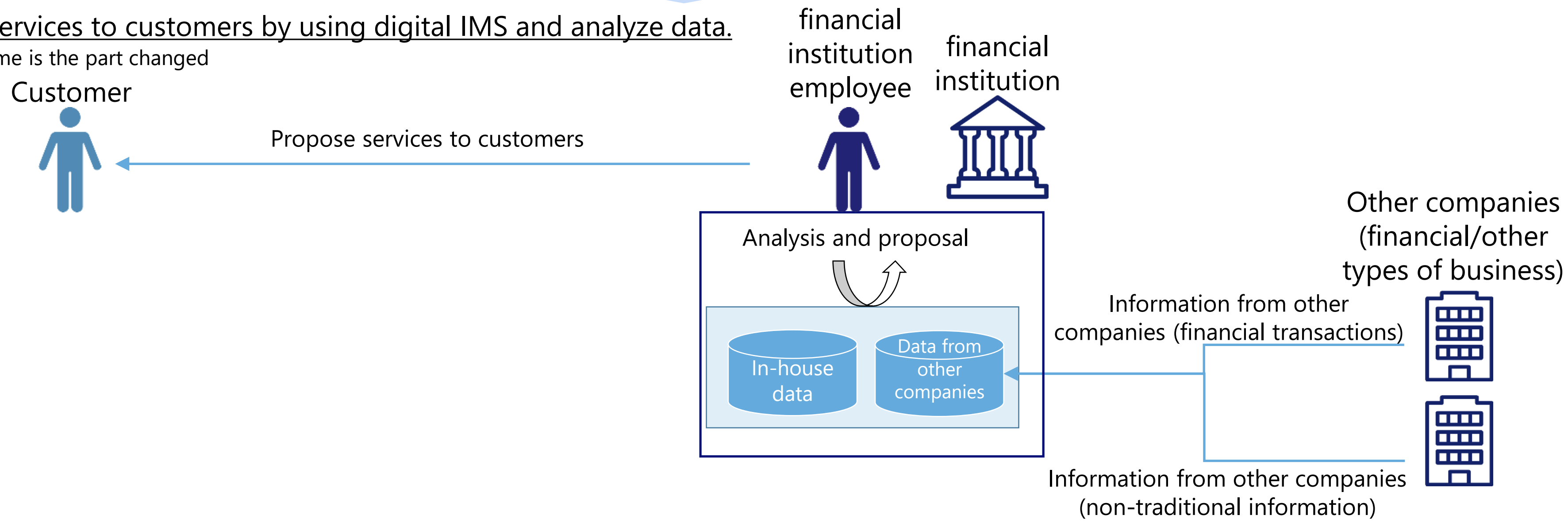
- Digital IMS will make it easier to collect and utilize identity information, including data held by other companies. It is expected to provide more optimal tailor-made services to customers.

Provide services to customers based on current analog operations.



Propose services to customers by using digital IMS and analyze data.

*The red frame is the part changed


Customer
financial institution employee
financial institution
Propose services to customers
Analysis and proposal
In-house data
Data from other companies
Other companies (financial/other types of business)
Information from other companies (financial transactions)
Information from other companies (non-traditional information)

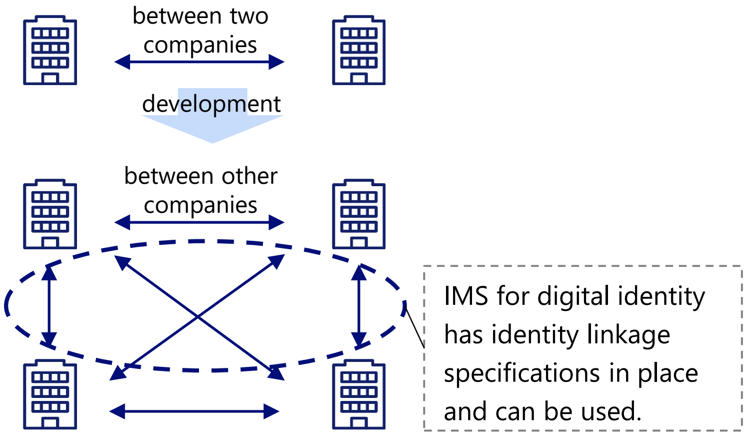
	onboarding	ongoing
AML	①Account Opening	②Ongoing Due Diligence
Service		③Provide service

2-3-3. Use Case Analysis Use Case (3) Provide services using information from other companies

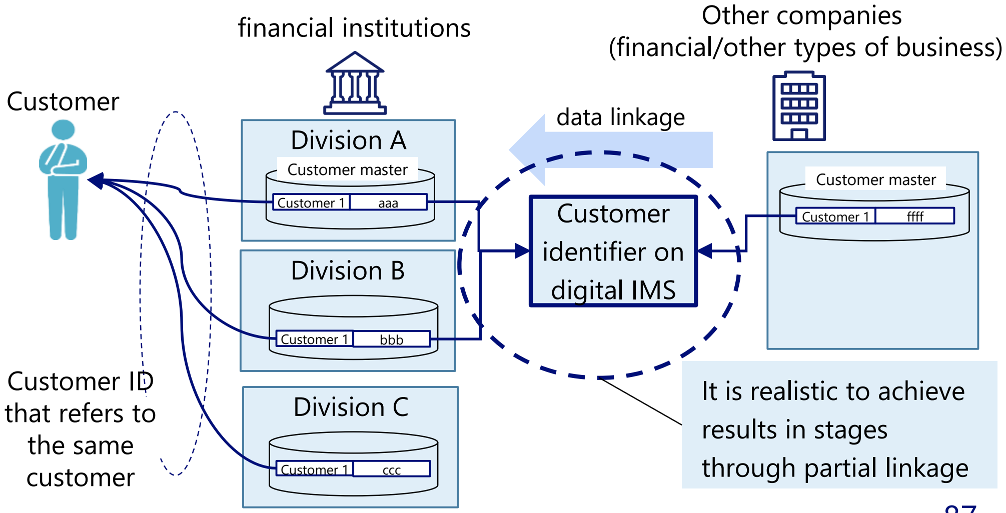
Solving issues with digital IMS: Linking customer identity information across departments/companies

- It is expected to promote data utilization within the company by managing customer identity information held in the DBs of each department within the company, as well as customer identity information held by other companies, by linking them to a common customer identifier on the digital IMS.
- The linkage of identity information is expected to spread from internal departments to inter-company, but the development of linkage specifications is important for efficient linkage. In this regard, in the digital IMS, identity information linkage is expected to become easier through the use of identity linkage specifications such as OpenID Connect ® described in Chapter 1. (Refer bottom left figure)
- Moreover, as discussed in 2-1-4, since there are cases where financial institutions have many individually optimized data systems, in reality, as shown in bottom right figure, it is possible to achieve results in stages by partially unifying systems that are similar in business and usage.
- However, in promoting data utilization, linking customer identity information is part of the solution and data licensing rules are reviewed with customers so that data can be used horizontally.

Image of the development of identity linkage and usage of identity linkage specifications


between two companies
development
between other companies
IMS for digital identity has identity linkage specifications in place and can be used.

Linking customer identity information using digital IMS


financial institutions
Other companies (financial/other types of business)
Customer
data linkage
Division A
Customer master
Customer 1
aaa
Division B
Customer 1
bbb
Division C
Customer 1
ccc
Customer identifier on digital IMS
Customer master
Customer 1
ffff
Customer ID that refers to the same customer
It is realistic to achieve results in stages through partial linkage

2-3-3. Use Case Analysis　Use Case (3) Provide services using information from other companies

Issues that will be resolved and new issues that will come up as a result of digital IMS for service provision using information from other companies

- As a result of ease in the collection and usage of identity information, including data held by other companies, issues related to the establishment of rules to receive and use information from other companies have come up.
- The main issues (highlighted parts in the table below) will be described in detail on the following pages (see the supplementary document for other issues).

Summary of issues that will be resolved and new issues that will come up as a result of digital IMS for service provision using information from other companies

Legend
~~Black:~~ Analog IMS issues to be resolved by digital IMS
Black: Identity management issues difficult to resolve even with digital IMS
Blue letters: New issues coming up from the use of digital IMS

		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of application		
	verification of the identity of the applicant		
	Transaction Filtering		
	Analysis and evaluation	• Burden of data consent management in order to utilize customer data across multiple services • Regarding providing information to third-party, as a data provider, the burden of handling customer consent is high. • Regarding providing information to third-party, burden of explaining to data provider and verification is too high for the data recipient.	~~• Data aggregation is difficult due to identifier mismatch~~ ~~=customer identifier mismatch due to management by each department/organization~~ ~~=customer identifier mismatch with third-party data~~ • Data aggregation is difficult due to inconsistent data formats inside and outside the company • Increased risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization
	Judgment and response		

2-3-3. Use Case Analysis Use Case (4) Provide services using information from other companies

Service Improvement: Issues related to the use of information from other companies

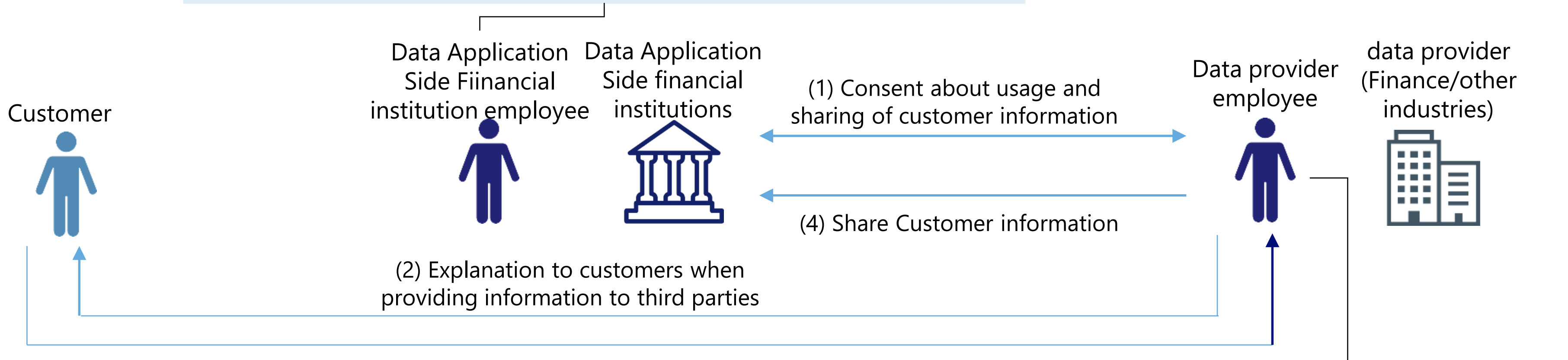
- When data utilization is carried out across companies, in addition to the burden of maintaining service licenses to utilize customer data across multiple services, there is a burden of handling information provided to the third-party on both the data provider side and the data utilization side.

Flow of obtaining consent from customers and issues in providing information to third parties

Issues on the data utilization side

Regarding providing information to third-party, Burden of explaining to data provider and verification is high for the data recipient.

- Burden of confirming the data acquisition process to the data provider
- Burden of explaining the purpose and content of data utilization to data providers and make them understanding



Customer

Data Application Side Fiinancial institution employee

Data Application Side financial institutions

(1) Consent about usage and sharing of customer information

(4) Share Customer information

Data provider employee

data provider (Finance/other industries)

(2) Explanation to customers when providing information to third parties

(3) Consent of the customer (data subject) to provide information to a third party

Issues on the data provider side

Regarding providing information to third-party, as a data provider, burden of handling customer consent is high.

- Burden of explaining data utilization to customers
- Burden of managing consent with customers, including the creation and storage of consent records

Other technical issues

■ Technical issues that are difficult to classify as use cases but have been pointed out in existing studies are listed as follows.

Issue classification	Summary of the issue	Issue Details
Cyber security Data Security	Increment in cybersecurity threats due to concentrated usage of digital ID	Centralized management of digital identities by identity providers increases the risk of criminals targeting large numbers of digital identities at once. A higher level of security is required. *1)
	Online identity theft	As identities are digitized, the risk of online identity theft increases. In parallel with the introduction of digital IDs, it is necessary to improve the security level for ID management. *2)*3)
	Sudden Death of Authoritative Source	If identity verification is performed by a third party, a failure in the process of verifying the identity of the Authoritative Source will widen the scope of impact and affect the entire ecosystem. *4)
	Insider threat	Centralized management of digital IDs by ID providers increases the risk of internal perpetrators; Administrative and security level of access privileges within ID providers must be improved. *1)
	Integrity of records	Records of digital ID creation and renewal must be complete, because if a digital ID created by one company is used by another and some issue comes up, the responsibility must be clearly defined.. *4)*5)

* References are listed on the next page.

2-3-4. Other technical issues

Other technical issues

Issue classification	Summary of the issue	Issue Details
Certification/ Approval	Verification whether the applicant is the true owner of the ID	It is necessary to verify that the applicant is the true owner of the ID by using more advanced techniques such as the use of biometrics and the use of verification and cancellation lists in the ID database. *4)
	Ongoing measurement of the effectiveness of certification technology	Attributes associated with an identity may change due to the lack of mature measurement methods for continuous authentication technologies. Analytic systems may be able to detect risk signals suggesting that IDs are being misused by fraud, etc. *2)*3)

*1) Digital Identities in Financial Services Part 2: Responsible Digital Identities, The Key to Creating More Inclusive Economies(Oct 2019) https://www.iif.com/Portals/0/Files/content/Innovation/10142019_responsible_digital_ids.pdf

*2) Guidance on Digital Identity (March 2020) http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

*3) OIX The value of digital identity to the financial service sector (Dec 2016) https://openidentityexchange.org/networks/87/item.html?id=202

*4) DG-FISMA ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

*5) DG-FISMA Report on existing remote on-boarding solutions in the banking sector https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

2-3-5. Issues related to data references from financial institutions

[AML/CFT] Trends in issues related to the verification of ultimate beneficial owners of corporations

- In the interviews with domestic financial institutions, they expressed the opinion that the burden of verification of ultimate beneficial owners of a corporation is high.
- Currently, in the "Best-practices-beneficial-ownership-legal-persons" *1) released in October 2019, the FATF recommends a method to determine the ultimate beneficial owners by combining multiple pieces of information (see table below), in light of the actual situation in each country as indicated in the FATF's mutual assessment and the burden of verification itself is unavoidable.
- Rather, the fundamental issue that the FATF is recommending to be addressed is **that there is no mechanism in place to ensure the veracity of ultimate beneficial owners' information when verifying the ultimate beneficial owners of a corporation**.

FATF's Recommended approach to collect information on ultimate beneficial owners *2)

No.	Approach Name	Overview	Source of reference of ultimate beneficial owners' information	
1	The Registry Approach	Consolidate up-to-date and correct information on ultimate beneficial owners in the register.	Register	
2	The Company Approach	Each company to maintain up-to-date and correct information on its ultimate beneficial owners.	Each company	
3	The Existing Information Approach	Use existing sources of information	External information source	Company registration information and other types of registries (e.g. registration of land, motor vehicles, movable property, etc.)
				Financial institutions and DNFBP*3)
				Other authorities (regulators and tax authorities), information held by stock exchanges, commercial databases, etc.

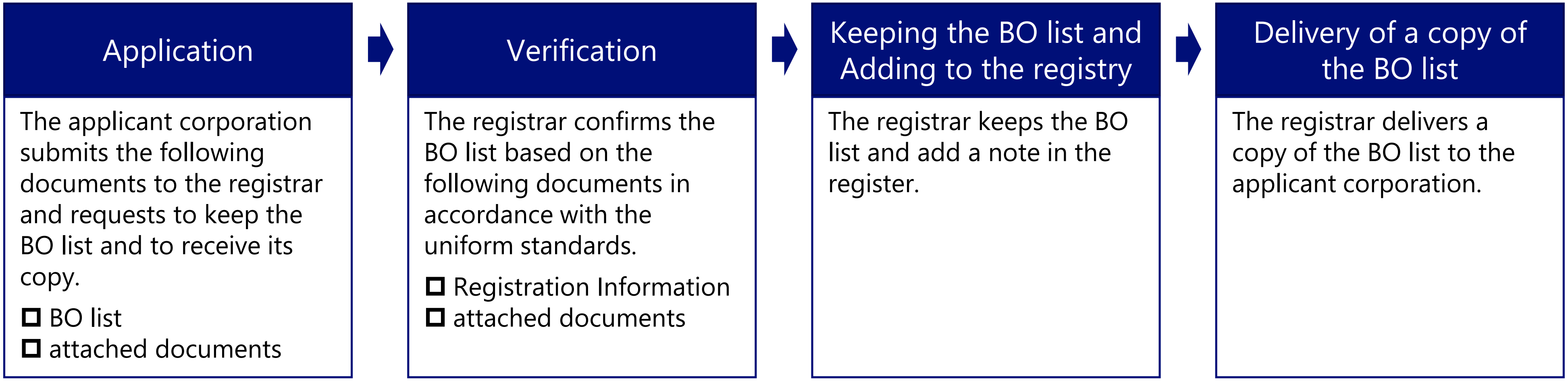
*1)FATF, best-practices-beneficial-ownership-legal-persons, Oct 2019 https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf
*2)Created by NRI based on *1)
*3) Designated non-financial businesses and professions

2-3-5. Issues related to data references from financial institutions

[AML/CFT] Trends in issues related to the verification of ultimate beneficial owners of corporations

- In response to the issues mentioned in the previous page, various countries are considering policies. For example, the following is being considered in Japan.
  - The Civil Affairs Bureau of the Ministry of Justice is considering a system in which commercial registration offices would keep a list of BOs and issue copies of the list of ultimate beneficial owners (hereinafter referred to as BOs) as stipulated in Article 11, Paragraph 2, Item 1 of the Enforcement Regulations of the Act on Prevention of Transfer of Criminal Proceeds. (From “Summary of the Study Group on Promoting the Understanding of Information on Ultimate Beneficial Owners of Corporations at Commercial Registration Offices", Civil Affairs Bureau, Ministry of Justice, July 2020)
    - In Japan, the BO information is verified by a notary at the time of incorporation through the BO declaration system for stock companies, etc. in the certification of articles of incorporation performed by a notary.
    - Future issues include (1) continuous monitoring of BO after the establishment of the corporation and (2) access to BO information, which is known to public institutions, by investigative agencies, etc.
    - By having the registrar of the commercial registry, who has expertise in this field, act as the hub to verify the ultimate beneficial owner and make a unified judgment, it is said that the uniformity of operation and a certain level of judgment level will be ensured, which will improve the reliability compared to the current situation where individual financial institutions check each time at the counter.

Flow of storage of BO list and delivery of its copy



Application

The applicant corporation submits the following documents to the registrar and requests to keep the BO list and to receive its copy.

□ BO list
□ attached documents

Verification

The registrar confirms the BO list based on the following documents in accordance with the uniform standards.

□ Registration Information
□ attached documents

Keeping the BO list and Adding to the registry

The registrar keeps the BO list and add a note in the register.

Delivery of a copy of the BO list

The registrar delivers a copy of the BO list to the applicant corporation.

Source: Ministry of Justice, Summary of the Study Group on Promoting the Understanding of Information on the Ultimate Beneficial Owners of Corporations at Commercial Registration Offices, Jul 2020 *the above English version was created by NRI based on the figure from the source
http://www.moj.go.jp/content/001324012.pdf

2-3-5. Issues related to data references from financial institutions

[AML/CFT] Trends in Cross-Border Trade issues

- According to the FSB's Stage 1 report*2) on initiative *1) to improve cross-border remittances presented to the G20 in April 2020, it has been pointed out that there are issues in cross-border remittances as they are costly, slow with limited access and less transparent.
- Regarding issues related to legal regulation and supervision framework , the report points out the friction in conducting cross-border remittances across multiple countries and regions with diverse legal and regulatory practices. It is required to consider the initiatives to improve the efficiency and reduce the cost of AML/CFT and other compliance processes without compromising the quality of compliance and also conduct adequate monitoring.
- As a related discussion, regarding the notification obligation (so-called travel rule) imposed at the time of transfer of cryptocurrency assets as per FATF Interpretation Note revised in June 2021, the introduction of AML / CFT laws and regulations in each country is progressing, and FATF itself recognizes the issue of handling the differences* 3)

From the above,
it can be seen that identity management issues in cross-border transactions are mainly related to legal and regulatory aspects, such as differences in AML/CFT regulations between countries, legal barriers (e.g., data protection legislation in each country,etc.) to cross-border data sharing in implementing FATF standards and other regulatory and supervisory requirements. (This is not expected to be solved by converting analog IMS of financial institutions to digital IMS.

- In addition, first report of FSB*2) mentions digital identity initiatives such as "expanding the use of Legal Entity Identifiers (LEIs) for businesses and digital identities for individuals. This is considered to be an effort to develop peripheral information that will enable financial institutions to verify identity information of individuals and corporations more efficiently.
  - In our interviews with domestic financial institutions, some of them mentioned the burden of collecting information on cross-border customers in cross-border transactions, and we believe that this is an expected measure.

*1) At the G20 Finance Ministers and Central Bank Governors Meeting in February 2020, it was decided to work on improving cross-border remittances as a priority. Requested the Financial Stability Board (FSB) to prepare a roadmap for improving cross-border remittances by October 2020, in cooperation with Committee on Payments and Market Infrastructures (CPMI), etc.
*2)FSB, Enhancing Cross-border Payments Stage 1 report to the G20,Apr 2020 https://www.fsb.org/wp-content/uploads/P090420-1.pdf
*3)ACAMS Today, Travel Rule Issues in the "12-Month Review of the New FATF Standards for Crypto Assets and Crypto Asset Exchangers", Nov 2020
https://www.fsa.go.jp/frtc/kikou/2020/FSA_article_ACAMSToday2020_Sept-Nov.pdf

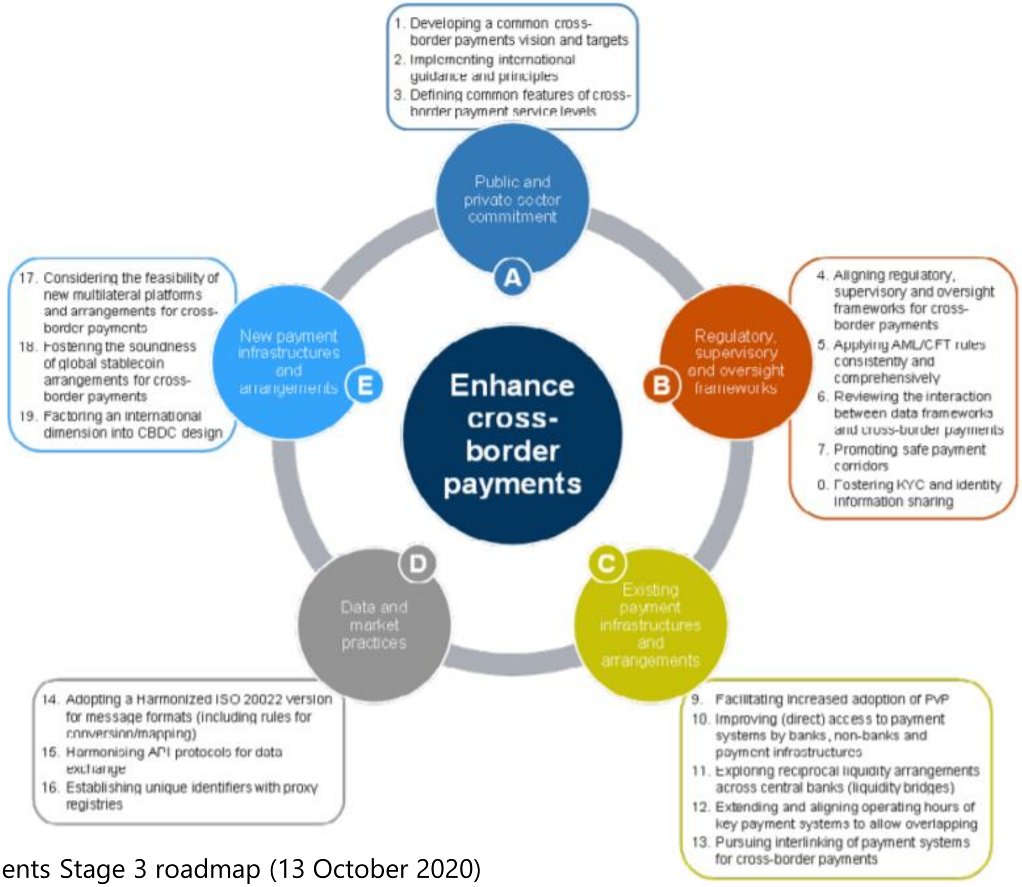
2-3-5. Issues related to data references from financial institutions

[AML/CFT] Trends in Cross-Border Trade issues

■ Efforts to resolve issues by FSB

- ● In July 2020, the FSB released its second report identifying 19 building blocks (BBs) to make improvements in resolving the issue. In October 2020, the roadmap for each BB was published as the third report. *1)
- ● The issues related to digital identity are being discussed mainly in BBB5、BB6、BB8、BB16 in the figure below.

Focus area and related building blocks*1)



Enhance cross-border payments

A Public and private sector commitment

1. Developing a common cross-border payments vision and targets
2. Implementing international guidance and principles
3. Defining common features of cross-border payment service levels

B Regulatory, supervisory and oversight frameworks

4. Aligning regulatory, supervisory and oversight frameworks for cross-border payments
5. Applying AML/CFT rules consistently and comprehensively
6. Reviewing the interaction between data frameworks and cross-border payments
7. Promoting safe payment corridors
8. Fostering KYC and identity information sharing

C Existing payment infrastructures and arrangements

9. Facilitating increased adoption of PvP
10. Improving (direct) access to payment systems by banks, non-banks and payment infrastructures
11. Exploring reciprocal liquidity arrangements across central banks (liquidity bridges)
12. Extending and aligning operating hours of key payment systems to allow overlapping
13. Pursuing interlinking of payment systems for cross-border payments

D Data and market practices

14. Adopting a Harmonized ISO 20022 version for message formats (including rules for conversion/mapping)
15. Harmonising API protocols for data exchange
16. Establishing unique identifiers with proxy registries

E New payment infrastructures and arrangements

17. Considering the feasibility of new multilateral platforms and arrangements for cross-border payments
18. Fostering the soundness of global stablecoin arrangements for cross-border payments
19. Factoring an international dimension into CBDC design

*1) Enhancing Cross-border Payments Stage 3 roadmap (13 October 2020)
（Japanese Abstract Translation by NRI） https://www.fsb.org/wp-content/uploads/P131020-1.pdf

Analog IMS issues to be solved by digital IMS Summary of Use case analysis results

- Many issues such as administrative burden of verifying identity evidence, etc. has been resolved.
- On the other hand, issues related to data utilization, such as data licenses for utilizing data from multiple services within the company and data from other companies, remain.
  - Issues related to data references from financial institutions are not listed in the table below, as they are not issues of Analog IMS.

Legend: ~~Character~~: Non-face-to-face and analog IMS issues eliminated by digital IMS

		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of application	~~• Burden of converting evidence information into data~~	• Burden of applying on the web ~~• Burden of applying for a similar account at each financial institution.~~ ~~• Burden of returning the post~~
	Verification at the time of transaction	~~• Difficulty in verifying analog identity evidence~~ ~~• Burden of verifying customers who have already been verified by other companies from scratch~~ ~~• Increasing difficulty in verifying identity with the shift to non-face-to-face interaction~~ ~~• Verification burden for a large number of customers~~	~~• Security risks during transactions (e.g., password theft during non-face-to-face access)~~
	Customer Filtering	~~• Burden of verifying customers who have already been verified by other companies from scratch~~	
	Analysis and evaluation	~~• Burden of collection of analog customer information, postal and electric costs and data conversion~~ ~~• Limitations of crime detection using only in-house data~~ • Maintenance burden of data license to utilize customer data across multiple services	~~• Data aggregation is difficult due to identifier mismatch~~ ~~• Customer identifier mismatch due to management by each department/organization~~ ~~• Customer identifier mismatch with third-party data~~ • Data aggregation is difficult due to inconsistent data formats inside and outside the company • Increased risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization
	Judgment and response	~~• Cost of mailing account opening notification to verify location~~	

New issues coming up from the shift to digital IMS　Summary of use case analysis results

■ With the shift to digital IMS, the following issues will newly come up.

		Issues related to AML/CFT (financial institutions/authorities)	Issues related to service improvement (customers/financial institutions)
Operation Process	Receipt of Application	• Inadequate business model and division of responsibilities among ID linking parties	• Financial exclusion of people who are not digitally compatible • Burden of dealing with complicated ID linkage specifications • Consent management burden for ID linkage • UX degradation due to excessive security measures to prevent information leaks in Ongoing Due Diligence
	Verification at the time of transaction	• Develop a regulatory framework to promote appropriate use of digital IMS. • Difficult to make investment decisions with regards to changing the existing and optimized operations to use digital IMS	• Respond to new security risks, such as the opening of accounts in a chain. • Increased risk of dependence on specific financial institutions (IdPs)
	Customer Filtering		
	Analysis and evaluation	• Regarding providing information to third-party, as a data provider, burden of handling customer consent is high. • Regarding providing information to third-party, Burden of explaining data provider and confirming is high for the data recipient.	
	Judgment and response		

2-3-8. Issue Summary

List of identity management issues that have not been resolved by digital IMS and new issues that will come up with digital IMS

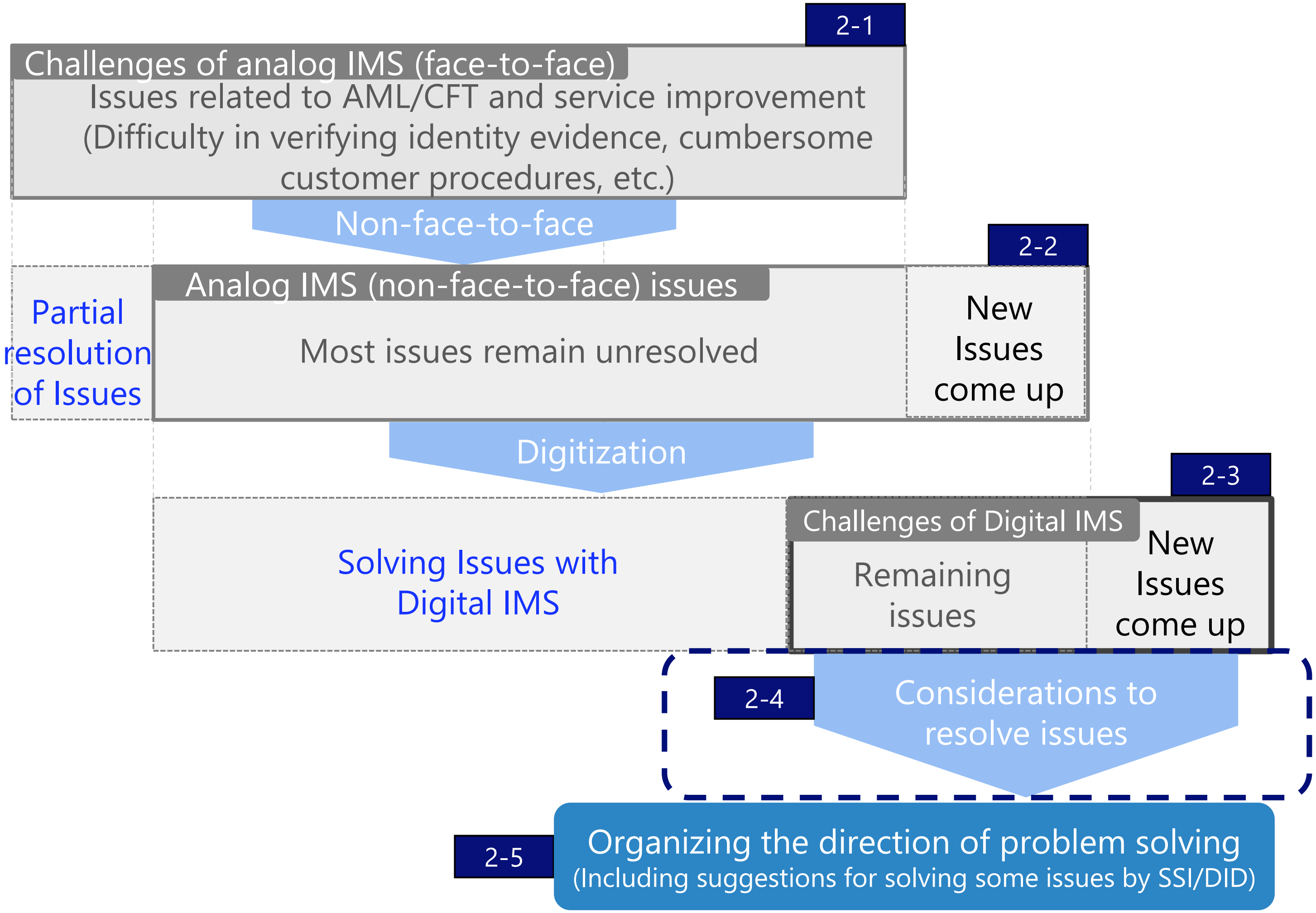
- The issues can be organized into the following nine perspectives.
- Note that 8) and 9) are limited to the presentation of issues in this survey, and the descriptions in the following sections are omitted.

Perspective of the issue	Issue
1) IAL	• Develop a regulatory framework to promote appropriate use of digital IMS.
2) ID linkage (focusing on the division of responsibilities)	• Inadequate business model and division of responsibilities among ID linkage parties • Increased dependence on specific financial institutions (IdPs)
3) Privacy (Consent management, data minimization)	• Consent management burden for ID linkage • Maintenance burden of data license to utilize customer data across multiple services • Regarding providing information to third-party, as a data provider, burden of handling customer consent is high. • Regarding providing information to third-party, burden to handle customer consent is high for the data recipient. • Increased risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization
4) Financial inclusion	• Financial exclusion of people who are not digitally compatible
5) Interoperability	• Burden of dealing with complicated ID linkage specifications
6) Investment decisions for transitioning to new operations	• Difficult to make investment decisions with regards to changing an existing and optimized operations to use digital IMS
7) Issues related to data references from financial institutions	• Issues related to verification of ultimate beneficial owners of corporations • Issues of cross-border transactions
8) Other business issues (UX improvement, IT infrastructure development)	• Burden to apply on the web • UX degradation due to excessive security measures to prevent information leakage in Ongoing Due Diligence • Responding to new security risks, such as the opening of accounts in a chain. • Data aggregation is difficult due to inconsistent data formats inside and outside the company
9) Other technical issues	• A series of technical issues as described in 2-3-4

2-4. Problem solving (Implications from advanced case studies)

2-4. Problem solving (implications from advanced case studies)

Subject of discussion in this section


2-1

Challenges of analog IMS (face-to-face)

Issues related to AML/CFT and service improvement (Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)

Non-face-to-face

2-2

Partial resolution of Issues

Analog IMS (non-face-to-face) issues

Most issues remain unresolved

New Issues come up

Digitization

2-3

Solving Issues with Digital IMS

Challenges of Digital IMS

Remaining issues

New Issues come up

2-4

Considerations to resolve issues

2-5

Organizing the direction of problem solving

(Including suggestions for solving some issues by SSI/DID)

2-4. Problem solving (Implications from advanced case studies)

Use of advanced case studies to solve problems

- As mentioned in previous chapter, there are various issues in the development and operation of a digital IMS, but there are some advanced examples in overseas countries that address these issues.
- In this chapter, we will discuss the issues of analog IMS that have not been solved even with the shift to digital IMS, as mentioned in the previous chapter, and the issues that newly come up with the shift to digital IMS.
  - Regarding 7), we will only address issues related to cross-border transactions among the issues related to data references from financial institutions, for which advanced examples can be found overseas.

Perspective of the issue	Example
1) IAL	(1) EU (2) Singapore (3) India (4) UK
2) ID Linkage (focusing on the division of responsibilities)	(5) ID linkage service (6) Efforts of standardization organizations.
3) Privacy (consent management and data minimization)	Since this is an area where SSI/DID is expected to solve problems, this issue will be discussed in detail in Chapter 3.
4) Financial inclusion	(3) India
5) Interoperability	(9) Australia (6) Efforts of standardization organizations
6) Investment decisions for transitioning to new operations	(5) ID linking service
7) Issues in cross-border transactions	Two examples of cross-border trades (cross-border finance) (7) ID issued by private sector (8) Major European financial institutions

2-4. Problem solving (Implications from advanced case studies)

(1) Efforts to integrate financial regulations and Identity Assurance Framework (eIDAS) in the EU

- The EU is considering expanding the scope of eIDAS private services for public services.
- At the same time, the revision of the AML Directive to unify customer management regulations is under consideration.

	Before	After
Directions to address issues	• The LoA (IAL) of eIDAS, identity verification and customer management in finance could not be addressed at the EU level, and was left to the regulations of the member states, resulting in a patchwork of regulations and increased compliance costs. • Regarding privacy protection, correspondence with GDPR is being considered, but only to point out the issues.	• By using eIDAS-compliant digital IDs for financial institutions to provide cross-border financial services in EU, it is expected that the unification of IAL in financial sector will be promoted. • At the time of enactment of the next AML Directive or revision of the AML rulebook, unified customer management rules based on eIDAS will be established and shall be reflected in the AML/CFT rules of member countries. • Privacy protection is expected to be announced by the European Commission related to the scope of possible data sharing in the EU.

Background. success factor

- ✓ With initiative taken by European Commission, eIDAS has been widely introduced into public services since its implementation in 2016.
- ✓ The enforceability of the AML Directive has led to the continuous revision of AML/CFT regulations in member countries over the past 30 years.

Results

- ✓ Expansion of application of eIDAS to private sector services and the unification of customer management regulations are expected to facilitate cross-border financial services among member countries.
- ✓ The unification of customer management regulations is expected to strengthen AML/CFT in member countries.

Future Issues

- ✓ Can we achieve interoperability with the rest of the EU to promote cross-border financial services?
- ✓ Can the entire KYC process be harmonized among member countries when the Uniform Customer Relationship Management Rules become national law?

2-4. Problem solving (Implications from advanced case studies)

(1) Efforts to integrate financial regulations and Identity Assurance Framework (eIDAS) in the EU

- Progress is being made in exploring the use of eID in the financial sector based on eIDAS to improve AML/CFT (e.g., remote onboarding) and cross-border transactions.

When	Event	Remarks
2010	Publication of ICT strategy “European Digital Agenda” as part of the EU's "Europe 2020" growth strategy.	DSM was developed and dissolved.
2013	Connecting Europe Facility (CEF) adopted as EU budget for 2014-20	Use of eID specified as one of the CEF initiatives
2014	Adoption of eIDAS regulations	Enforcement: July 2016
2015	Digital Single Market (DSM) Strategy Released	eIDAS positioned as a component and emphasis on using eID for cross-border transactions between EU member states
November 2015	PSD2 (European Payment Services Directive) adopted	Article 97 requires SCA (strong customer authentication); Article 98 gives provision to EBA to develop RTS (regulatory technical standards) for SCA. eID is not a legal obligation (only a recommendation).
2017	Establishment of eID/KYC Expert Group at DG FISMA	Examine methods to promote cross-border use of eID and KYC portability based on identification and authentication tools under eIDAS
November 2017	RTS related to SCA for PSD2 released by EBA	Provide stricter authentication methods for electronic payments.
July 2018	AMLD5 (Fifth Anti-Money Laundering Directive) came into effect.	Use of eID is recommended, but not specified for LoA level.
same as above	Regarding CEF framework, DG Connect released a report on the use of eID in eBanking.	The potential for using eID in the banking sector and regulatory issues (e.g., the relationship between major regulations and eID) are summarized (see the attached detailed report).
December 2019	The report of the above eID/KYC Expert Group has been completed (published in March 2020).	Two reports on the use of digital IDs, including eIDAS, in finance*1)*2) (See Appendix: Detailed Report)
July-October 2020	Public consultation for eIDAS revision	Proposed amendments will be released in the summer of 2021.
September 2020	Digital Finance Strategy for Europe published	(1) Establishment of guidelines to enable reliance on customer management conducted by other financial institutions by Q3 2021, (2) EU-wide unification of AML/CTF regulations, and (3) extension of eIDAS regulations to private sector IDs.

*1) Report on existing remote on-boarding solutions in the banking sector
https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf
*2) ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR: The case for an attribute-based & LoA-rated KYC framework for the digital age
https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

2-4. Problem solving (Implications from advanced case studies) 1) EU case study

(1) Efforts to integrate financial regulations and Identity Assurance Framework (eIDAS) in the EU

- DG-FISMA suggests attribute elements required for identity verification and customer management*1) .

Core Identity Attributes (Individual)

- A set of attributes that uniquely identifies an individual.
- Name, date of birth, place of birth, name, nationality, personal ID, etc.

Core Identity Attributes (Corporate)

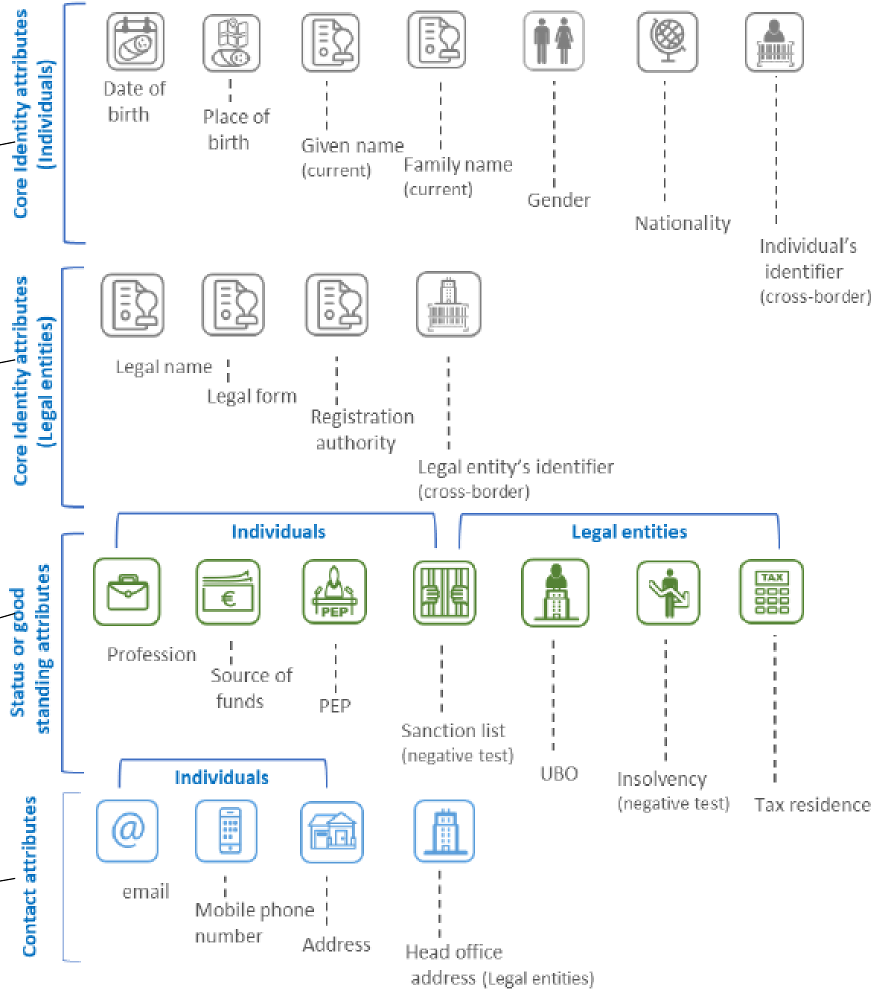
- A set of attributes that uniquely identifies a corporate
- Corporate name, registered address, corporate ID, etc.

Status (personal) or good standing (corporate) attribute

- Attributes required for customer management purposes
- (Individual) Occupation, source of income, etc.
- (Corporations) ultimate beneficial owner, history of default, etc.

Contact Attributes

- Attributes that help you contact the person in question
- Address, etc.


Core identity attributes (Individuals)
Date of birth
Place of birth
Given name (current)
Family name (current)
Gender
Nationality
Individual's identifier (cross-border)
Core identity attributes (Legal entities)
Legal name
Legal form
Registration authority
Legal entity's identifier (cross-border)
Status or good standing attributes
Individuals
Legal entities
Profession
Source of funds
PEP
PEP
Sanction list (negative test)
UBO
Insolvency (negative test)
TAX
Tax residence
Contact attributes
Individuals
email
Mobile phone number
Address
Head office address (Legal entities)

*1) ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR
https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd- solutions-in-the-banking-sector-december2019_en.pdf

2-4. Problem solving (Implications from advanced case studies)

(2) Improving the efficiency of onboarding process using national ID in Singapore

- In Singapore, the government has been promoting national ID for nearly 20 years.
- Leveraging this infrastructure, major financial institution has been successful in making its onboarding process more efficient.

Directions to address issues

Before

- SingPass is a shared authentication system for the use of government online services, and MyInfo is a common personal information registration system among government services that was launched on a centralized platform but not opened to the private sector.
- On the other hand, MAS 626 and the Interpretation Notes have detailed the identification documents and verification methods for non-face-to-face transactions.

After

- By opening up SingPass and MyInfo to private services, private services can use government-owned identification information, facilitating IAL unification within jurisdictions.
- The government-led implementation of biometric,multi-factor authentication and information updates are uniformly bottoming out the IAL for financial services using the platform.

Background/ success factor

✓ National IDs have been promoted and used for nearly 20 years under the strong leadership of the government.
✓ SingPass was opened to private services in 2018 and MyInfo in 2017.

Results

✓ New onboarding of a major financial institution was conducted in remote basis and onboarding costs got reduced.
✓ Drop rate was improved by linking customer information during remote onboarding from government data and by reducing the number of input items.

Future Issue

✓ SingPass and MyInfo cannot be used for AML/CFT, and each financial institution is implementing countermeasures based on its own accumulated and verified data.
✓ Hurdle to open accounts and use financial services for those who do not possess a national ID or a long-stay visa is increasing.

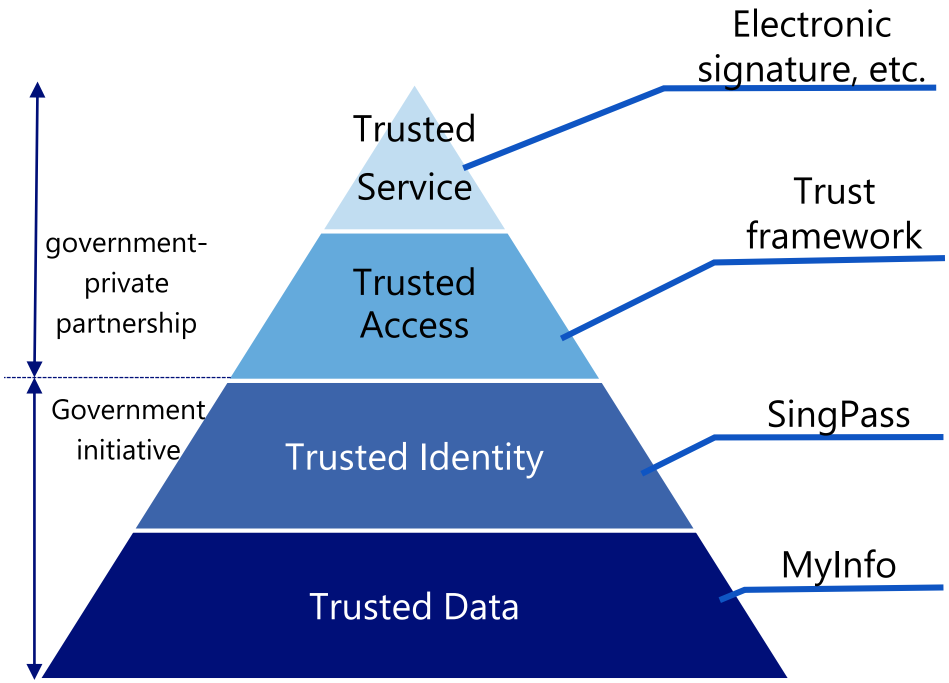
(2) Improving the efficiency of onboarding process using national ID in Singapore

- Strengthen authentication and security of SingPass, which is triggered by the use of SingPass based on national IDs for administrative services.
- In addition, we are building and promoting NDI, a common digital authentication platform for the public and private sectors, based on SingPass and MyInfo.

History regarding usage of national IDs

When	Event
1948	Introduction of National ID
2003	Introduction of SingPass (Usage of administrative services with national ID and password)
2014	Smart Nation Concept
2015	Introduction of SingPass 2-step authentication
2016	Introduction to MyInfo
2017	Open MyInfo to private sector services
2018	SingPass opened to private services Introducing SingPass Mobile (Fingerprint and face recognition is now possible with smartphones)
2020	Establishment of NDI (National Digital Identity), a common digital authentication platform for the public and private sectors, based on SingPass and MyInfo

Concept of NDI Stack



1) IAL

4) Financial inclusion

2-4. Problem solving (Implications from Advanced Cases) (3) India case-study

(3) Expanding private sector services in India using India Stack

- In India, the government is taking the lead to move to digital payments and has developed the India Stack, a certified payment infrastructure centered on Aadhaar.
- Along with the development of private sector services using India Stack, there has been an explosion of registration and usage.
  - In addition, there have been criticisms about privacy since its introduction, and the Supreme Court ruling in September 2018 restricted the private use of identity verification by Aadhaar, but after that, the revision of the Aadhaar law ensured that if there is consent of the concerned person then private companies can use Aadhaar for identity verification.

Directions to address issues

Before

- There has been an issue of fraudulent receipt of social security and benefits for low-income and remote groups. Government aimed at providing an identification to people to direct social security benefits by remitting directly into the account of beneficiaries.
- Since the literacy rate was about 70%, the use of biometrics was being considered.

After

- The government has established public institutions such as NPCI and UIDAI to develop and provide Aadhaar and Aadhaar-based authentication, payment, and account registration functions ("India Stack") as a public infrastructure, with the aim of assigning identification numbers to all citizens and direct transfer of benefits.
- The Modi government's "Digital India Plan" has led to an explosion in the registration and use of Aadhaar and India Stack.

Background/ success factor

- ✓ The government is leading the shift to digital payments and has developed an authenticated payment infrastructure and API infrastructure (India Stack) with Aadhaar at its core.
- ✓ Government has implemented policies and legal developments to expand the use of digital payments (Universal Bank Account Project, Aadhaar Act, etc. under Digital India, a digitization policy announced in 2015)

Results

- ✓ Although registration is not mandatory, over 99% of adults are currently registered with Aadhaar.
- ✓ Financial inclusion has increased, and the poor and remote rural populations who do not have official identification can now access financial services.
- ✓ It was able to strengthen the crackdown on money laundering and underground economy (tax evasion) and ensure that benefits reach the beneficiaries.

Future Issue

- ✓ Privacy: It has been pointed out that the linkage with bank accounts and PAN cards leads to the "obligation" to register, and that letting others know the 12-digit number that each of us has is a violation of privacy.
- ✓ Security: It has been pointed out that if the system is cyber-attacked, all registration data will be at risk.

Source: Digital Financial Services (April 2020) https://documents1.worldbank.org/curated/en/750421502949470705/pdf/118736-BRI-EMCompass-Note-42-DFS-Challenges-and-Opportunities-PUBLIC.pdf
, NNA Asia Reporting Note, “Universal Numbering, a Reform that Creates Opportunities and Perils” (September 2017) https://www.nna.jp/nnakanpasar/backnumber/170901/feature_001

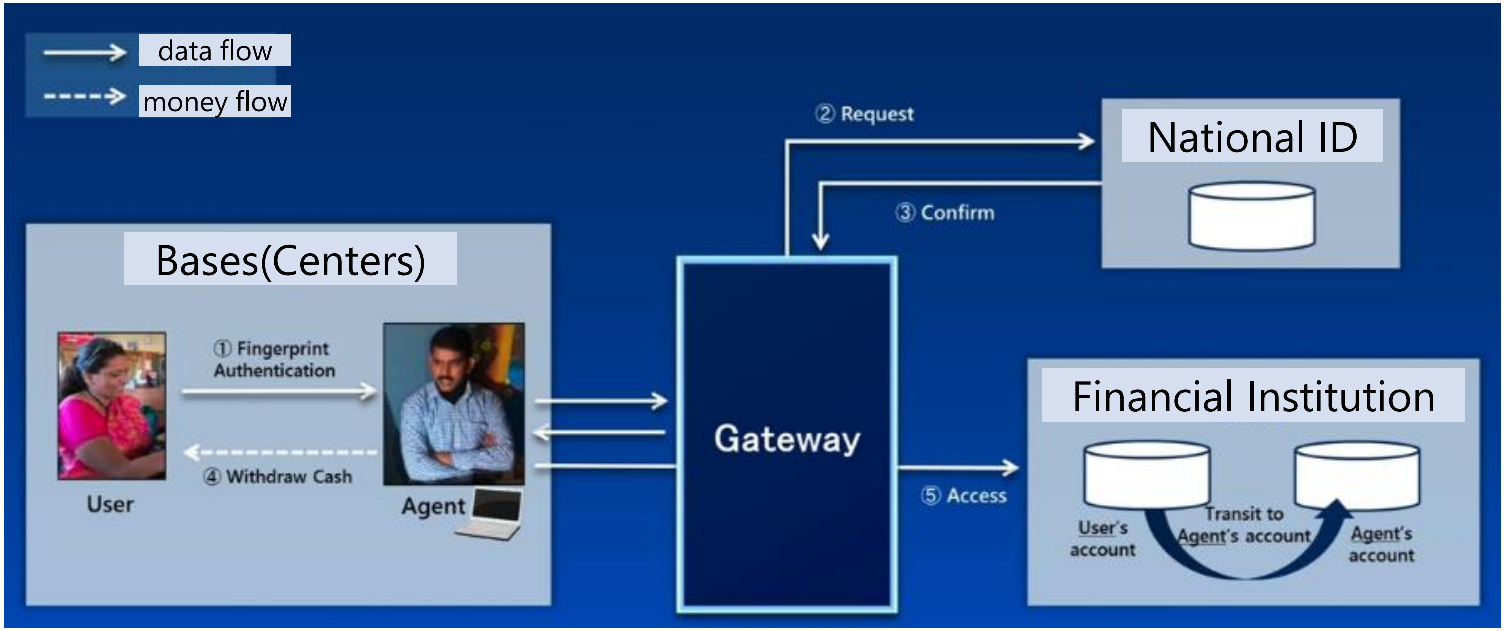
(3) Expanding private sector services in India using India Stack

■ A case study of financial transactions in a rural area with undeveloped digital infrastructure*1)

- The majority of Indian citizens live in rural areas, where there are no financial institution branches/ATMs around and customers do not have mobile devices.
- Therefore, agents dispatched by the financial institutions to operate biometric authentication of customers and to receive cash from and to the customers ensured that financial services are provided to the rural population without the need to build branch/ATM network of financial institutions.

<Example: Withdrawal>

After verifying the identity of the customer with biometric authentication and handing the cash from the agent to the customer, the agent processes the transfer from the customer account to the agent account.



*1) Government Internet TV Super City/Smart City Forum 2019: "Aadhaar Success Secrets and Financial Services in India *The English translation of the Japanese sections were prepared by NRI
https://nettv.gov-online.go.jp/prg/prg19513.html

1) IAL

2-4. Problem solving (Implications from advanced case studies)

(4) Implementation of GOV.UK Verify as an alternative to the national ID in the UK

- The UK has failed multiple times to promote national IDs and has introduced GOV.UK Verify (see details below) as an alternative.
- However, the number of users, the number of services, the success rate of identity authentication, and profits have all fallen short, and IdPs have begun to withdraw.

Directions to address issues

Before

- The ID Card Act was enacted, and ID registration numbers and ID cards were issued to individuals over the age of 16 who stayed in the UK for more than three months.
- In addition to being used as a passport within the EU, it can be used as proof of identity when using private services.
- The ID card law was abolished due to strong sense of government control and surveillance of society.

After

- GOV.UK Verify has been developed so that IDs issued by private companies can be used as a means of authentication when accessing public services.
- Each individual can access public services through GOV.UK Verify from the IdP of his choice.
- Gave individuals the right to choose, use, and discontinue IdPs instead of centralized control of national IDs by the government.

Background/ success factor

- ✓ Led by the Government Digital Service (GDS), which is responsible for digital services across government.
- ✓ The government has provided financial support of 20 pounds per person*1) to private companies participating as IdPs. (Until October 2021)

Results

- ✓ 22 different public services are available to be used using GOV.UK Verify (as of January 2020).
- ✓ 7 certified businesses (as of October 2014) and 6 million users (as of January 2020) are using.

Future Issue

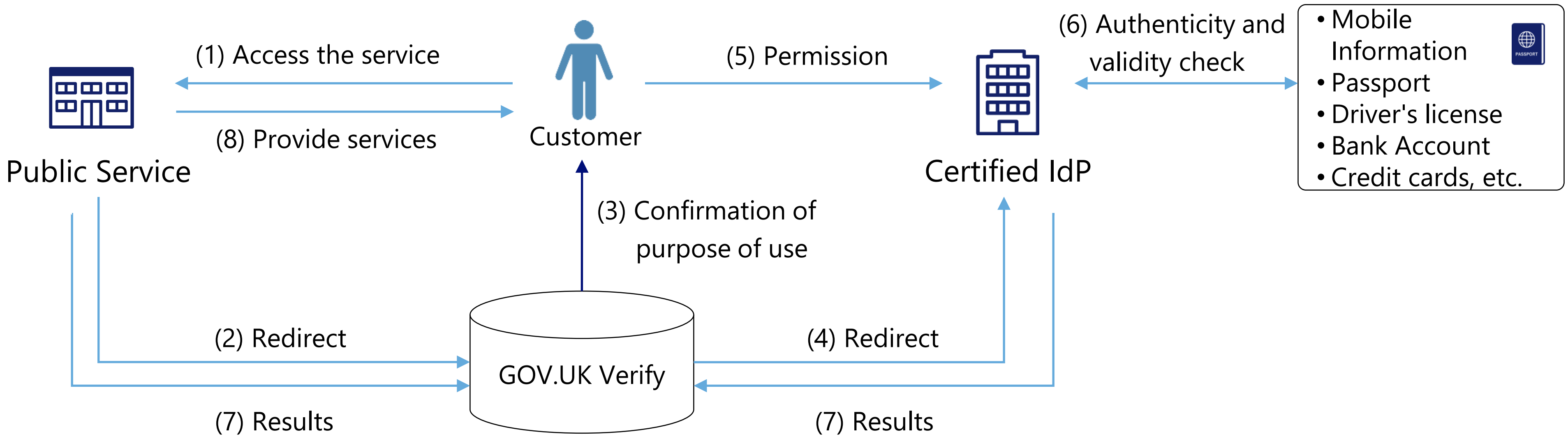
- ✓ As of March 2020, the number of IdPs has decreased to two due to successive withdrawals by IdPs as the number of users and services did not reach the initial forecast and costs increased.
- ✓ Major banks are considering alternatives, such as issuing digital identities on their own or through regulations by industry groups such as TISA,etc.

*1) https://www.governmentcomputing.com/identity/news/commercial-concerns-push-two-idps-away-verify-heads-towards-private-sector- delivery

(4) Implementation of GOV.UK Verify as an alternative to the national ID in the UK

- Gov.UK Verify is an authentication technology equivalent to Level 2 of the eIDAS framework.
- A means of authenticating an individual's identity when accessing public services through GOV.UK Verify from the IdP selected by each individual

Flow to verify authenticity and validity of identities



2-4. Problem solving (implications from advanced case studies)

(5) Division of responsibility in ID linkage services

- In the case of ID linkage services 1 and 2, IdP is responsible only for information that has been authenticated or is at a high authentication level.
- In ID linking service 3, RP is responsible for the information because the information is for reference purpose.

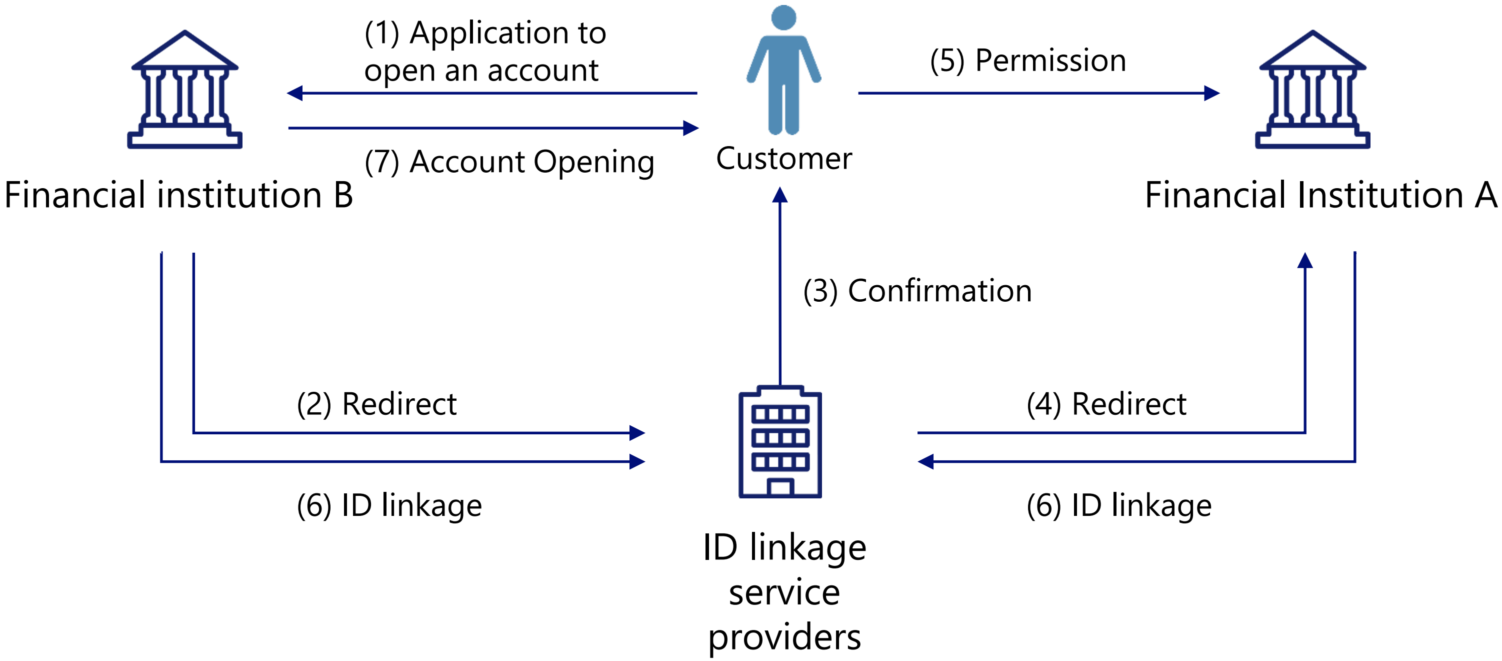
Services	ID linkage service1	ID linkage service2	ID linkage service3
Areas served	Europe	Northern Europe	Japan
Contents	Link verified information (claims) as a Qualified Trust Service Provider (QTSP) in eIDAS	Provide all citizens with a unified ID that can be used for both public and private services.	Linkage of verified identity information held by financial institutions to enable businesses to implement eKYC
Attribute items that can be linked	Compliant with specifications of OpenID Connect® regulations or OpenID Connect for Identity Assurance® regulations	Attribute items that meet AML/CFT requirements in addition to attributes required for account opening	Not disclosed
Main participants	IdP: Financial institution in the jurisdiction RP : Not disclosed	IdP: Financial institution in the jurisdiction RP : Retail, financial institutions in the jurisdiction, government services	IdP: Financial institution in the jurisdiction RP : Not disclosed
Rate structure	Identity-verified information: Paid Information on unverified identity: Free	High authentication level information: Paid Low authentication level information: Paid	Identity-verified information: Paid Information on unverified identity: -
Demarcation of responsibility	Identity verified information: IdP responsibility Unidentified information: RP responsibility	Authentication level high: IdP responsibility Authentication level low: RP responsibility	RP takes full responsibility. ※As it is reference information

2-4. Problem solving (implications from advanced case studies)

(5) Division of responsibility in ID linkage services

- All of the ID linkage services 1 to 3 have a common point that IDs are linked through the platform of the ID linkage service.
- Responsibility of IDs varies depending upon the ID linkage service.
- Price of the IDs linked varies depending on the ID linkage service.

Account opening flow using digital identities created by other companies



2) ID linkage (focusing on the division of responsibilities)

5) Interoperability

2-4. Problem solving (Implications from advanced case studies)

(6) Initiatives of Standard Organizations: Trends of standardization that financial authorities should pay attention to, particularly

- The following table shows the standardization activities that are likely to have a significant impact on the identity management operations of financial institutions, along with the issues that each standardization activity will help to solve.

Organization name	Concerned Group	Outline of Activities	Status	Perspectives to watch	Target Issue
ISO	ISO TC 68 Financial services SC8 Reference data for financial services WG4	• ISO 17442-2: Development of a standard for legal entity identifier (LEI)	Completed	• LEI is an identifier that identifies legal entities in financial transactions, and its use in AML is being discussed.	2-3-5 Issues related to referencing data from financial institutions
	ISO TC 68 Financial services SC8 Reference data for financial services WG7	• ISO/DIS 24366: Standardization of Natural Person Identifier (NPI).	Discussions are underway to create the first version.	• NPI is a personal identifier and the first version is currently under review, but as with LEI, there is discussion of its use in AML and other applications.	2-3-5 Issues related to referencing data from financial institutions
OIDF	eKYC & Identity Assurance WG	• Consider the specifications of a standard to link metadata that indicates verification methods, etc., in addition to attribute information and extend the "Open ID Connect" ID linkage protocol	Implementation Draft2 has been released.	• Use cases that will lead to enhanced compliance with AML regulations are being considered, such as metadata linkage of verified attributes of individuals and information linkage of corporate related parties.	2) ID linkage (See details below.)
	FAPI WG	• Formulation of FAPI (Financial-grade API) 1.0	FAPI2.0 Implementation Draft1 issued	• Widely used for PSD2 support in UK Open Banking.	6) Interoperability
OIX	Digital ID for AML Banks in the Identity Market	• Discuss issues specific to finance, such as the use of AML services by financial institutions	Under consideration	• Implementing AML and other finance-specific initiatives	6) Interoperability

2) ID linkage (focusing on the division of responsibilities)

5) Interoperability

2-4. Problem solving (Implications from advanced case studies)

(6) Initiatives of Standard Organizations: Open ID Foundation eKYC & Identity Assurance WG

■ With regard to the technical specifications for the linkage of IDs among businesses, in addition to attribute information, inkage technical specifications have been developed that enable the linkage of metadata (laws and verification methods used as the basis for verification, etc.), which is the basis for the reliability of IDs, and the linkage of detailed information related to legal entities, thereby contributing to the enhancement of measures such as compliance with AML regulations and fraud prevention.

Directions to address issues

Before

- Although the WG developed technical specifications for linkage IDs, the WG was unable to share attribute verification rules, verification status, verification methods,etc. based on regulations and contracts, which are prerequisites to generate trust in linkage IDs.
- For legal entities, it is not possible to link the details of the legal entity and the information of the natural person (representative, etc.) acting on behalf of the legal entity.

After

- In this WG, the ID linkage protocol "Open ID Connect" will be extended and the ID linkage specification will be formulated to enable the linkage of metadata that indicates how it was verified in addition to attribute information.
- For legal entities, specification study is underway, starting from the linkage of information on natural persons acting on behalf of legal entities.

(more details are on the next page)

Background/ Success factor

✓ Made considerations based on demands for stricter regulations in the digital space due to the progress of digitization

Results

✓ Implementing improvement of measures such as compliance with AML regulations and fraud prevention by adding metadata about IDs and linking detailed corporate information

Future Issue

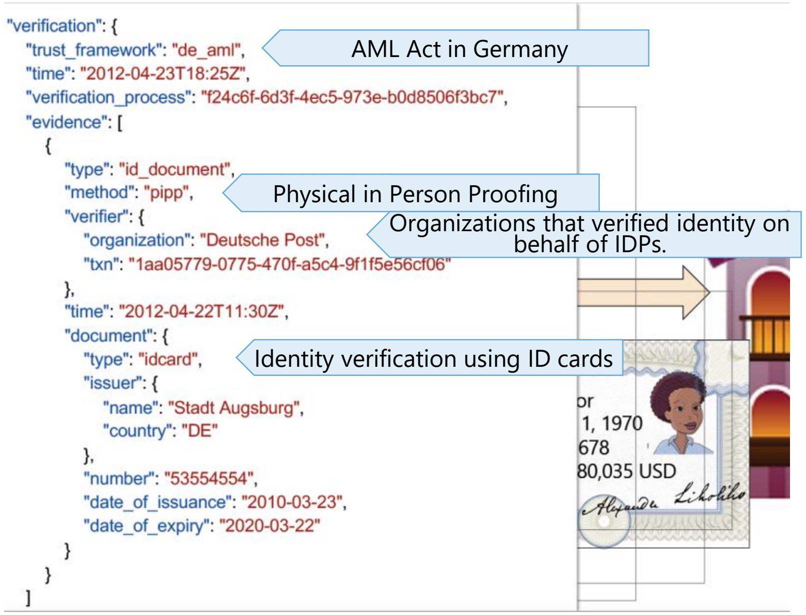
✓ Establishment of a legal system is required which corresponds with technical specifications, such as stipulation of laws and guidelines so that IDs based on the laws of other countries can be used reliably for financial institution operations.

(6) Initiatives of Standard Organizations: Open ID Foundation eKYC & Identity Assurance WG

Outline of Activities

- In the eKYC & Identity Assurance WG, specifications of OIDC4IDA are being worked upon which is a data format standard to extend the "Open ID Connect" identity linkage protocol to link attribute information and metadata information on how it was verified (attribute verification rules based on laws and contracts, verification methods, etc.).
- For legal entities, technical specifications for the linkage of “Authority Claims” that enables the acquisition of information on natural persons acting on behalf of legal entities, are being studied.

Image of ID linkage specifications for natural persons

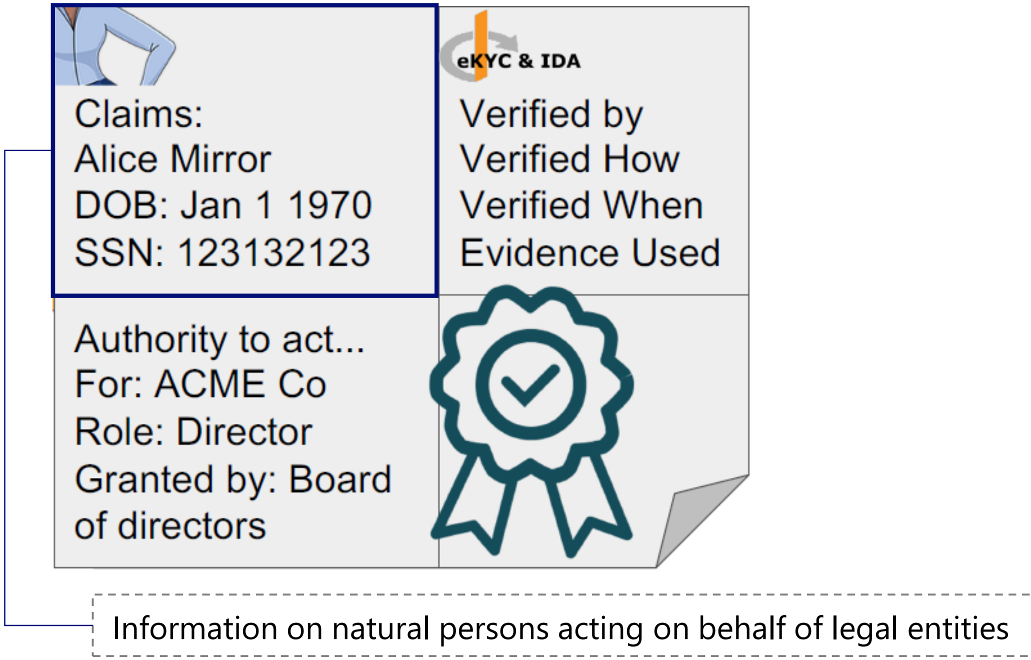


```
"verification": {
  "trust_framework": "de_aml",
  "time": "2012-04-23T18:25Z",
  "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
  "evidence": [
    {
      "type": "id_document",
      "method": "pipp",
      "verifier": {
        "organization": "Deutsche Post",
        "txn": "1aa05779-0775-470f-a5c4-9f1f5e56cf06"
      },
      "time": "2012-04-22T11:30Z",
      "document": {
        "type": "idcard",
        "issuer": {
          "name": "Stadt Augsburg",
          "country": "DE"
        },
        "number": "53554554",
        "date_of_issuance": "2010-03-23",
        "date_of_expiry": "2020-03-22"
      }
    }
  ]
```

AML Act in Germany
Physical in Person Proofing
Organizations that verified identity on behalf of IDPs.
Identity verification using ID cards
or
1, 1970
678
80,035 USD

Source: Overview of KYC Initiatives at Open ID Foundation Japan (2021)
https://www.slideshare.net/oidfj/openid-foundationjapankyc-openid-bizday-14

Image of ID linkage items for corporations
(Information in the blue frame is being considered currently)



Claims:
Alice Mirror
DOB: Jan 1 1970
SSN: 123132123

Verified by
Verified How
Verified When
Evidence Used

Authority to act...
For: ACME Co
Role: Director
Granted by: Board of directors

Information on natural persons acting on behalf of legal entities

Source: Same as left

2-4. Problem solving (implications from advanced case studies)

(7) Cross-border transactions with privately issued IDs

- Currently, private IDs penetration within a jurisdiction is a top priority, and we have not been able to have full-scale cross-border transactions using such IDs.
- The company plans to expand into cross-border services after the new eIDAS is enacted and the IDs become available throughout the EU.

Directions to address issues

Current

- When issuing the IDs, you need to visit a financial institution.
- Since the ID is compliant with both eID and eSignature [*1], it can be used in other adjacent jurisdictions, but it is practically unexplored in cross-borders.
- Government IDs used to exist, but these IDs can now be used for both public and private services.

After the establishment of the new eIDAS

- Article 24 of the current eIDAS regulations has been revised and it is expected to allow issue such IDs without going over the counter.
- With the approval of the EU List of eIDAS Trusted Lists [*2], it will be available for use throughout the EU.
- The government of the jurisdiction is planning to issue its own eID(government ID), but it is expected to continue to dominate as a supplement to the privately issued ID.

Background/ success factor

- ✓ It is possible to select the level of certification according to the risk of the service provided.
- ✓ From the beginning, the design was implemented to ensure interoperability with IDs in adjacent jurisdictions.

Results

- ✓ Widespread among most adult citizens in the jurisdiction. (No full-scale cross-border implementation)
- ✓ IDs issued by private companies can be used to access public and private services inside and outside the jurisdiction.

Future Issue

- ✓ While the European Commission's authority over the IDs in question has been strengthened, the jurisdictional regulator's authority has weakened.

*1） Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures （replaced by eIDAS(2016.7)） https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093

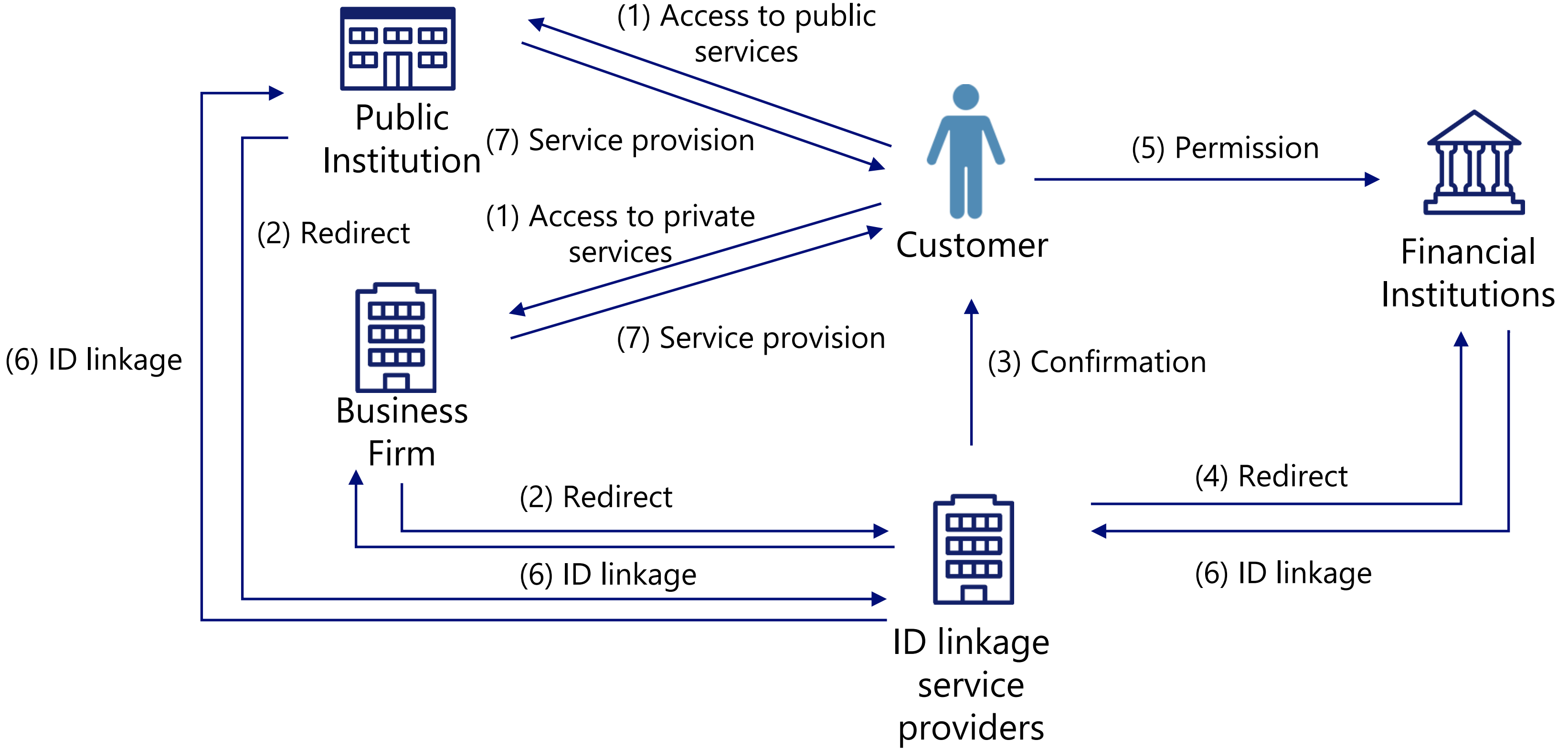
*2) the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists https://webgate.ec.europa.eu/tl-browser/#/

2-4. Problem solving (Implications from advanced case studies)

(7) Cross-border transactions with privately issued IDs

- ■ An ID is issued by opening an account at a financial institution.
- ■ It is possible to use public services and business services using that ID.

ID linkage flow using digital identities created by financial institutions

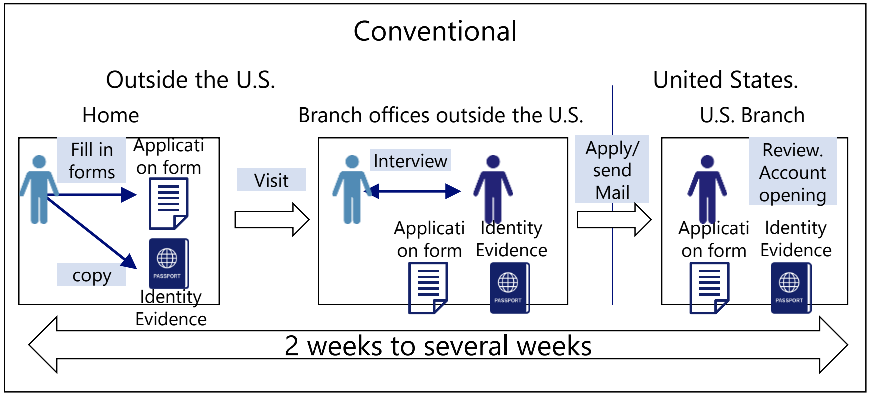


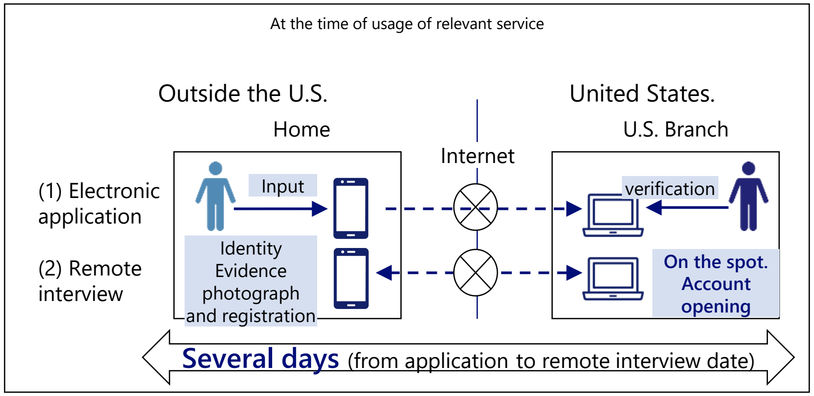
2-4. Problem solving (Implications from advanced case studies)

(8) Opening of cross-border accounts by major European financial institutions

- Only between jurisdictions where there are no restrictions such as firewall regulations and personal information protection rules, major European financial institutions are offering remote account opening services from outside the country for some customers only.
- Non-face-to-face risk is controlled by limiting it to the customers who have high status..

Directions to address issues




At the time of usage of relevant service
Outside the U.S.
Home
(1) Electronic application
(2) Remote interview
Input
Identity Evidence photograph and registration
Internet
United States.
U.S. Branch
verification
On the spot. Account opening
Several days (from application to remote interview date)

Background./ success factor

- ✓ Between jurisdictions that did not have restrictions such as firewall regulations and privacy rules, the information of customers having high status accounts was shared globally.
- ✓ There was a mechanism to open accounts in other countries using the relevant customer information.

Results

- ✓ Customers residing outside of the U.S. who have high status accounts can now open accounts in a short period of time through a simple remote procedure.
- ✓ Number of top status accounts in the U.S. is increasing.

Future Issue

- ✓ Although there is a need to realize services in other jurisdictions, it is difficult to do so among jurisdictions that have restrictions such as firewall regulations and personal information protection rules, or in jurisdictions that have not yet utilized digital identities.

Source: Compiled by NRI based on the website of the relevant financial institution and the contents of the press release.

2-4. Problem solving (Implications from advanced case studies)

(9) Interoperability of Public and Private Services in Australia

■ The Australian government expected that government IDs such as myGovID will not be used in the financial industry, and has developed the TrustID framework.

■ In addition to central banks and the financial industry, DTA is participating in this project, which aims to link and unify IDs among financial IdPs.

Directions to address issues

Before

- The Digital Transformation Agency (DTA) is the lead agency in developing the TDIF and certified myGovID (DTA) and DigitaliD (Postal Service) as IdPs on the TDIF.
- However, the application of TDIF to financial services did not proceed due to the time required for processing and the various restrictions placed on it.

After

- The TrustID framework to be designed by APC (Australia Payment Council) will be made interoperable with TDIF which is expected to enable mutual service access.
- By running IDs issued by private companies on both the TDIF and TrustID frameworks, it functions as an identity verification hub between IdPs and private and government RPs.

Background/ Success factor

✓ DTA and the Central Bank of Australia participated in the development of the TrustID framework to ensure interoperability with the TDIF.

✓ Involving the Postal Service has made it possible to manage administrative IDs using IDs issued by private companies.

Results

✓ It can be used for both customer ID management and authentication in the private sector and for national ID management, such as for receiving benefits from the government.

✓ It became possible to save cost in high value-added use cases, such as providing evidence of attributes for mortgage applications, etc.

Future Issue

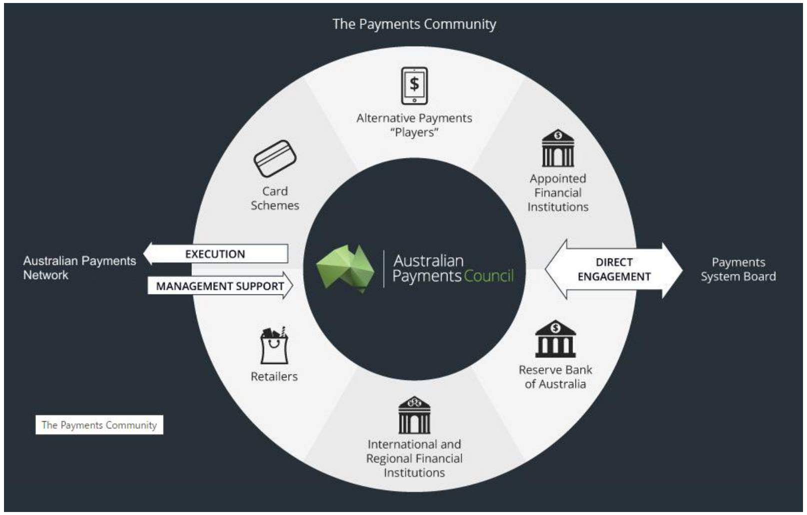
✓ The TrustID Framework is not certified by TDIF, and IDs issued by private companies are not certified by both TDIF and the TrustID Framework.

✓ There is no commercial framework other than IDs issued by private companies, and full-scale commercial operation is yet to come.

2-4. Problem solving (Implications from advanced case studies)

(9) Interoperability of Public and Private Services in Australia

- The PSB (Payment System Board) is a committee within the RBA that examines the efficiency and competitiveness of risk management/payment system of the financial system, and established the APC as a coordinating body with the payment industry.
- APC developed the TrustID framework as an alternative to government IDs, and also made it interoperable with TDIF to enable access to both public and private services.
- Some have argued that the background to the development of the TrustID framework, with the involvement of DTA and the Central Bank of Australia, is that it has become difficult for the government to expect that the IdPs on the TDIF, such as DTA's myGovID and the Postal Service's DigitaliD, will be widely adopted within financial services.


The Payments Community
Alternative Payments "Players"
Appointed Financial Institutions
Card Schemes
Australian Payments Council
EXECUTION
MANAGEMENT SUPPORT
Australian Payments Network
DIRECT ENGAGEMENT
Payments System Board
Retailers
Reserve Bank of Australia
International and Regional Financial Institutions
The Payments Community

(Reference) Organizations participating in the TrustID framework (as of 2019)

Bank

- Australia and New Zealand Banking Group Ltd
- Bendigo & Adelaide Bank Ltd
- Commonwealth Bank of Australia
- National Australia Bank Ltd
- Suncorp-Metway Ltd
- Westpac Banking Corporation

Payment

- eftpos Payments Australia Ltd
- MasterCard Asia/Pacific (Australia) Pty Ltd
- Visa AP (Australia) Pty Ltd
- PayPal Pty Ltd
- Cuscal Ltd

Other Services

- Coles Group Ltd (Retail)
- Woolworths Ltd (Retail)
- Optus (Communication)
- Australian Postal Corporation(Postal Corporation)

Administrative agencies, etc.

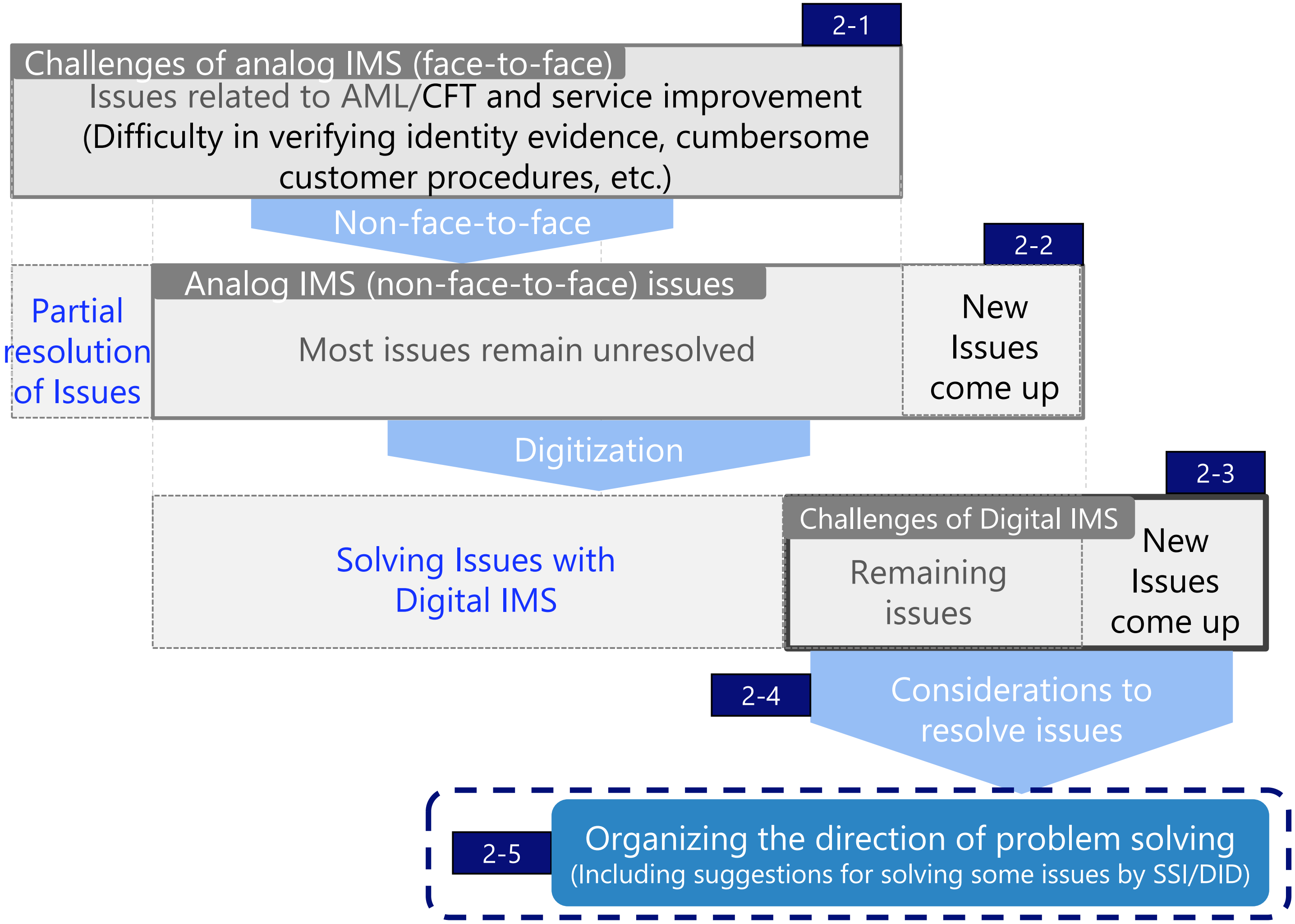
- Digital Transformation Agency
- Reserve Bank of Australia

Source: DTA HP, APC annual report 2019, it news

2-5. Organizing the direction of problem solving

2-5. Organizing the direction of problem solving

Subject of discussion in this section



2-1

Challenges of analog IMS (face-to-face)

Issues related to AML/CFT and service improvement (Difficulty in verifying identity evidence, cumbersome customer procedures, etc.)

Non-face-to-face

2-2

Partial resolution of Issues

Analog IMS (non-face-to-face) issues

Most issues remain unresolved

New Issues come up

Digitization

2-3

Solving Issues with Digital IMS

Challenges of Digital IMS

Remaining issues

New Issues come up

2-4

Considerations to resolve issues

2-5

Organizing the direction of problem solving
(Including suggestions for solving some issues by SSI/DID)

Summary of considerations in this section

- As discussed in the previous section, there have been advanced examples in overseas countries that address various issues for the establishment and operation of a digital IMS.

- In this section, the direction of solutions to the "identity management issues that have not been solved by digital IMS and new issues that will come up with digital IMS" listed in 2-3-8 will be re-organized based on the examples listed in 2-4.
    - Issues that are expected to be solved through the use of SSI/DID will continue to be discussed in Chapter 3. 2) Some of the issues related to identity coordination and 3) Some of the issues related to privacy are applicable.

- On the other hand, in promoting specific problem solving, it is assumed that there are multiple stakeholders, each with different concerns. The issues in promoting problem solving will be discussed in Chapter 4, where the possible stakeholders and their concerns will be organized and the approaches to solving them will be discussed.

List of issues to be considered in this section

■ Issues mentioned in the table below are in scope as discussed in 2-3-8.

Perspective of the issue	Issue
1) IAL	• Develop a regulatory framework to promote appropriate use of digital IMS.
2) ID coordination (focusing on the division of responsibilities)	• Inadequate business model and division of responsibilities among ID linking parties • Increased dependence on specific financial institutions (IdPs)
3) Privacy (Consent management, data minimization)	• Consent management burden for ID linkage • Maintenance burden of data license to utilize customer data across multiple services • As a data provider, burden of handling customer consent regarding the provision of information to third parties is high. • The burden of providing information to a third party is too great for the data recipient. • Increased risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization
4) Financial inclusion	• Financial exclusion of people who are not digitally compatible
5) Interoperability	• Burden of dealing with complicated ID linkage specifications
6) Investment decisions for transitioning to new operations	• Difficult to make investment decisions with regards to making changes in existing and optimized operations to use digital IMS
7) Issues in cross-border transactions	• National differences in AML/CFT regulations and legal barriers to cross-border data sharing in implementing FATF standards and other regulatory and supervisory requirements

2-5-2. Direction of solutions for each issue

1) Details of “IAL” issues, examples of initiatives, and suggestions obtained

Category	Issue	Issue description	Examples of Initiatives and Implications
1) IAL	• **Develop a regulatory framework to promote appropriate use of digital IMS.**	• FATF guidance points out that it is necessary to use a system that ensures an IAL that is appropriate for regulatory purposes such as AML/CFT. There is a suggestion[*1)] • In order to maintain an appropriate IAL, the IAL and the identity verification rules are integrated (= the identity verification rules are stipulated so that financial institutions can use highly reliable digital IMS appropriately according to the risk.) Is desirable. However, currently, although there are provisions for identity evidence in each jurisdiction, they are not clearly linked to the IAL, and there is room for improvement.	• As a countermeasure, it is possible to set an appropriate IAL and develop AML / CFT regulations that are combined with the IAL. • As an approach to maintenance, assuming that highly reliable IDs will be widely used, the case suggests a measure to develop AML regulations for that. (Case(2)(3)) • In developing specific AML / CFT regulations, it is necessary to give each financial institution room for ingenuity in consideration of the incorporation of technological innovation. • Also, regarding the scope of IAL maintenance, it is possible to take measures such as stepping up to the assurance level of customer attributes required for AML support without specializing in identity verification (Case(1)).

*1)FATF Guidance on Digital Identity (March 2020 http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

2) Details of “ID linkage” issues, examples of initiatives, and suggestions obtained

Category	Issue	Issue description	Examples of Initiatives and Implications
2) ID linkage	• **Inadequate business model and division of responsibilities among ID linking parties**	• When implementing ID coordination among financial institutions, it has been pointed out that the ID coordination business will not be viable if the following points are not in place. • Clarification of the scope of responsibility of the identity provider to guarantee the ID linkage (whether it is limited to identity verification (IAL: ID Proofing) or KYC beyond identity verification (+Due Diligence), etc.). • (2) Distribution of responsibility in the event that a customer or a financial institution to which IDs have been linked suffers some damage due to a data error. • In order to implement new account opening and continuous customer management, it is necessary to clarify the rules and responsibilities for ensuring the freshness of data when linking IDs, since the data must be fresh enough to be acceptable in practice. • Agreement on compensation commensurate with the division of responsibility for the above three points	• The division of responsibilities has been clarified as below, through consultations among the concerned parties(case(5)). – Clarification of the scope of responsibility that the ID issuer guarantees when linking IDs – In order to open a new account and carry out Ongoing Due Diligence, it is necessary to have latest data that is acceptable in practice, so the rules and responsibilities to ensure that the data is latest, when linking IDs are clarified. – Clarification of the boundary of responsibility in the event that a customer or a financial institution using an ID suffers some kind of damage due to a data error.
	• **Increased dependence on specific financial institutions (ID providers)**	• When a customer opens an account with multiple financial institutions using an identity issued by one financial institution (hereafter referred to as the identity provider), the dependency on the identity provider increases, and there are concerns about risks. For example, if a problem is discovered in the verification of the identity provider, there is a concern that the services of all the financial institutions to which the identity is linked will be affected, such as being suspended. • Furthermore, if a problem occurs with a financial institution that is an ID provider, users who rely on IDs issued by that financial institution may suffer damage en masse, and there is concern that the impact will be magnified.	• In order to reduce the dependency on a specific ID provider, SSI/DID is considered to be one of the solutions to the issue, as discussed in Chapter 3, so the discussion will be continued in Chapter 3.

3) Details of “Privacy” issues and examples of initiatives and suggestions obtained

Category	Issue	Issue Details	Examples of Initiatives and Implications
3) Privacy	• **As a data provider, the burden of dealing with customer consent regarding the provision of information to third parties is high.** • **The burden of providing information to a third party is too great for the data recipient.** • **Maintenance burden of data license to utilize customer data across multiple services**	• Due to the personal information protection legislation, when linking IDs, consent management with regards to providing information to a third party is required between the linking source and the linking destination. • Regarding consent management related to providing information to a third party, following burden will increase as ID linkage expands. (burden on the data provider) –Burden of explaining data utilization to customers –The burden of managing consent with customers, including the creation and storage of consent records (burden on the data receiver) –The burden of confirming the data acquisition process to the data source –The burden of explaining the purpose and content of data utilization to data providers and gaining their understanding	• Since this is a legal response, measures in accordance with the personal information protection laws of each country need to be taken. • In the mid-to-long term, there is also the idea of reviewing the form of third party provision itself and reducing the burden by using the SSI/DID mechanism and having customers agree on data utilization with each company based on their own sovereignty.

3) Details of “Privacy” issues and examples of initiatives and suggestions obtained

Category	Issue	Issue Details	Examples of Initiatives and Implications
3) Privacy	• **Increment in risk of discrepancies between customers and financial institutions regarding the purpose and scope of data utilization**	• The following points have been pointed out as issues in interviews with domestic experts. -If the explanation of data use from financial institutions is unclear, customers may be concerned that their data may be used in ways they do not intend. - On the other hand, it is difficult for individuals, in particular, to fully understand the explanations given by financial institutions and to verify whether the financial institutions are using the data as explained. - As a result, there are cases where the customer agrees for the time being and allows data to be used in ways that the customer did not intend.	• It is considered necessary for financial institutions to provide management functions that allow customers to correctly recognize how the data provided by users will be used by financial institutions, etc., rather than obtaining formal consent. • In addition, it is considered necessary for a third party to audit the financial institution in order to verify that the above management function itself is functioning correctly. • Moreover,an information bank could be one solution. The information management is entrusted to the information bank, which is responsible for providing the data. In some cases, consumer groups have established certification systems for information banks. *1)

*1) "Information Bank" certification system by the Information Technology Federation of Japan https://www.tpdms.jp/system/index.html

2-5-2. Direction of solutions for each issue

4) Details of "Financial Inclusion" issues, examples of initiatives, and implications

Category	Issue	Issue Details	Examples of Initiatives and Implications
4) Financial inclusion	• **Financial exclusion of people who are not digitally compatible**	• Regarding concerns about financial exclusion from the perspective of digital infrastructure development, the FATF guidance points out the following. *1) • In areas where it is difficult to utilize digital infrastructure due to reasons such as mobile phones and smartphones not being sufficiently widespread and areas where Internet access is limited, there is a concern that promotion of digitalization will lead to financial exclusion. • Regarding concerns about financial exclusion from the perspective of digital literacy, interviews were conducted with overseas experts where following has been pointed out. • Elderly people comprise majority of the population of non-digitized people and the reason they hesitate to use digital services and mobile phone banking apps is that they fear of incorrect usage, such as making a mistake. It is a mental barrier such as fear of pushing a button and sending money to the wrong place.	• Responses will depend on the current state of business development of financial institutions in each country and the political system in each country. –The policy is to develop digital identity infrastructure (identity management infrastructure and payment infrastructure) nationwide, and to incorporate all citizens digitally (Case(2) Singapore, (3) India). –There is a policy to acceptboth analog and digital forms, utilizing existing operations as well. (Japan and other developed countries) . –There are policies where a role similar to that of an existing administrative scrivener has been established to handle operations on behalf of minorities. –Since digitization is also being used to strengthen compliance with AML regulations, it is necessary to take measures that balance the strengthening of AML regulations and financial inclusion.

*1)FATF Guidance on Digital Identity (March 2020) http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

5) Details of “Interoperability" issues, examples of initiatives, and suggestions obtained

Category	Issue	Issue Details	Examples of Initiatives and Implications
5) Interoperability	• **Burden to handle complicated ID linkage specifications**	• The following issues regarding the burden of ID linkage have been pointed out in interviews with domestic experts. –If each financial institution implements a digital IMS based on its own specifications, it will be necessary to support connections based on a different set of technical specifications for each connection betweenfinancial institutions when they perform identity coordination. –This will lead to an increase in the connection burden, which in turn will result in ID linkage not working as a business because it will not lead to an increase in ID linkage, customers will not be able to use digital identities widely, and the speed of the spread of digital identities throughout society will not increase.	• There are also examples of public-private partnerships for the development of technical specifications and related laws and regulations, aiming at wide dissemination throughout society (Case(10)). • The issues on the left are mainly related to the scope of one jurisdiction, but the same applies to the interoperability of technical specifications across countries, and the standardization of ID linkage specifications is being promoted globally (Case(6)Initiatives of standardization organizations). • The following was pointed out in the interviews with domestic experts. – Implementation burden would be enormous even if each country were to have separate specifications. – For this reason, unification of international standards is seen as more desirable by vendors and others. – Vendors consider implementation of each country’s specifications to be very complicated, and are actively participating in global standardization activities such as ISO activities. • In addition to the development of standards, mechanism to verify compliance with the standards and ensure their correct dissemination, such as the development of a certification program, are also coming out. （Example）FDX(Financial Data eXcahnge) [*1)] – It also provides a mechanism to mechanically verify compliance and certify standards compliance. – Verify the parts that can be shared globally and the parts that depend on each country's system. (Test procedure for FDX Certificate) 1st test: OIDF Certificate (FAPI ConformanceTest) 2nd test: Test according to each country's specific requirements

[*1)]FDX Press-Release “Financial Data Exchange, OpenID Foundation Take Step Towards Global Standard for Financial Data Sharing” (March 2019)
https://openid.net/2019/04/02/financial-data-exchange-openid-foundation-take-step-towards-global-standard-for-financial-data-sharing/

2-5-2. Direction of solutions for each issue

6) Details of “Investment decisions to be made for transitioning to new operations” issues, examples of initiatives, and suggestions obtained

Category	Issue	Issue Details	Examples of Initiatives and Implications
6) Investment decisions to transition to new operations	• **Difficult to make investment decisions with regards to making changes in existing and optimized operations to use digital IMS**	• The following issues have been pointed out in interviews with domestic experts. –The initial investment for the use of digital IMS is purely an additional cost during the transition period from analog IMS, and it is difficult to find an incentive to change the current optimized operations to accommodate it. –It is necessary to continuously invest in security and other measures in line with technological progress, but it is difficult to determine to what extent investment should be made to keep up with the latest technology. –It is difficult to formulate a monetization plan for a new initiative alone. It is necessary to create a plan that takes into account the reduction of existing costs associated with the transition from existing processes.	• Cost recovery by monetizing one's own identity information can be considered as a countermeasure (case 5 (ID coordination)). • There is also the idea of considering it as a comprehensive measure that takes into account the effect of reducing existing operation costs and reduction of cost *1) by reduction in theft and fraud, rather than the profit recovery model of recovering investment by the ID linkage business alone. • In addition, when using national ID as identity evidence, the national government and authorities need to consider the maintenance cost of national ID from the viewpoint of popularization cost in addition to infrastructure cost *2), and on the financial institution side, it is important to make irreversible investment according to the status of national ID rule development and popularization*1). These have been pointed out in the literature.

*1) WorldBankGroup, Private Sector Economic Impacts from Identification Systems https://elibrary.worldbank.org/doi/pdf/10.1596/31828

*2)WorldBankGroup, Public Sector Savings and Revenue from Identification Systems:Opportunities and Constraints https://documents1.worldbank.org/curated/en/745871522848339938/pdf/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf

2-5-2. Direction of solutions for each issue

7) Details of “Various issues in cross-border transactions” issues, examples of initiatives, and suggestions obtained

Category	Issue	Issue Details	Examples of Initiatives and Implications
7) Issues in cross-border transactions	• **National differences in AML / CFT regulations and legal barriers to cross-border data sharing in implementing FATF standards and other regulatory and supervisory requirements**	• Financial institutions are required to collect information on the source and destination of overseas remittances in excess of a certain amount. • FSB states that there are following legal barriers to verify remittance source and remittance destination. – Due to differences in AML/CFT regulations in different countries, the level of strictness of identity verification varies, raising concerns about the reliability of the information. – When it is necessary to share personal information about the remittance source and remittance destination across national borders, there are cases where data protection legislation of each country becomes a barrier.	• The FSB has prepared a roadmap for addressing the issues mentioned on the left, and continues to discuss the policy for addressing them (2-3-5 [AML / CFT] Refer to trends related to issues of cross-border transactions). • There are some individual moves being made by financial institutions and jurisdictions, such as trying to improve the efficiency of cross-border transactions by using an eID that can be used in a wide area such as the EU (case(7)), or accepting the opening of accounts from abroad by limiting customers to wealthy individuals and allowing them to bear the burden of operations (case(8).)

2-6. Conclusion of this chapter

Conclusion of this chapter

- The importance of digital identity has been recognized in the financial sector, and the establishment of a reliable digital IMS is expected to enhance compliance with AML regulations and eliminate many of the burdens of verifying identity evidence and other analog-based tasks. The results of the study are as follows

- For this reason, as in the overview of digital identity described in Chapter 1, It is becoming a federation model identity management system and the use of digital identity is expected to progress. In this way, the use of digital identities is expected to progress. The fact that banks have become IDPs in some cases, and that there are high expectations for their role as IDPs, is also expected to support this trend.

- In order to achieve this, it will be necessary to resolve issues such as regulatory development, division of responsibilities, development of technical specifications, privacy, consideration of financial inclusion, and investment for transitioning to new operations. In this chapter, we have summarized the directions for solving these issues by referring to precedent cases, etc. However, the actual resolution of these issues will require consultation among stakeholders such as regulators, financial institutions, and customers. The resolution of issues related to the promotion of consultations will continue to be discussed in Chapter 4.

- In addition, there is an expectation that the use of SSI/DID will further improve the response to dependence on specific financial institutions (ID providers) and privacy issues that have been identified as challenges for digital IMS. This point will be continued to be discussed in Chapter 3.

Chapter3 Self-Sovereign Identity (SSI) & Decentralized Identity (DID)

Overview of the Chapter

3-1. Summary of SSI/DID

- We summarized the discussion trends regarding Self-Sovereign Identity (SSI) as an idea and the Decentralized Identity (DID) that is being considered as means to realize SSI.
- Since there is no established standard for IMS based on the SSI model at this time, we defined the possible implementation visions of SSI/DID with DID in this study, based on typical use cases. As a result, we derived the following four characteristics:
  1. Separation of Authentication and Attributes, 2. Utilization of Distributed Attribute Information and Selective Presentation, 3. Confidentiality of Presentation Destination (ensuring unlinkability), 4. Long-term Storage and Usage of Digital Identities

3-2. Elements Required in order to Realize SSI/DID

- We looked at the implementation methods proposed by several standardization organizations, and we extracted and organized the necessary components from both technical and control perspectives for the realization of the same characteristics.

3-3. Major SSI/DID Preceding and PoC Projects

- We summarized the precedent cases and PoC cases of SSI/DID. In particular, Verified.Me in Canada and Alastria_ID/Dalion in Spain, which have been attracting attention as advanced cases, are summarized in detail.

3-4. Advantages of SSI / DID and Issues Toward Realization

- In SSI/DID, by utilizing the four characteristics, the following advantages can be expected: (1) Self-sovereignty acquisition, (2) Privacy consideration, (3) Improvement of convenience and cost control for the entire industry.
- On the other hand, there are issues that need to be continued to consider from the following perspectives:
  (1) technology, (2) legal/public systems, (3) operation, and (4) business.
  In addition, these issues include "decomposition of responsibilities" and "study of compatible use cases," which were faced in the past when SSI was implemented using the federation method. This indicates that the same challenges need to be continued to consider even if the method is changed to SSI/DID.

3-5. Financial Regulatory Issues in the Use of SSI/DID

- We analyzed financial regulatory issues when deploying SSI/DID into financial transactions. Unique issues for SSI/DID, we identified and discussed (i) approach to financial regulation of Wallet and (ii) Legal treatment of new identification information .

3-1. Self-Sovereign Identity (SSI)/Decentralized Identity (DID)

Main Points of this Section

Overview of SSI and DID

- SSI is "an idea that aims to allow individuals to control their own identity without the intervention of an identity management entity”.
- DID is “a mechanism that aims to reduce the dependence of a user's digital identity on a particular IdP”.

Characteristics of SSI/DID

- Based on the definitions regarding SSI/DID, the following four characteristics were identified.

Items to be Realized	Overview
Separation of Authentication and Attributes	• Separate Recognition (authentication) and Selfness (attribute information), to decrease dependency on specific IdP(s). • The claim provider (CP) issues attribute information in the form of an assert to a DID, and then authenticates the claim to the relying party (RP) using the DID.
Utilization and Selective Presentation of Distributed Attribute Information	• Obtain and assert claims from multiple CPs • Present selectively from Wallet to RP
Confidentiality of Presentation Destination (Unlinkability)	• By asserting claims via Wallet, claims are asserted to the RP while keeping where the claims are sent to CP confidential.
Long-term Storage and Usage of Digital Identities	• By storing the materials used to verify issued claims in a distributed repository for a long period of time, it is possible to verify claims issued in the past even if the CP no longer exists. (Some standardization organizations propose methods to ensure the integrity and transparency of materials required for verification by adopting technologies with immutable characteristics such as blockchain for the distributed repository.

3-1-1. Complete Picture of SSI/DID

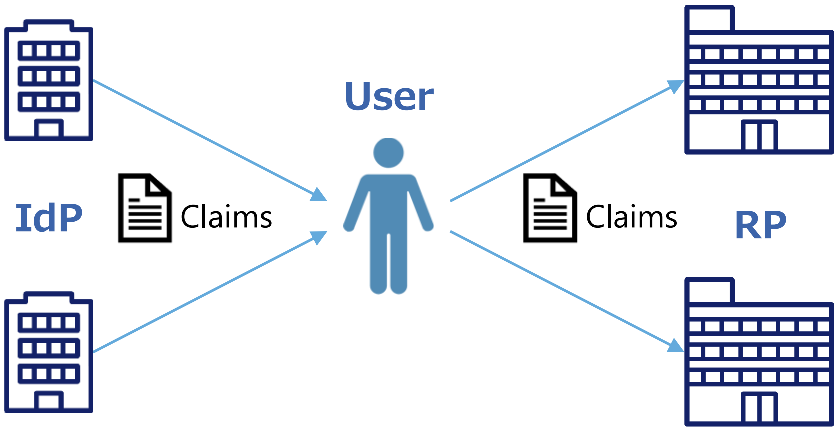
What is Self-Sovereign Identity (SSI)?

- SSI is an idea that aims to allow individuals to control their own identity without intervention of an identity management entity(*).

  *: Sovrin Foundation, https://sovrin.org/faq/what-is-self-sovereign-identity/

- After ensuring that the user has the right to control their own attribute information, information issued by a trusted organization can be obtained and asserted to RPs and other organizations within the scope permitted by the user.

Conceptual Diagram of SSI



[Example]

→ Flow of Claim

What is Decentralized Identity (DID)?

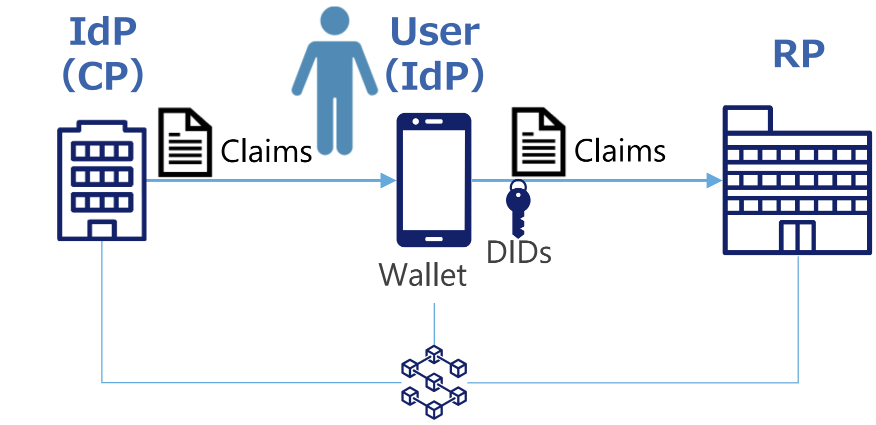
- While SSI aims to allow users to control their own digital identity, Decentralized Identity (DID) aims to reduce the dependency of a user's digital identity on a specific IdP.
- In order to achieve this, the use of distributed repositories such as blockchain is often proposed. For example, Microsoft, which has published a white paper on distributed identity, defines it as follows(*).

> “Decentralized identity is a trust framework that replaces identifiers such as usernames with self-owned, independent identities and enables data exchange using blockchain and distributed ledger technologies to protect privacy and secure transactions. ”(Microsoft)

※ : Microsoft, https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain

- In order to implement the DID concept, the World Wide Web Consortium (W3C), for example, is considering the following two technologies.
  - Decentralized Identifiers (DIDs)
  - Verifiable Credentials (VCs)

Conceptual Diagram of DID



Distributed repositories (e.g., blockchain)

[Example]

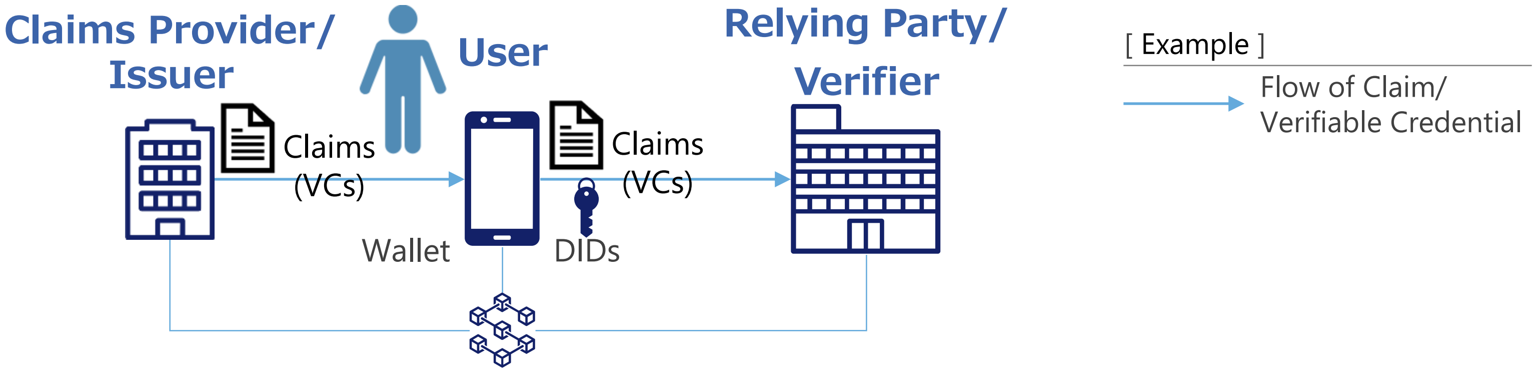
→ Flow of Claim

3-1-1. Complete Picture of SSI/DID

This Study on SSI/DID and Terminology in Standardization Organizations

- SSI/DID specifications are being developed by the standardization organizations listed in Section 3-2-2, and the names of concepts in SSI/DID differ depending on the organization.
- For this reason, the names of concepts related to SSI/DID in this study will continue to be based on the terminology used in Section 1-1, "Major Actors Constituting IMS," which is based on ISO/IEC24760-1 and OpenID Connect Core 1.0. While the following terminology will be used in W3C and other organizations to explain the figures and specifications.

This study on SSI/DID and terms by W3C



#	Terms in this Study	Terms in W3C	Definitions of Terms in this Study	Definitions of Terms in W3C*
1	Claim	・ Verifiable Credential	・ Some attribute sets of entities that are identities	・ A set of attributes of an entity that has a cryptographically verifiable creator and is tamper-evident.
2	Claims Provider: CP	・ Issuer	・ Entity that provides a claim	・ An entity that asserts a claim, generates a Verifiable Credential from the claim, and sends the Verifiable Credential to the holder.
3	Relying Party: RP	・ Verifier	・ Entity that relies on the verification of identity information for a particular entity	・ Entity that receives the Verifiable Credential

※Source) Created be NRI based on Verifiable Credentials Data Model 1.0 1.2 Ecosystem Overview https://www.w3.org/TR/vc-data-model/

3-1-1. Complete Picture of SSI/DID

The "Seven Laws of Identity" and Organization Policy for this Chapter

- As described in Section 1-3, Kim Cameron has presented the "Seven Laws of Identity in SSI" based on the "Seven Laws of Identity", and specifically, Principles 5 and 6 have been updated.
- In this chapter, we will organize the components of SSI/DID based on these two principles.

#	Principles	Contents
1	Law of User Control and Consent	• Identity systems must only reveal information identifying a user with the user's consent.
2	Law of Minimal Disclosure For A Constrained Use	• The identity system must disclose the least identifying information possible, as this is the most stable, long-term solution.
3	Justifiable Parties	• Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
4	Directed Identity	• A universal identity system must support both "omni-directional" identifiers for use by public entities and "uni-directional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
5	Standardized identity hub	• User can represent him/herself and use identity in a consistent manner across providers, with identity being separated across the context at the same time
6	Standardized DID for long-terms identity stability	• After storing personal data in a way that it is not dependent on the operators, survive the identity operators and retain relationships with service
7	Human Integration	• Identity systems must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

3-1-2. Items to be Realized for SSI/DID

Items to be Realized for SSI

- Each standardizing organization (W3C, DIF, OpenID Foundation, etc.) has different protocols for implementation, but they all mention the following four items as the means to achieve Item 5 "Standardized identity hub(*)" and Item 6 "Standardized DID for long-terms identity stability" of the seven principles of SSI. The following four items are mentioned in both cases.

Items to be Realized	Overview
Separation of Authentication and Attributes	• Separate Recognition and Selfness (attribute information), which were previously the role of IdPs. • The claim provider (CP) issues attribute information in the form of an assert to the DID, and then authenticates the claim to the relying party (RP) using the DID.
Utilizing and Selectively Presentation of Distributed Attribute Information	• Obtain and assert claims from multiple CP • Present selectively from Wallet to RP
Confidentiality of Presentation Destination（Unlinkability）	• By asserting claims via Wallet, claims are asserted against the CP while keeping the RP to which the claims are sent confidential.
Long-term Storage and Usage of Digital Identities	• By storing the materials used to verify issued claims in a distributed repository for a long period of time, it is possible to verify claims issued in the past even if the CP no longer exists. (Some standardization organizations propose a method to ensure the integrity and transparency of materials required for verification by adopting technologies with immutable characteristics such as blockchain for the distributed repository.

(*) An identity hub is "a distributed, off-chain personal data store that puts the management of personal data in the hands of users”.

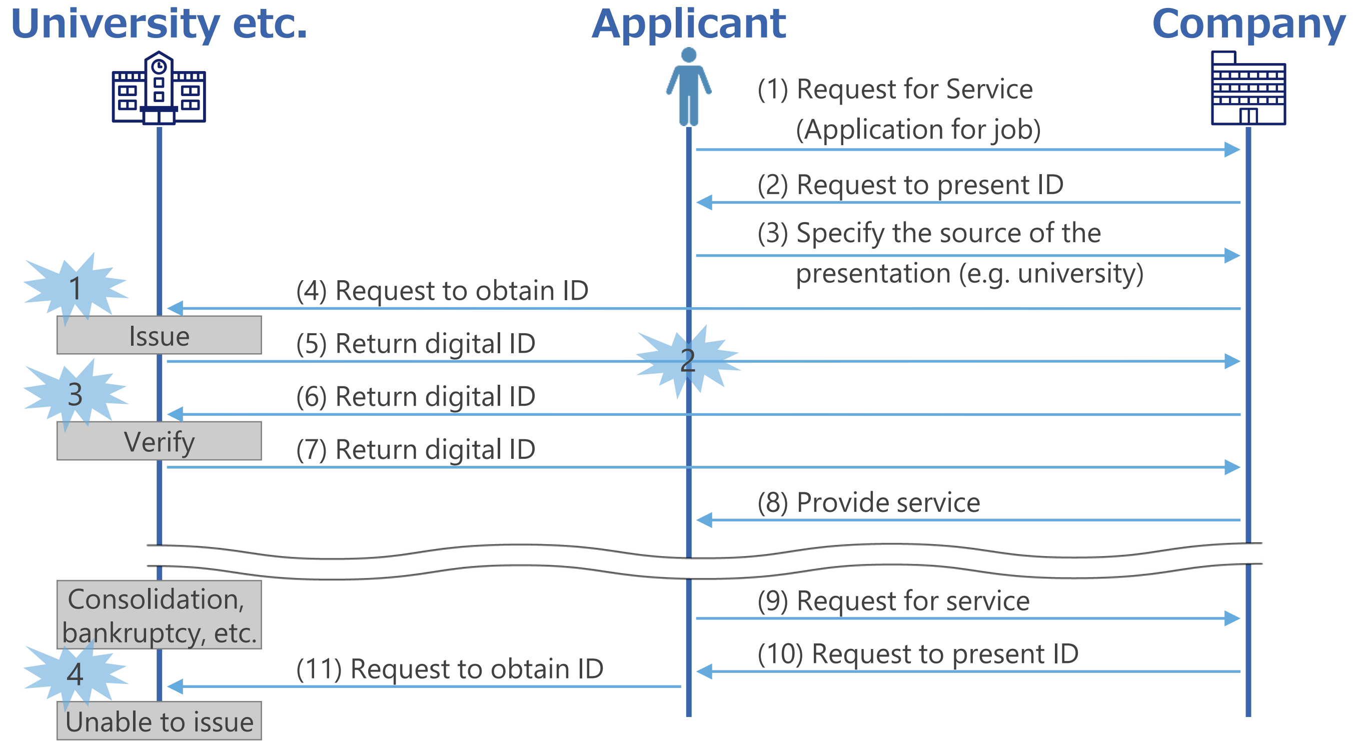
Source) Microsoft, “Identity Hubs as personal datastores” (Mar. 2019)}

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/identity-hubs-as-personal-datastores/ba-p/389577

Use Case: Presenting Diplomas to Companies when Job Hunting [Existing Model]

- In the use case that a job seeker presents the necessary documents (university diploma, transcript, etc.) to the company required, in the existing model using the current federation, the following flow is generally handled in the current existing model.
- The existing model relies heavily on IdPs (e.g. universities) to manage claims, which leads to the following risks.
  - When presenting claims, the user needs to be authenticated by the university. It will be difficult to obtain an ID as a result of being accredited by the university.
  - Applicants have no control over the information they present to companies.
  - Universities will know which companies they are applying to.
  - In the event of a university ceasing to exist in the future due to consolidation, bankruptcy, etc., it will not be possible to obtain a certificate from that university.

The case of presenting diplomas to employers when looking for job in existing model


University etc.
Applicant
Company
(1) Request for Service (Application for job)
(2) Request to present ID
(3) Specify the source of the presentation (e.g. university)
1
(4) Request to obtain ID
Issue
(5) Return digital ID
2
3
(6) Return digital ID
Verify
(7) Return digital ID
(8) Provide service
Consolidation, bankruptcy, etc.
(9) Request for service
(10) Request to present ID
4
(11) Request to obtain ID
Unable to issue

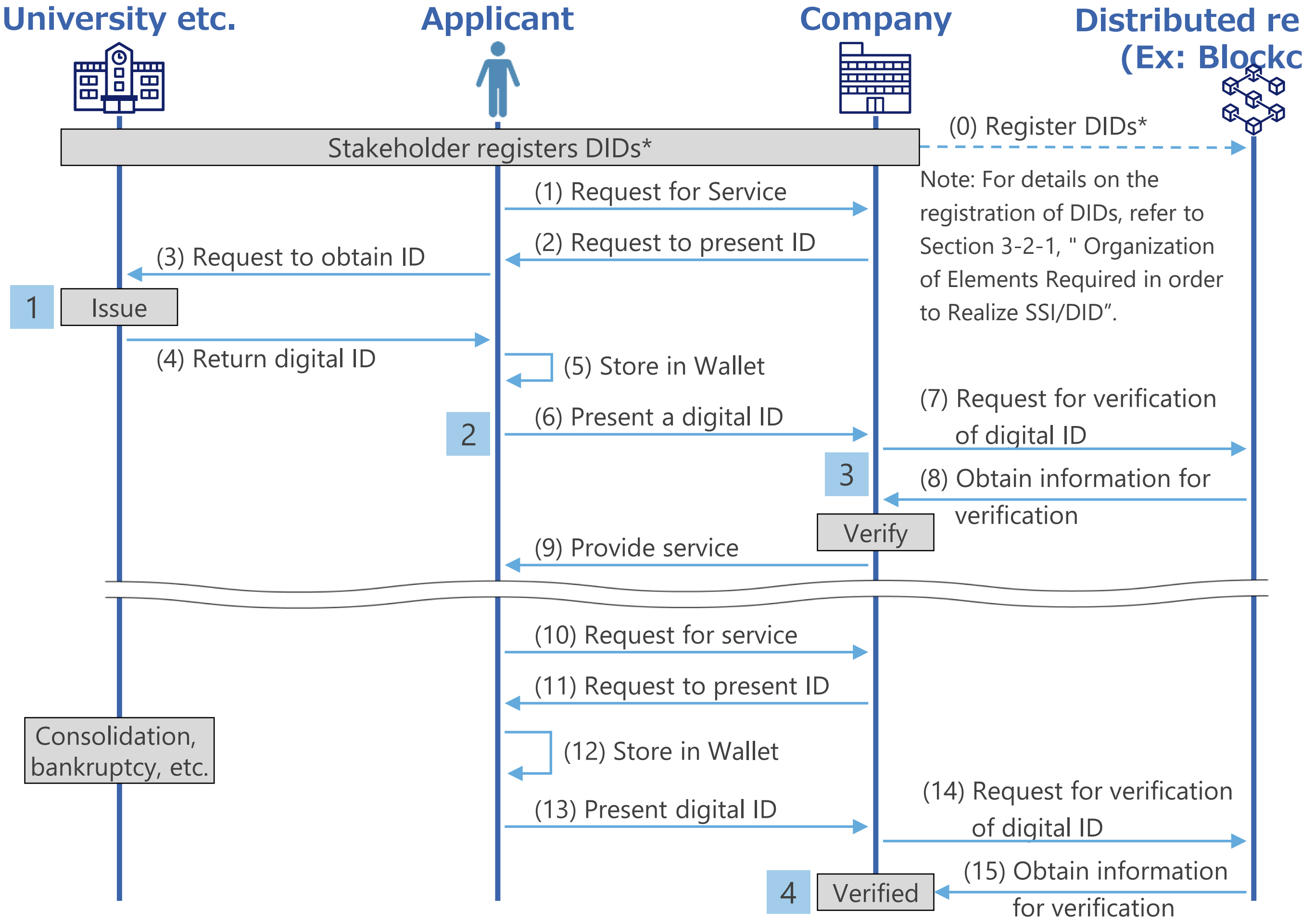
Potential risks in existing model

1. Banned accounts by the university, the IdP
2. No right to control the presentation of information including in the certificate
3. The university knows who to present claims to (the company) using the communication during issue/verification
4. Unable to reissue the claim

Use Case: Presenting Diplomas to Companies when Job Hunting [SSI Model]

- The SSI model is said to be a model that can solve these issues of existing models. Specifically, the features presented by the SSI model, such as (1) Separation of Authentication and Attributes, (2) Utilizing and Selectively Presentation of Distributed Attribute Information, (3) Confidentiality of Presentation Destination, (4) Long-term Storage and Usage of Digital Identities, have the potential to resolve the concerns of existing models.

The case of presenting diplomas to employers when looking for job in SSI model


University etc.
Applicant
Company
Distributed repository (Ex: Blockchain)
Stakeholder registers DIDs*
(0) Register DIDs*
(1) Request for Service
(2) Request to present ID
(3) Request to obtain ID
1
Issue
(4) Return digital ID
(5) Store in Wallet
2
(6) Present a digital ID
(7) Request for verification of digital ID
3
(8) Obtain information for verification
Verify
(9) Provide service
(10) Request for service
(11) Request to present ID
Consolidation, bankruptcy, etc.
(12) Store in Wallet
(13) Present digital ID
(14) Request for verification of digital ID
4
Verified
(15) Obtain information for verification

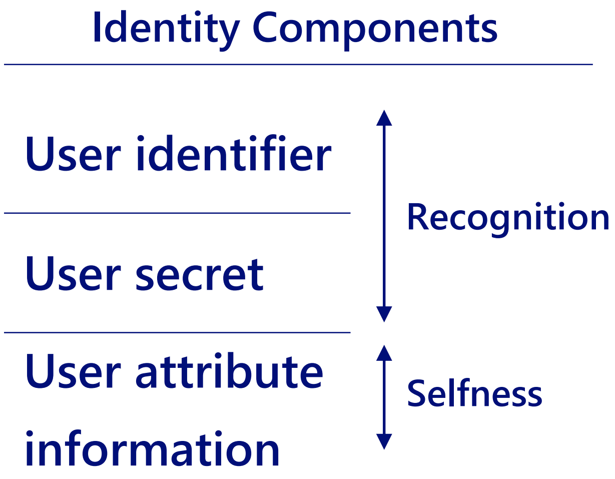
Note: For details on the registration of DIDs, refer to Section 3-2-1, " Organization of Elements Required in order to Realize SSI/DID".

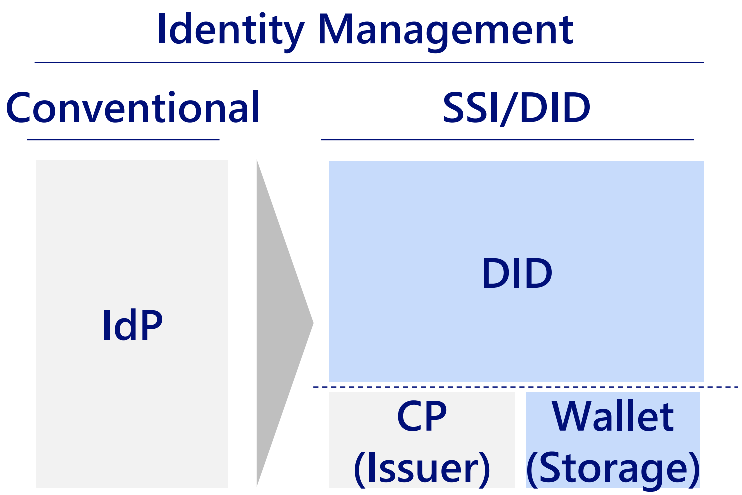
Features of the SSI model contributing to the elimination of risks in existing models

1. Separation of Authentication and Attributes
2. Utilizing and Selectively Presentation of Distributed Attribute Information
3. Confidentiality of Presentation Destination
4. Long-term Storage and Usage of Digital Identities

Items to be Realized for SSI - (1) Separation of Authentication and Attributes

- "Separation of Authentication and Attributes" is intended to separate Recognition (person authentication) from Selfness (attribute information).
  - Exchange of decentralized data is possible
    - Using the user's "wallet" as a hub for data storage, it is now possible to assert the obtained claims to various RPs. As a result, users can control their own personal information and provide value to various companies by providing the necessary information.
    - Separate credential information (identifiers such as user ID and secrets such as password) required for peer to peer facing authentication, and attribute information to be linked.
  - Reduce risks related with existing models
    - Unreasonable user account suspensions (account bans) by IdPs have made it impossible for users to obtain their own attribute information. In contrast, users can avoid account suspensions by using DID.
    - In addition to the CP, the wallet also holds the claim. Historical signatures using DLT and long-term signatures ensure the authenticity of the data at the time (makes IdPs to tamper difficult).



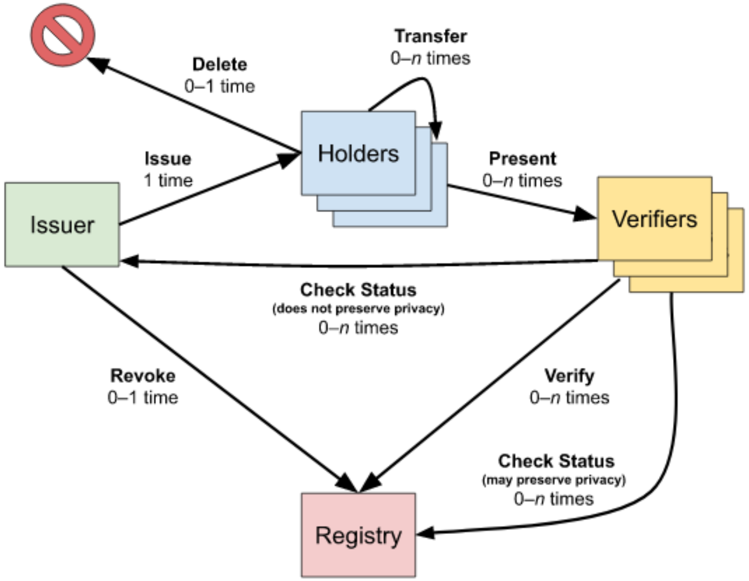


Items to be Realized for SSI - (2) Utilizing and Selectively Presentation of Distributed Attribute Information

■ "Utilizing and Selectively Presentation of Distributed Attribute Information" means that claims can be collected from scattered CPs and only those claims intended by the user can be deployed in the RP.

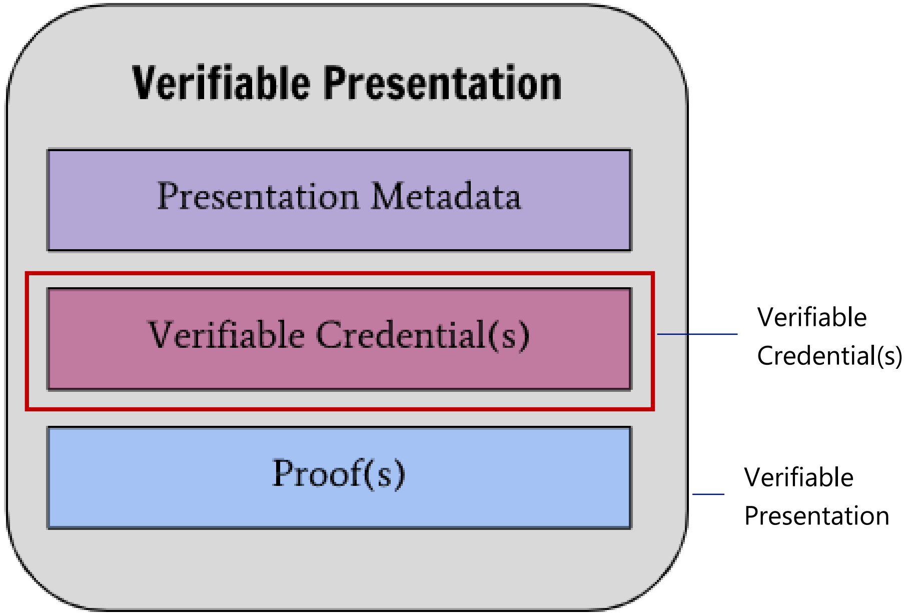
- For example, the "Verifiable Credentials Data Model" defined by W3C shows a model that allows users to bundle VCs obtained from claims providers and present them as a subset of their own persona (called Verifiable Presentation).

Verifiable credentials data model life cycle
For verifiable credential



In W3C, the role of issuing verifiable claims is defined as "Issuer"
and the role of "Verifier" as receiving claims and verifying their origin, authenticity, etc.

Conceptual diagram of verifiable credential(s) and verifiable presentation
In the verifiable credentials data model



Source) Verifiable Credentials Data Model 1.0
3.2 Credential 3.3 Presentations https://www.w3.org/TR/vc-data-model/

Items to be Realized for SSI - (3) Confidentiality of Presentation Destination （Unlinkability）

- "Unlinkability" is intended to allow the Holder to assert and verify claims without the CP knowing to which RP the issued claim was asserted.
  - After the RP receives the Claim, it needs to verify its authenticity (Verify). At that time, if the verification key used to verify the assigned signature value is sent to the CP, the issuer of the claim, the party to which the claim is asserted will be exposed.
  - By having the RP obtain the verification key by referring to metadata deployed in distributed repositories, etc., from the viewpoint of the above Claims Provider, the "user" who issued the Claims and the "RP" to which they are asserted will not be identified. (This satisfies CP-RP Unlinkable*).

*Follow the notation of ISO/IEC 27551

Overview of claims assertion via holder and claims validation mechanism in RP

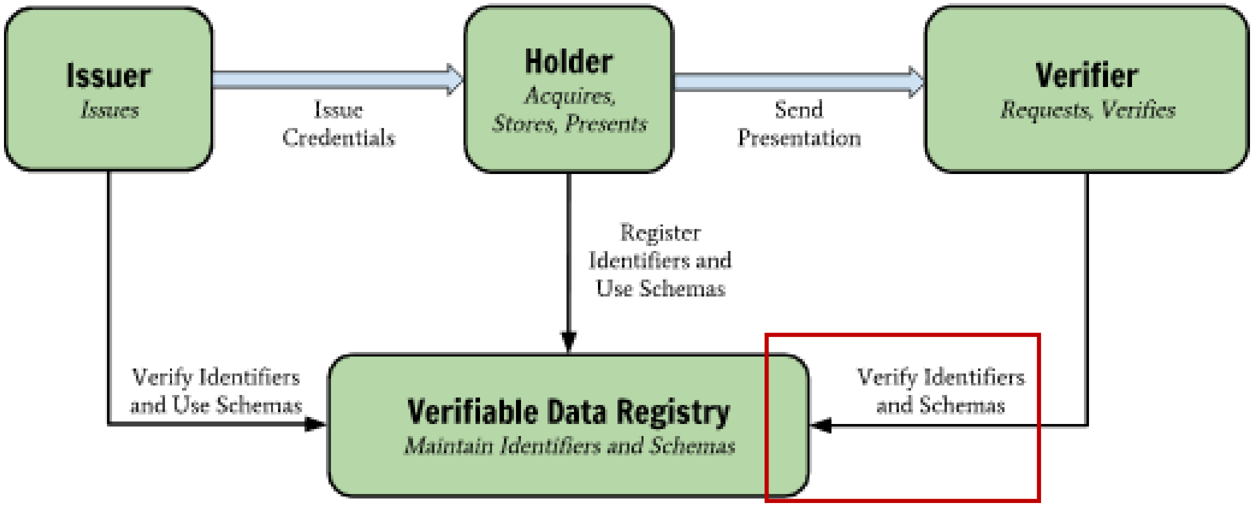

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

Figure 1 The roles and information flows forming the basis for this specification.

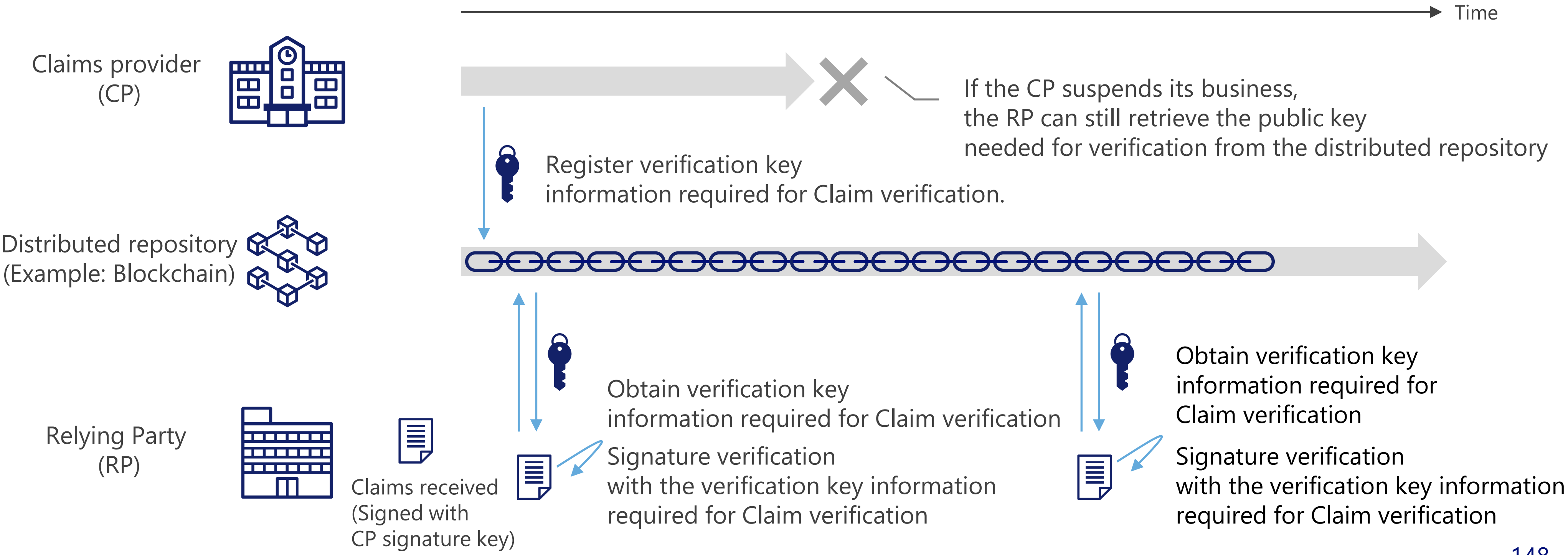
Source) Verifiable Credentials Data Model 1.0
https://www.w3.org/TR/vc-data-model/

Items to be Realized for SSI - (4) Long-term Storage and Usage of Digital Identities

■ "Long-term Storage and Usage of Digital Identities" is intended to ensure that once a Holder is issued, it remains available on a continuous basis, regardless of the status of the Claims Provider.

- For example, if the CP is a university, there is a possibility that the CP will no longer exist due to consolidation. Even in this case, it is possible to confirm that the claims issued in the past are legitimate (i.e., their authenticity is guaranteed).
- Even if the CP attempts to tamper with the contents of the Claims after they are issued, the authenticity of the Claims issued in the past can be verified.

Overview for long-term storage of digital identities


Time
Claims provider (CP)
If the CP suspends its business,
the RP can still retrieve the public key
needed for verification from the distributed repository
Register verification key
information required for Claim verification.
Distributed repository (Example: Blockchain)
Relying Party (RP)
Claims received (Signed with CP signature key)
Obtain verification key
information required for Claim verification
Signature verification
with the verification key information
required for Claim verification
Obtain verification key
information required for
Claim verification
Signature verification
with the verification key information
required for Claim verification

3-2. Elements Required in order to Realize SSI/DID

3-2. Elements Required in order to Realize SSI/DID

Main Points of this Section

- Organizing Components
  - There is no established standard for IMS based on the SSI model at this moment, but the four characteristics commonly appear in all models proposed by various standardization organizations. In this study, we defined a processing flow to realize these characteristics, based on typical use cases.

- Technical Aspects
  - As methods of realizing the SSI model, the protocols that are being developed by each organization to realize the processing flow described above and their outlines are organized.
  - As for the trends of interoperability, there are some trends of cooperation and convergence, such as the trends among organizations (liaison agreement between OpenID Foundation and DIF) and the trends of specification development (e.g. Presentation exchange/DID Comm, CHAPI/Verifiable Presentation Request). However, while some discussions on data models are under consideration, further convergence is expected for the communication layer and the utility layer.

- Control Aspects
  - When exchanging identity information among the participants in the IMS operation of the SSI model, it is necessary to maintain mutual trust before exchanging data. For this purpose, "Trust Framework" exists for to define the stakeholders participating in the system and assures the trustworthiness of the entire system by ensuring that each stakeholders of the system appropriately assume the roles and responsibilities.
  - The OIX Guide to Trust Framework, which is a guide for practitioners of the IMS trust framework, defines each stakeholder and the associated role including "Holder," which is a characteristic actor of the SSI model. Based on this guide, we organized the roles required of stakeholders in the SSI model and the control requirements that must be fulfilled.
  - As a result, it became clear that while the control requirements do not change from the conventional centralized and federation models' IMSs, there may be conflicts of interest among stakeholders that were not assumed in the conventional model, depending on which stakeholders play which roles in the SSI/DID model.

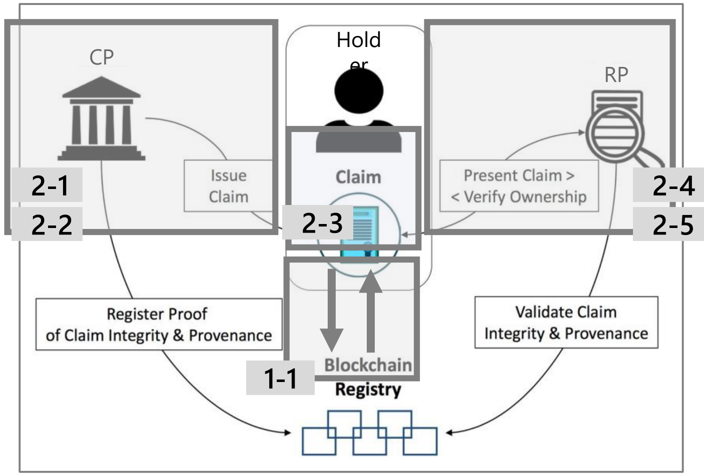
Definition of the Processing Flow

- For the use cases described in 3-1-2, processes for generation for DIDs and claims federation are defined.

1. DID registration process
   User performs ID Proofing, DID Activation process , and the DID is switched to the valid state.
2. Claim Federation
   The Holder becomes the IdP after obtaining the DID and performs the Claim assertion between the CP and Holder, and between the Holder and RP.

Process	Overview of the process
1. DID Registration Process (Process until the DID transitions to the valid state)	
1-1. Generation and registration of DIDs and metadata	Generation and registration of DID and metadata
2. Claim Federation	
2-1. Binding of a user on a CP and a DID owner	• The user authenticates to the CSP in the CP • CP receives from user "information that the user's DID held and controlled", checks the entity operating the DID and entity operating an account on the CP are the same, and then complete the binding
2-2. Claim issuance	Verify that a claim to be provided is for an entity requesting claim provision, and then issue a claim using the information received during 2-1)
2-3. Claim storage in the wallet	Store the claims received at 2-2) to the wallet
2-4. User authentication to RP	Mutual authentication between the wallet and RP, using the DID and its metadata from 1-1)
2-5. Claim assertion	• After mutual authentication at 2-4), assert claims received at 2-3) • RP verifies whether the received claim is issued on the binding with the DID of the user authenticated at 2-4) (Verification), and whether the asserted claim is valid (Validation)

Overview of the DID process flow



3-2-1. Organization of Elements Required in order to Realize SSI/DID

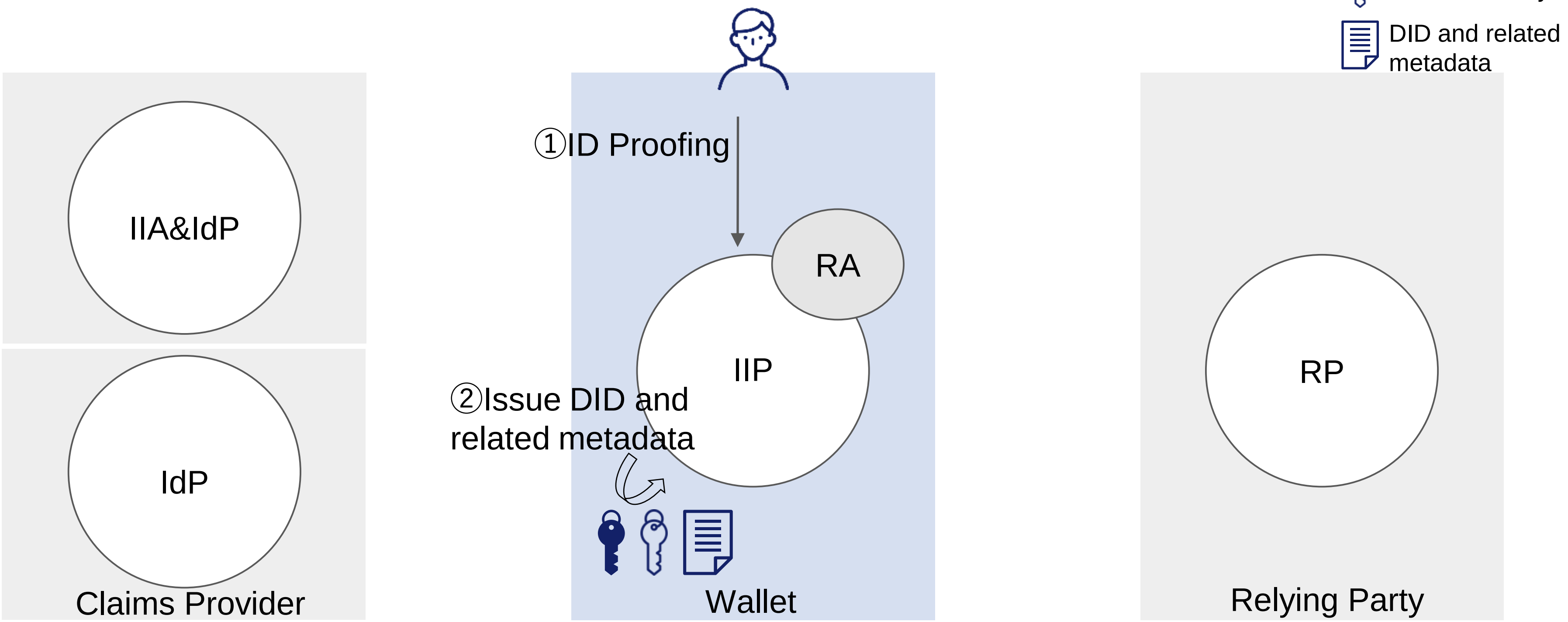
Definition of the Processing Flow – 1. DID Registration Process

■ 1-1. Generation and registration of DIDs and metadata

① The user generates and registers a Decentralized Identity (DID), which is used to claim assertion, via the Registration Authority (RA).

② As in the previous IMS, after some ID proofing is performed, the user issues DID and related metadata using wallet feature. (Upon DID generation, a key pair of private and public keys for to prove as a DID owner is also generated.)

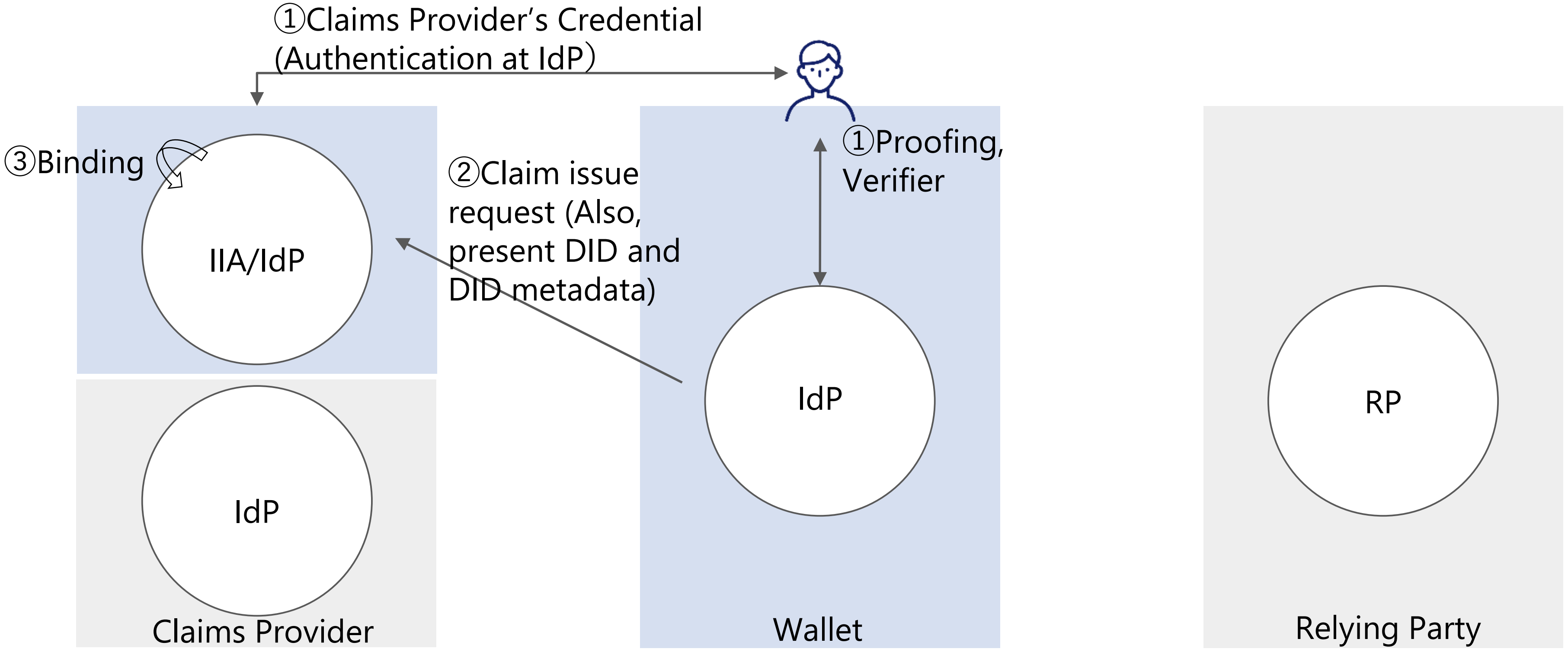
Example）
DID Private key
DID Public key
DID and related metadata



Definition of the Processing Flow – 2. Claim Federation

■ 2-1. Binding of a user on a CP and a DID owner

- The Claims Provider performs the Binding between the DID ownership information provided by the user and the active user's Identifier on the Claims Provider
- The user authenticates at the claims provider’s IdP (①) and requests for claim to be issued. At the same time, the user presents “information that the user holds and controls the user’s DID” to prove ownership of the DID (②).
- If there is no problem with the results of (①) and (②), the Claims Provider’s IdP performs the Binding between the Identifier controlled by the IdP and the Holder that requested for the Claim issue (③).



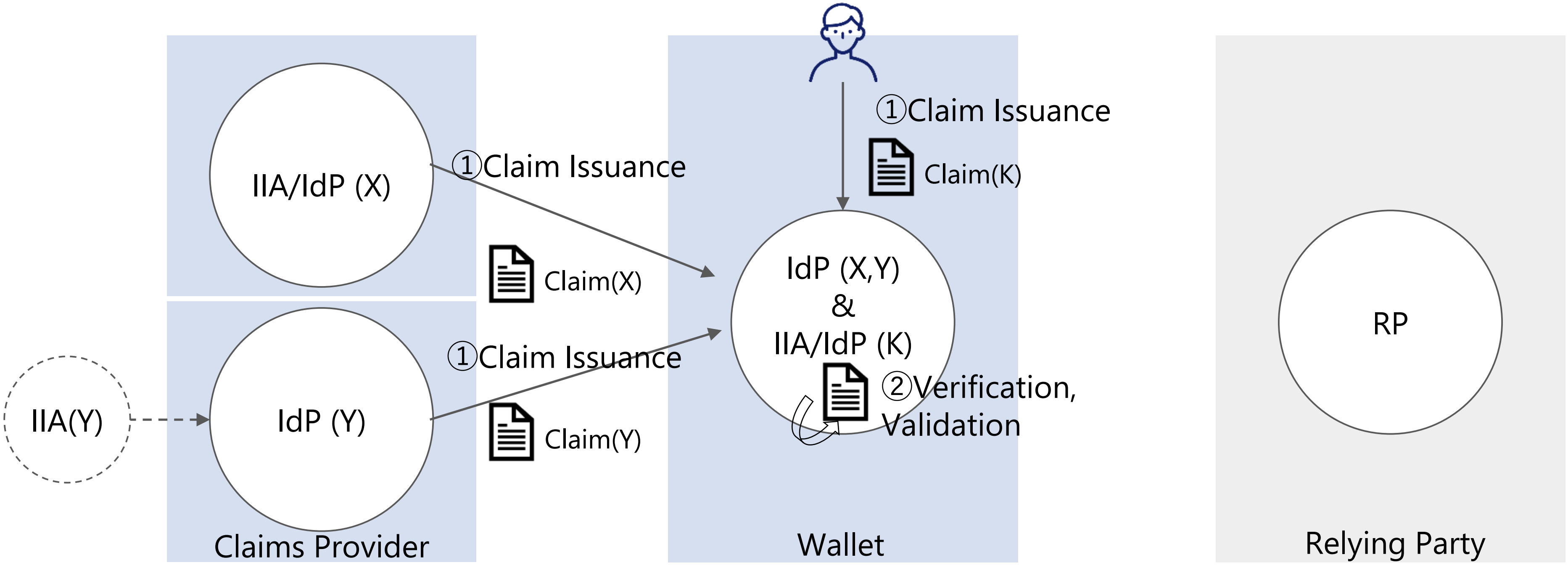
Definition of the Processing Flow – 2. Claim Federation

■ 2-2. Claim issuance

- Based on the binding content, Claims Provider issues a claim for DID and sends it to the wallet (①). Claims could be aggregated to the wallet from multiple IdPs, as shown in the drawing below.
- The IdP of collection could have separated IIA or serve both as IIA and IIP.
- In some cases, the user who asserts attribute information could issue claim (self certification claim). (Refer the Claim(K) in the drawing below.)

■ 2-3. Claim storage in the wallet

- Holder verifies and validates claims, then store the claims to the wallet (②)



3-2-1. Organization of Elements Required in order to Realize SSI/DID

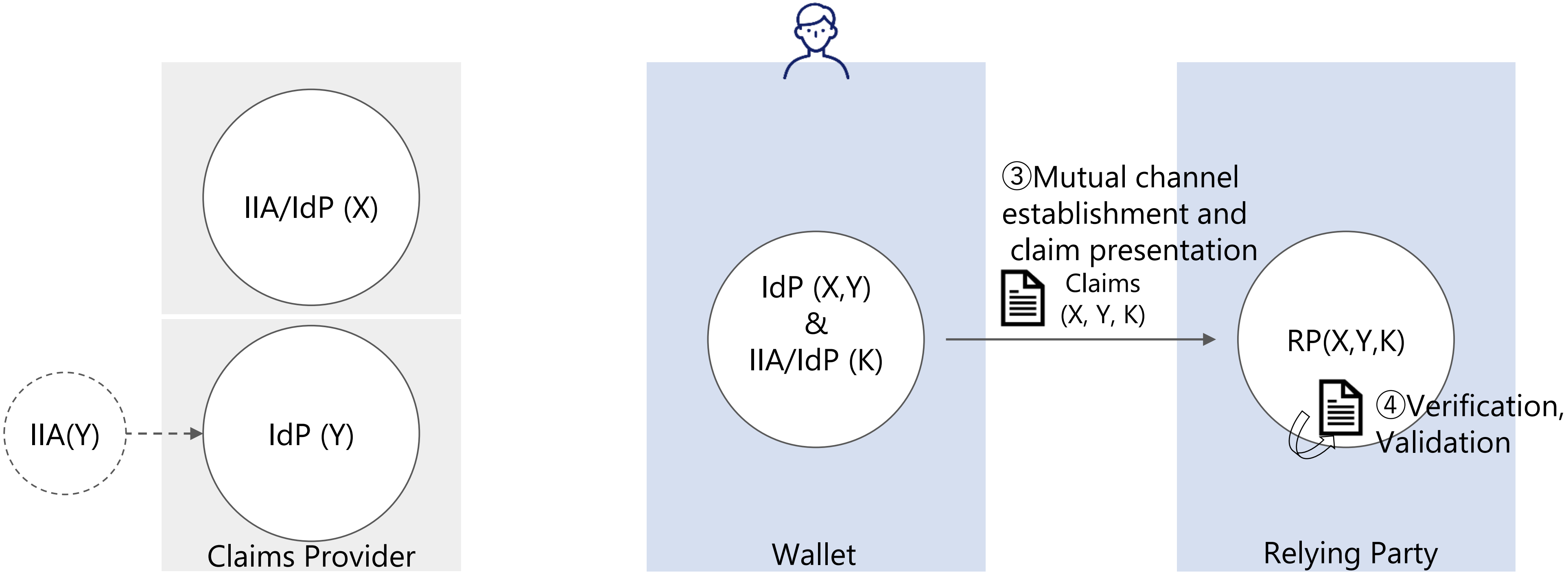
Definition of the Processing Flow – 2. Claim Federation

■ 2-4. User authentication to RP

- Using the DID and related metadata, establish a secure channel between wallet and RP (③).
  Mutual authentication technology specifications are established by several formalization organizations, though most of them are based on the public-key cryptosystem using the private and public keys generated during 1-1.

■ 2-5. Claim assertion

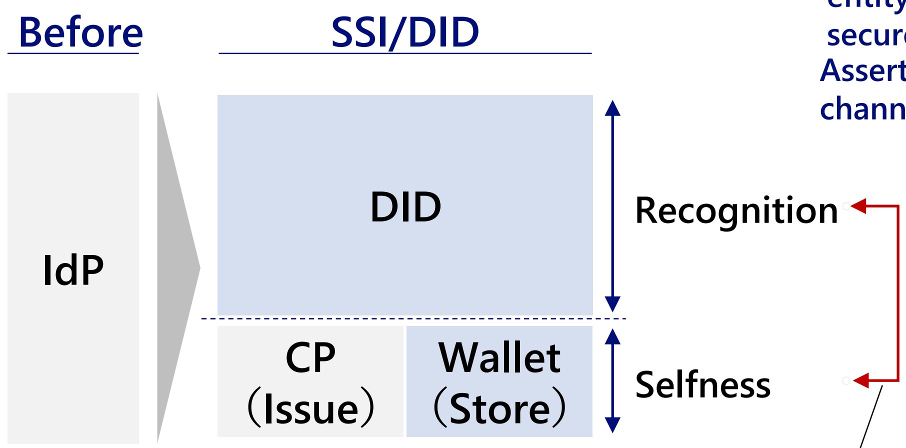
- User presents to the relying party only those claims that they have allowed to be presented. (③) Relying Party verifies and validates the received Claims (④) and provides service to the user If no problem is found.



(Reference) Considerations in Binding - Necessity of Binding

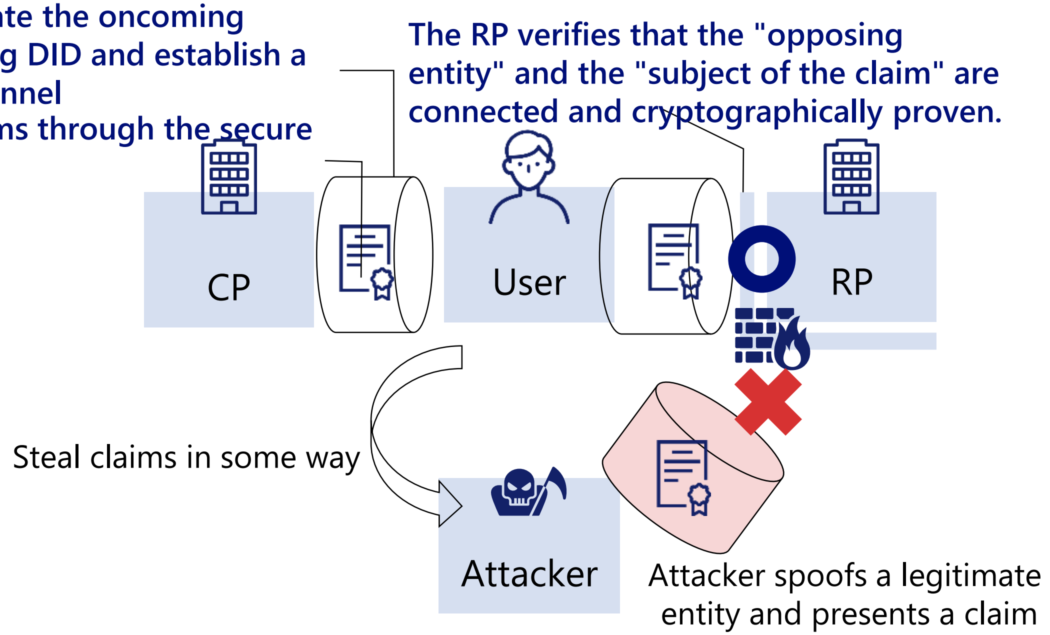
- As described in section 3-1-2, one of the characteristics of SSI/DID is the separation of Recognition (authentication) and Selfness (attributes). On the other hand, when separating these two, it is necessary to perform binding in order to enable determinization of whether the linked claim (attribute) is related to the person (entity) who is performing authentication.
  - As a specific concern, when a user presents a claim to an RP, the RP needs to verify that the claim was issued to the relative user. If this is not done, it is possible to "spoof" using a stolen claim.
  - In order to prevent this, it is necessary to "bind" the user and claim from the claim issuance request stage. (Details described in the next page.)

Binding when "authentication" and “attributes“ are separated



At the time of issuing a claim, it should be possible to cryptographically probable that the claim is Bind in some way.

Prevention of "spoofing" using stolen claims by "binding"



Authenticate the oncoming entity using DID and establish a secure channel

Assert claims through the secure channel

The RP verifies that the "opposing entity" and the "subject of the claim" are connected and cryptographically proven.

Steal claims in some way

Attacker spoofs a legitimate entity and presents a claim

(Reference) Considerations in Binding - Binding Method

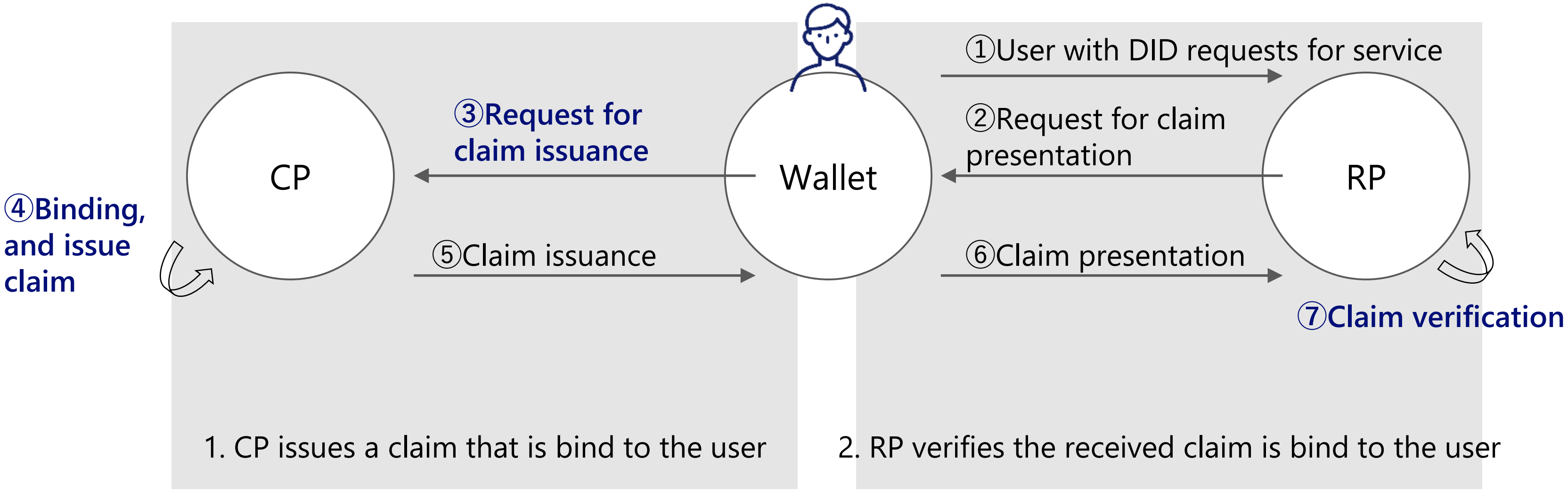
■ To "bind" a user and a claim, the following two points are necessary

1. When the CP issues a claim, it issues the claim to the relative entity (user).
2. When the RP receives a claim, it verifies that it is a claim issued to the relative entity (user).

■ In order to achieve the above, the following processes are necessary.

- Upon requesting the claim issuance: For the CP to issue a claim tied to the user, the user present information that indicates its own entity, which is cryptographically proven and verifiable by the RP later. (process ③).
- Upon claim issuance: The CP issues a claim by linking it to the information received in process ③. (process ④)
- Upon claim verification: The RP that receives a claim via the user's wallet verifies that the claim is cryptographically proven to be associated with the relative user (⑦). This is a perspective to be considered apart from the perspective of verifying using digital signatures that the claim was issued by the CP.

Where to consider Binding when issuing claims


CP
Wallet
RP
①User with DID requests for service
②Request for claim presentation
③Request for claim issuance
④Binding, and issue claim
⑤Claim issuance
⑥Claim presentation
⑦Claim verification
1. CP issues a claim that is bind to the user
2. RP verifies the received claim is bind to the user

(Reference) Considerations in Binding - Binding implementation examples

- For example, the "OpenID Connect Claims Provider "*1) developed by the OpenID Foundation specifies the following processes.
  1. In “Process ③: Request for claim issuance" on the previous page, the "Request Object" *2) specification in the OpenID Connect Core specification is used to sign the request telegram with the DID private key, and the CP verifies the signature to determine whether the request telegram came from the DID owner (who can control the DID private key).
  2. In “Process ④: Binding and issue claim” and “Process ⑦: Claim Verification" on the previous page, by issuing a claim with the wallet's UUID, DID identifier (Decentralized Identifier), or DID public key information as the binding information, it is possible for the RP to verify whether the claim is linked to the DID owner when receiving the claim.

Process ③: Request for claim issuance, binding to the DID holder, and confirmation

Credential Endpoint Request Parameters

~~~
POST /credential HTTP/1.1
Host: https://issuer.example.com
Authorization: Bearer <access-token>
Content-Type: application/json
{
  "request": <signed-jwt-request-obj>
}
```
~~~

Holder signs the request with its own signature key (DID private key)

Processes ④/⑦: Binding of claim and DID holder and its confirmation

Binding information with entity	Example of Binding information description on the claim*1)

UUID related to the wallet	{(Omitted)
	“credentialSubject”: {
	“id”: “urn:uuid:dc000c79-xx (Omitted)”,
	(Omitted)
	}

DID identifier	{(Omitted)
	"credentialSubject": {
	"id": "did:example:1234",
	(Omitted)
	}

Store the metadata (e.g., UUID, DID identifier, and DID public key) of entity who is to claim be issued, in the “credentialSubject” value of the claim.

*1) “OpenID Connect Credential Provider”, http://lists.openid.net/pipermail/openid-specs-ab/attachments/20210528/2f163c71/attachment-0001.bin

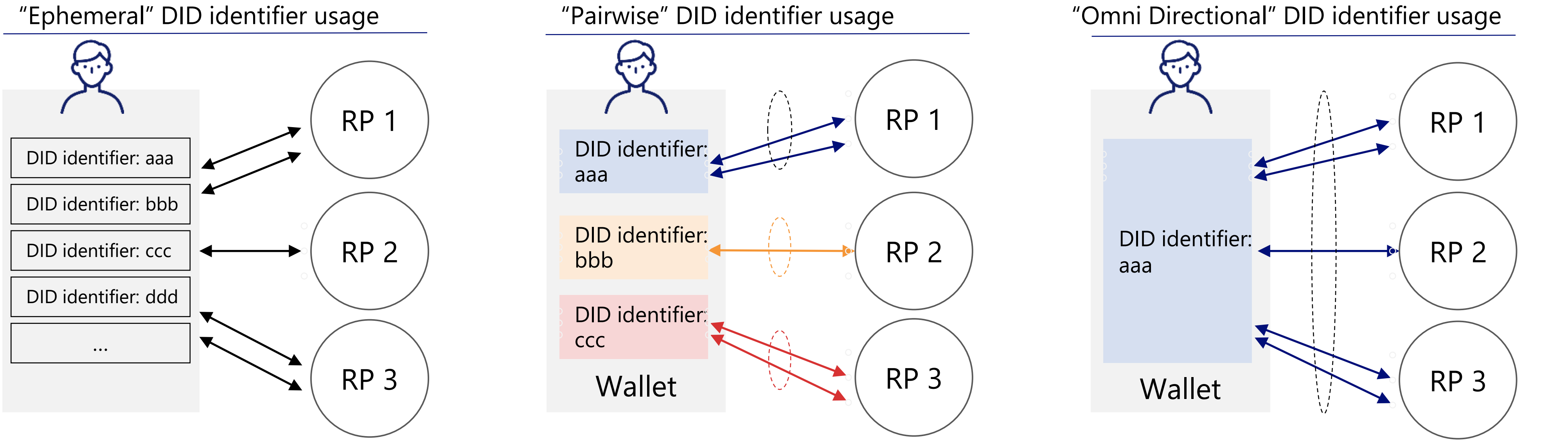
*2) “OpenID Connect Core 1.0 incorporating errata set 1”, https://openid.net/specs/openid-connect-core-1_0.html#RequestUriParameter

(Reference) Considerations in Binding - Concerns of Binding using DID Identifiers (1/3)

- While it is possible to prove the bind between an entity and a claim by storing the binding information in the claim, it is also necessary to consider and take measures against concerns about unjustified collation using that information.
- The DID identifier can be used in multiple ways, as shown in the figures below. In the case of Pairwise, where different DID identifiers are used for each RP, there is a concern that the DID identifiers contained in claims may be collided depending on the type of claim (details in next page).

Usage of DID identifier

Example) ◌ Using the same DID identifier



"Ephemeral" DID identifier usage

- Use different DID identifiers per RP
- Use different DID identifiers for the same RP each time (one-use)

No concern about collation by DID identifier

"Pairwise" DID identifier usage

- Use different DID identifiers per RP
- Use same DID identifiers for each RP every time

To avoid collation by multiple RPs by changing DID identifier per RP

"Omni Directional" DID identifier usage

- Use same DID identifiers for all RPs
- Use same DID identifiers for each RP every time

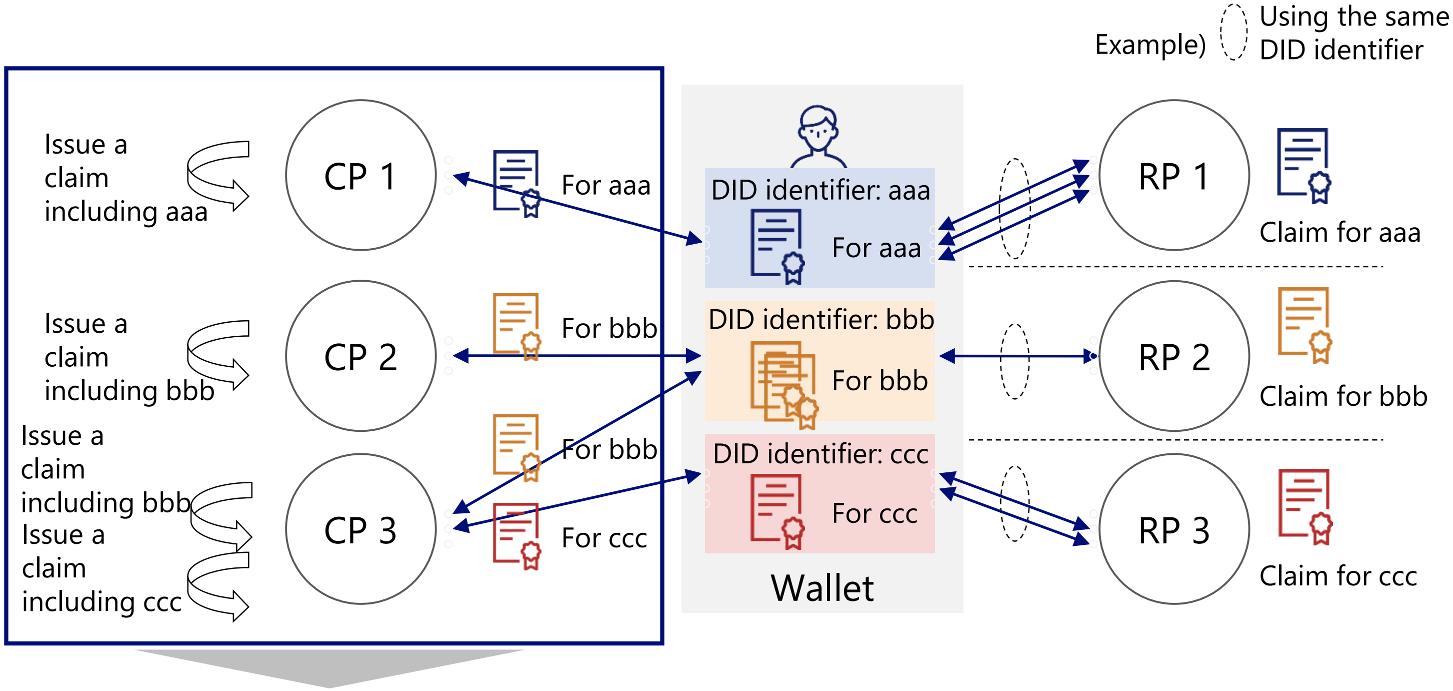
Use with assuming that the collation could happen

3-2-1. Organization of Elements Required in order to Realize SSI/DID

(Reference) Considerations in Binding - Concerns of Binding using DID Identifiers (2/3)

- When using “Pairwise” DID identifier, the DID identifier bind to the claim differs per RP.
- Therefore, each CP needs to be aware of the DID identifier for bind and issue it at the claim generation stage.

Example of claim assertion when using “pairwise” DID identifier

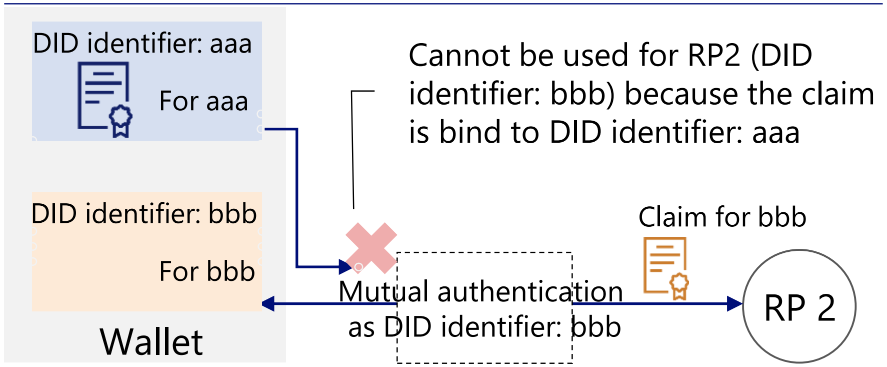


CP must bind the specified DID identifier with a claim when issuing the claim

(Reference) Considerations in Binding - Concerns of Binding using DID Identifiers (3/3)

- During onboarding when using RP2's service, a user first issues a DID identifier for RP2 for to prepare for claim presentation. At that time, even if the user tries to use previously issued claim, that claim is not bind to the newly generated DID identifier, so the claim must be newly generated. (Dynamic claim generation and acquisition will be required, which may limit the "long-term storage and usage of digital identities" described in section 3-1-2.)
- Also, the Verifiable Presentation (VP) of W3C's Verifiable Credentials Data Model 1.0 specifies that multiple VCs can be stored *1). In such case, if the DID identifier bind to the VC is different, at the recipient RP2, it can be exposed that the different DID identifiers are "associated with the same entity".

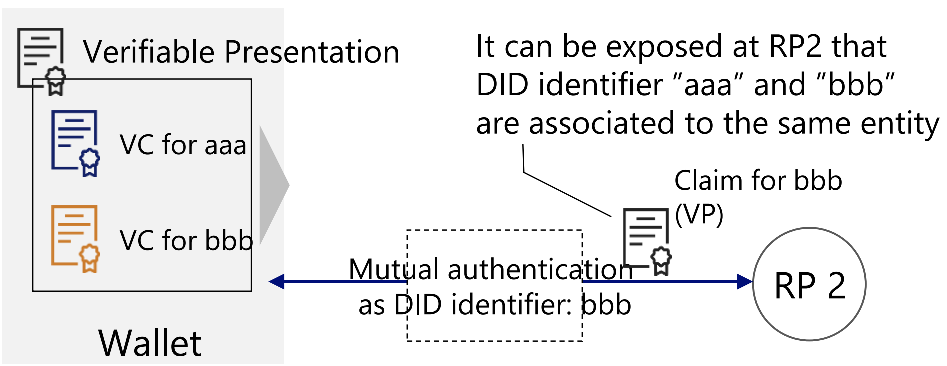
Concern①: Difficult to use static claims



Cannot be used for RP2 (DID identifier: bbb) because the claim is bind to DID identifier: aaa

- RP2 performs claim assertion after recognition of the wallet DID identifier as "bbb" and mutual authentication.
- The claim for DID identifier "aaa" is not bind to "bbb", so it cannot be used for RP2. Generation of a new claim for"bbb" is required. (Claim cannot be "Stock & Forward" , so an SSI's characteristic of "long-term storage and usage of digital identities" is difficult to be realized.

Concern②: DID identifiers and claims can be collated when claims are aggregated



It can be exposed at RP2 that DID identifier "aaa" and "bbb" are associated to the same entity

- If multiple RPs collude to collate the information used for binding, RP+RP'-U Unlinkability could be lost, which was accomplished by using the pairwise DID identifier per each RP.

*1) "Verifiable Credentials Data Model 1.0", https://www.w3.org/TR/vc-data-model/

(Reference) Considerations in Binding - Summary

- Considering privacy, the two requirements below are need to be considered in the implementation of Binding. Although, it is difficult to achieve both Binding and privacy by simply issuing claims with highly identifiable information.

Requirements in the Binding	Concerns of Binding using DID Identifiers
Static claim assertion instead of dynamic claim generation and acquisition. （Stock & forward）	• If a DID identifier is included in a claim for Binding, the claim needs to be reissued when the DID identifier used with the RP changes. • As a result, the claims stored in the Wallet in the past may become meaningless, which may make it difficult to achieve the "long-term storage and usage of digital identities" described in section 3-1-2 (it may be necessary to dynamically request the CP to issue claims each time).
Even if the multiple RPs collude to collate the information used for the above binding, they will not be able to collate the user. (RP+RP'-U Unlinkability)	• Some specifications assume the presentation of claims in the form of aggregating multiple claims (W3C Verifiable presentation*1), but if the DID identifiers bound to the included claims are different, there is a concern that different DID identifiers will be exposed to be associated with the same entity from the perspective of the RP that receives them (even if different DID identifiers are used, there is a concern about user collation).

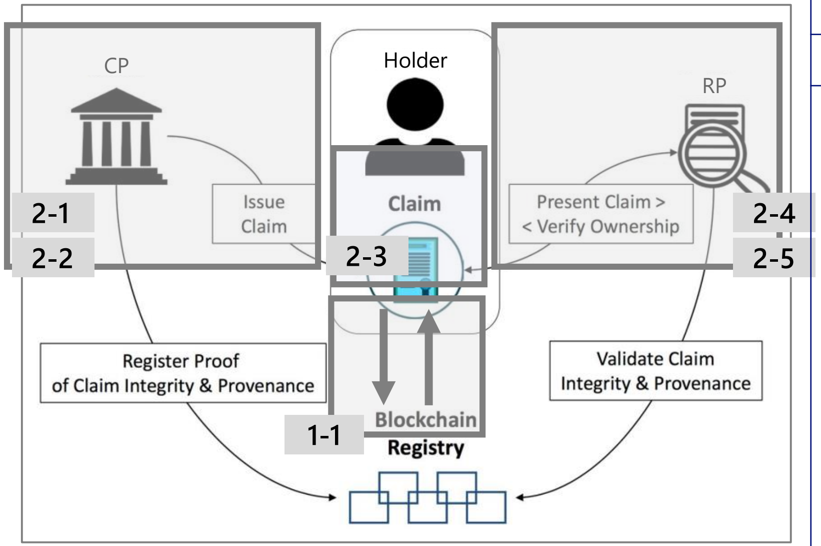
*1) "Verifiable Credentials Data Model 1.0", https://www.w3.org/TR/vc-data-model/

Specifications of Technical Components Considered by Standardization Organizations

- For the following use cases, the specifications specified by each standardization body were mapped to identify where the use cases are targeted.

1. DID Registration Process
   The user performs ID Proofing, the DID Activation process is completed, and the DID is switched to the valid state.
2. Claim Assertion
   The Holder becomes the IdP after acquiring the DID and performs the Claim assertion between the Claims Provider and Holder, and between the Holder and Service Provider.

Overview of the SSI/DID process flow



Process	Overview of the process
1. 1. DID Registration Process (Process until the DID transitions to the valid state)	
1-1. Generation and Registration of Subject Identifier and Metadata	Generation and registration of subject identifier and meta data (including authentication credential)
2. 2. Claim Federation	
2-1. Binding process for users and DIDs on the CP	• The user authenticates to the Credential Service Provider in the CP • Perform binding the DID received from the user in the CP and the user's Identifier managed in the CP..
2-2. Claim Issuance and Returning to wallet	Based on the binding process at 2-1) , issue a claim in a form of DID and bind.
2-3. Claim storage to Wallet	Store the Claim to the wallet received at 2-2)
2-4. User Authentication for Verifier	Authenticates RP using the Credential from 1-1) for the other side
2-5. Claim Assertion	• After mutual authentication at 2-4), present Claim received at 2-3) • RP verifies whether the received claim is issued by binding with the DID of the user authenticated in 2-4) (Verification), and whether the asserted claim is valid (Validation).

3-2-2. 技術構成要素に対する各標準化団体の議論動向

Specifications of Technical Components Considered by Standardization Organizations

Specifications with dotted lines mean that the policy is to refer to specifications defined by other organizations.

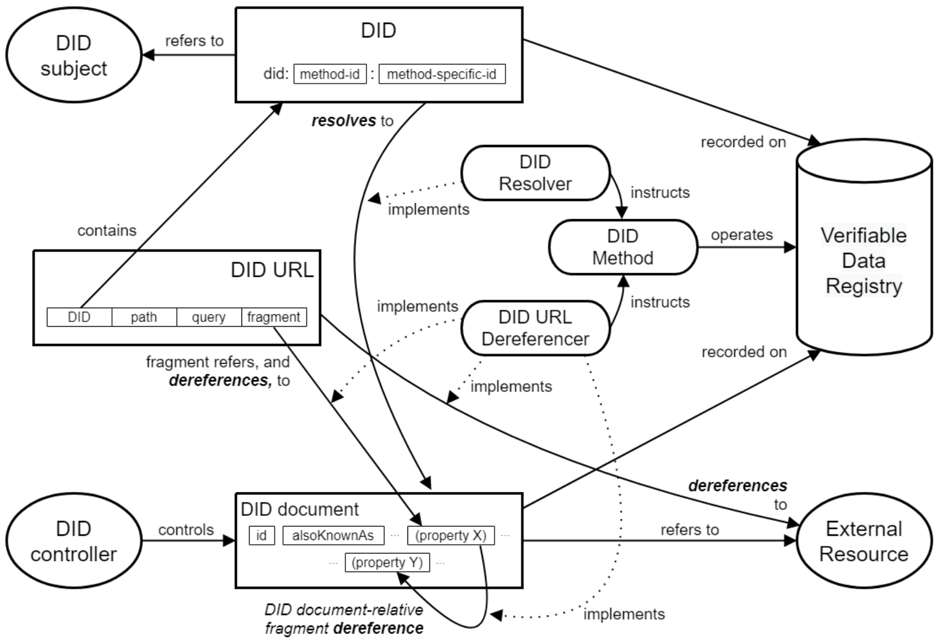
#	A) OpenID Foundation	B) W3C/W3C-CCG	C) DIF	D) Sovrin (hyperledger、Linux Foundation)
1-1. Generation and registration of DIDs and metadata	A-1) OpenID Connect Core（SIOP） OpenID Self Issued Identifiers ※	B-1) Decentralized Identifiers (DIDs) v1.0	B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1	B-1) Decentralized Identifiers (DIDs) v1.0
2-1. Binding of a user on a CP and a DID owner	OpenID Connect Credential Provider ※	B-2) Verifiable Credentials Data Model 1.0 BBS+ Signatures 2020 ※	OpenID Connect Credential Provider ※	D-1) Aries RFC 0023: DID Exchange Protocol 1.0 Hyperledger Ursa
2-2. Claim issuance	A-1) OpenID Connect Core（SIOP）	B-1) Decentralized Identifiers (DIDs) v1.0 vp-request-spec (W3C-CCG) ※	B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1	B-1) Decentralized Identifiers (DIDs) v1.0 D-1) Aries RFC 0023: DID Exchange Protocol 1.0 D-2 Aries RFC 0036: Issue Credential Protocol 1.0
2-3. Claim storage in the wallet	A-3) OpenID Connect Claims Aggregation	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0 B-3) Credential Handler API (W3C-CCG)	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0	B-2) Verifiable Credentials Data Model 1.0 B-1) Decentralized Identifiers (DIDs) v1.0
2-4. User authentication to RP	A-1) OpenID Connect Core（SIOP）	B-4) Confidential Storage 0.1 B-1) Decentralized Identifiers (DIDs) v1.0	B-4) Confidential Storage 0.1 B-1) Decentralized Identifiers (DIDs) v1.0	B-1) Decentralized Identifiers (DIDs) v1.0
2-5. Claim assertion	A-1) OpenID Connect Core（SIOP）	B-1) Decentralized Identifiers (DIDs) v1.0 vp-request-spec (W3C-CCG) ※ B-3) Credential Handler API (W3C-CCG)	DID-SIOP ※ B-1) Decentralized Identifiers (DIDs) v1.0 C-1) Self-Issued OpenID Connect Provider DID Profile v0.1 C-2) Presentation Exchange	B-1) Decentralized Identifiers (DIDs) v1.0 D-3) Aries RFC 0037: Present Proof Protocol 1.0

The specifications marked with (※) are not described in detail in this study because it was assumed that the contents of these specifications would change in the future due to integration with other specifications or duplication as of April 1, 2021.

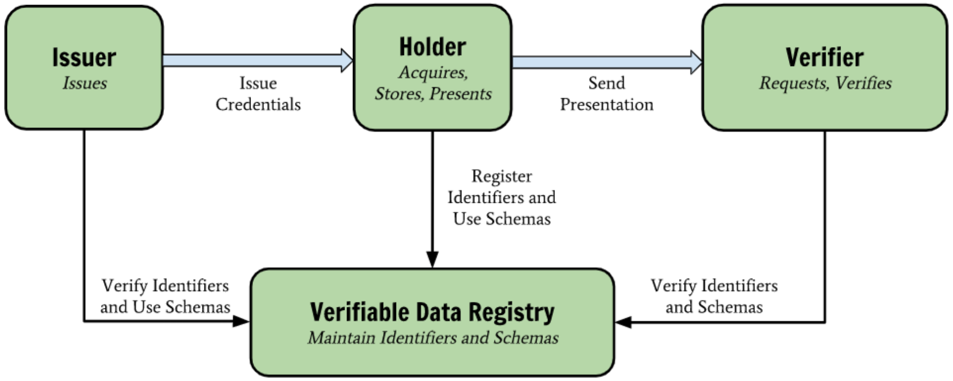
Approach for Realization by W3C

- As a means of realizing DIDs, W3C formulates a mechanism for the federation of Claims using a new type of globally unique identifiers called Decentralized identifiers (DIDs), which are designed to allow individuals and organizations to generate their own identifiers using a system they trust, and to recognize the identifiers using cryptographic proofs (e.g., digital signatures, privacy-preserving biometric protocols). The details of DIDs will be described later.
- In Verifiable Credentials Data Model 1.0, data models for Claims called Verifiable Credential (VC) and Verifiable Presentation (VP) are defined and it provides the definition of data to represent user properties and the lifecycle models of VC / VP.

Decentralized identifiers (DIDs) v1.0



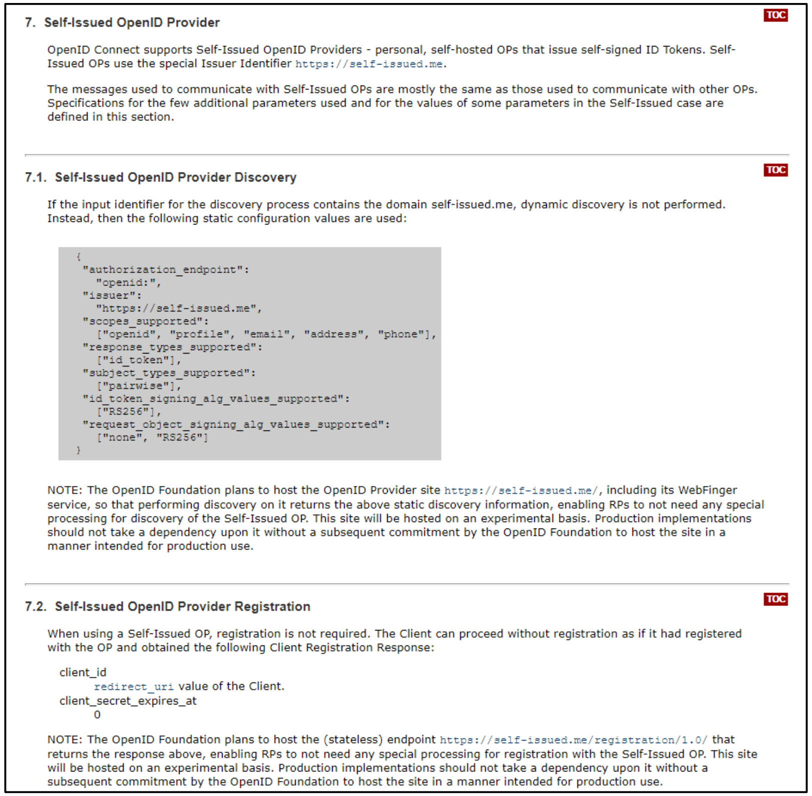
Verifiable credentials data model 1.0


Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas

Approach for Realization by OpenID Foundation

- The OpenID Foundation is working on a specification that uses the "Self-Issued OpenID Provider" in the existing specification to allow users to feature as OpenID providers, perform recognition, and then assert claims with the user as the hub.
- For attributes of data model, extension of the model to include W3C DIDs is being considered, and liaison with DIF is also being discussed for the part related to Binding with DIDs.

OpenID Connect Core 1.0 – Self issued OpenID provider



7. Self-Issued OpenID Provider

TOC

OpenID Connect supports Self-Issued OpenID Providers - personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs use the special Issuer Identifier `https://self-issued.me`.

The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs. Specifications for the few additional parameters used and for the values of some parameters in the Self-Issued case are defined in this section.

7.1. Self-Issued OpenID Provider Discovery

TOC

If the input identifier for the discovery process contains the domain self-issued.me, dynamic discovery is not performed. Instead, then the following static configuration values are used:

```
{
 "authorization_endpoint":
   "openid:",
 "issuer":
   "https://self-issued.me",
 "scopes_supported":
   ["openid", "profile", "email", "address", "phone"],
 "response_types_supported":
   ["id_token"],
 "subject_types_supported":
   ["pairwise"],
 "id_token_signing_alg_values_supported":
   ["RS256"],
 "request_object_signing_alg_values_supported":
   ["none", "RS256"]
}
```

NOTE: The OpenID Foundation plans to host the OpenID Provider site `https://self-issued.me/`, including its WebFinger service, so that performing discovery on it returns the above static discovery information, enabling RPs to not need any special processing for discovery of the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

7.2. Self-Issued OpenID Provider Registration

TOC

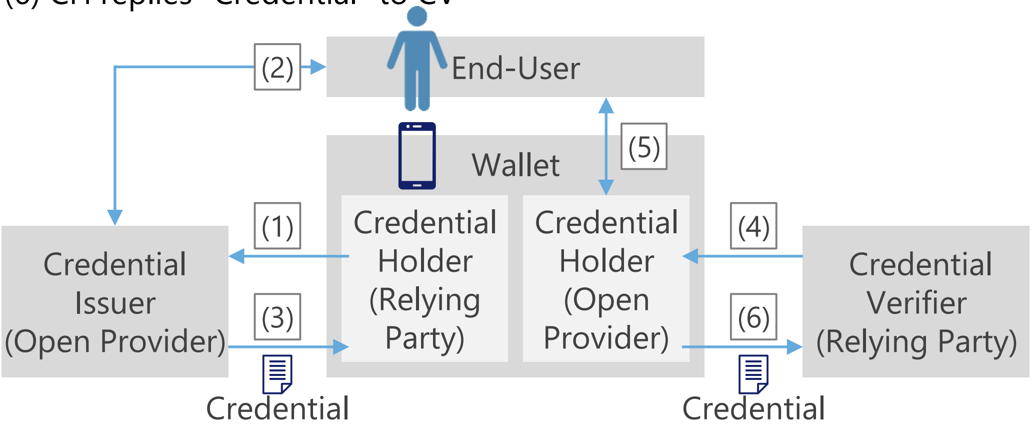
When using a Self-Issued OP, registration is not required. The Client can proceed without registration as if it had registered with the OP and obtained the following Client Registration Response:

client_id
    `redirect_uri` value of the Client.
client_secret_expires_at
    0

NOTE: The OpenID Foundation plans to host the (stateless) endpoint `https://self-issued.me/registration/1.0/` that returns the response above, enabling RPs to not need any special processing for registration with the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

OpenID Connect Credential Provider

(1) Credential Holder (CH) requests "Credential" from Credential Issuer (CI)
(2) CI authenticates the end user and obtains authorization
(3) CI replies "Credential" to CH
(4) Credential Verifier (CV) requests "Credential" from CH
(5) CH authenticates the end user and obtains authorization
(6) CH replies "Credential" to CV


(2)
End-User
(5)
Wallet
(1)
(4)
Credential Issuer (Open Provider)
Credential Holder (Relying Party)
Credential Holder (Open Provider)
Credential Verifier (Relying Party)
(3)
(6)
Credential
Credential

* Note: Binding between the generated Credential and DID is assumed to be realized by “Signed Request Object" specified in OpenID Connect Core 1.0 at the time of (1) request.

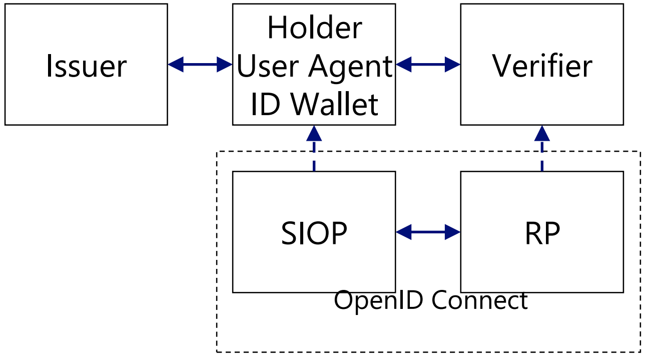
3-2-2. Trends in Discussions by Standardization Organizations on Technology Components

Approach for Realization by DIF

- Initially, the DIF was considering the concept of a Holder and specifications for combining it with the aforementioned DIDs and OpenID Connect, but due to the OpenID Foundation's extensive use and high scalability, the DIF signed a liaison agreement with the OpenID Foundation in November 2020 and decided to extend the specifications using OpenID Connect to realize the above.
- Several other working groups are also formulating specifications, including one that enables claim requests/presentations from Holder to RP, independent of transport protocols and claim data formats.

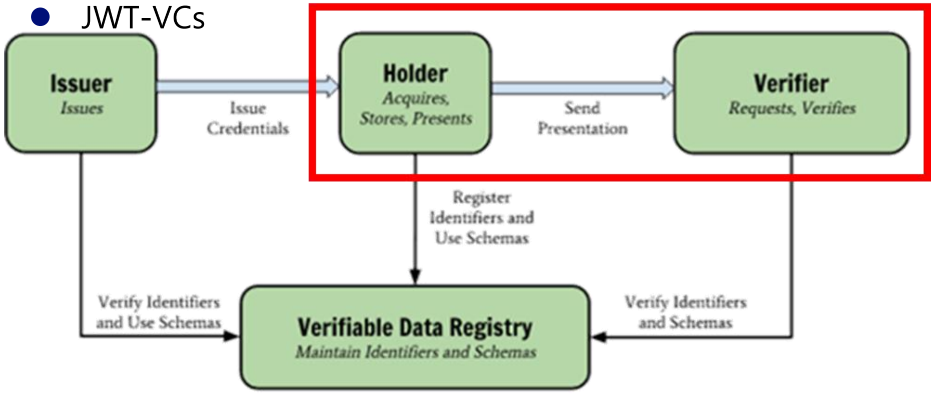
Background of liaison with OpenID Foundation (reason for selecting OIDC)

- Well-known and mature
- Widely used, and has a big community
- Enterprises are familiar with OIDC
- Simple and light-weight
- Flexible and extensible through profiles
- Additional (optional) support for credentials/ claims exchange
- Based on work incubated at RWOT, and IIW



Development of spec for Claim request/presentation (Presentation Exchange)

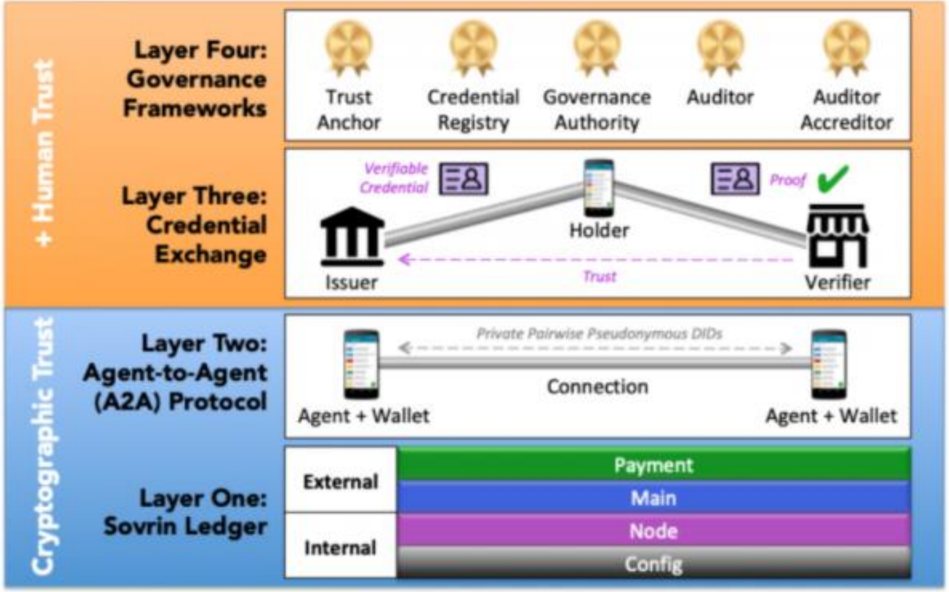
- Specify Proof request/presentation between Holder and Verifier
- The following formats can be supported for assertion via OpenID Connect, DID Comm, and Credential Handler APIs
  - JSON Web Tokens (JWTs)
  - Verifiable Credentials (VCs)
  - JWT-VCs


Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas

Approach for Realization by DIF

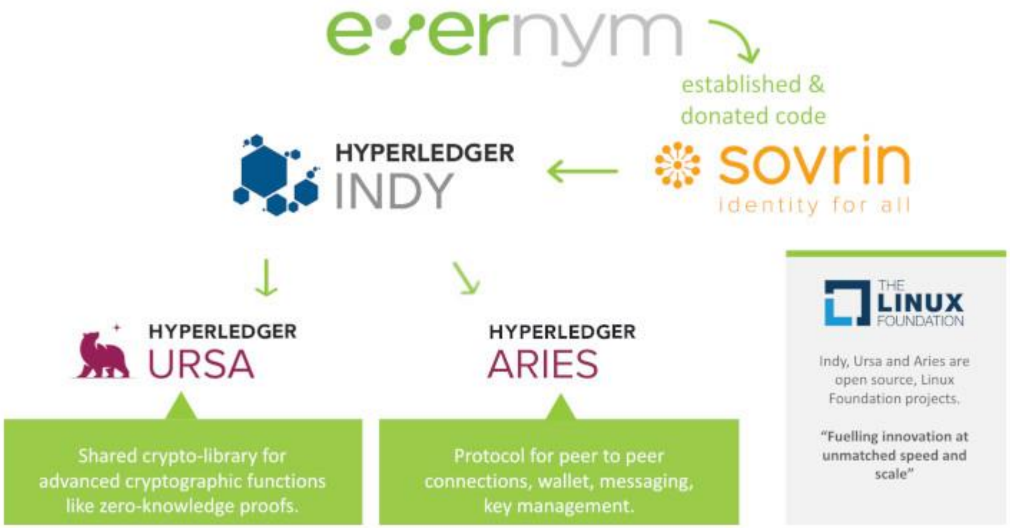
- The Sovrin Foundation has established the "Sovrin Governance Framework", which is necessary to realize the SSI model, and defines legal agreements, technical specifications, standards, and policies to be used, as well as criteria and processes for evaluating the suitability of the framework's policies. In addition, the framework defines four layers called "Sovrin Stack" as the configuration stack.
- As normative components, W3C's DIDs, VC Data Model, and DID Method 1.0 Specification are mentioned. As for the distributed ledger technology for DID/DID Document management, Evernym has launched the Sovrin Network and provided the code, which is now being deployed as an open source project called Hyperledger Indy.
  - As a contributor to extended specifications such as the Aries project, which specifies the Peer to Peer Connection / Wallet / Messaging / KeyManagement protocols, and the USRA project, which aims to provide cryptographic libraries for cryptographic features such as ZKP.

Sovrin Stack diagram by Sovrin Foundation



Source) Sovrin Foundation
https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf
https://sovrin.org/2020-how-ssi-went-mainstream/

Details for Founding of Hyperledger Indy and related projects


evernym
established & donated code
HYPERLEDGER INDY
sovrin
identity for all
HYPERLEDGER URSA
HYPERLEDGER ARIES
Shared crypto-library for advanced cryptographic functions like zero-knowledge proofs.
Protocol for peer to peer connections, wallet, messaging, key management.
THE LINUX FOUNDATION
Indy, Ursa and Aries are open source, Linux Foundation projects.
"Fuelling innovation at unmatched speed and scale"

Source) Evernym Hyperledger Aries: The Next Major Step Towards Interoperable SSI
https://www.evernym.com/blog/hyperledger-aries/

3-2-3. Consideration Specifications of each Standardization Organization

Overview of each Specification

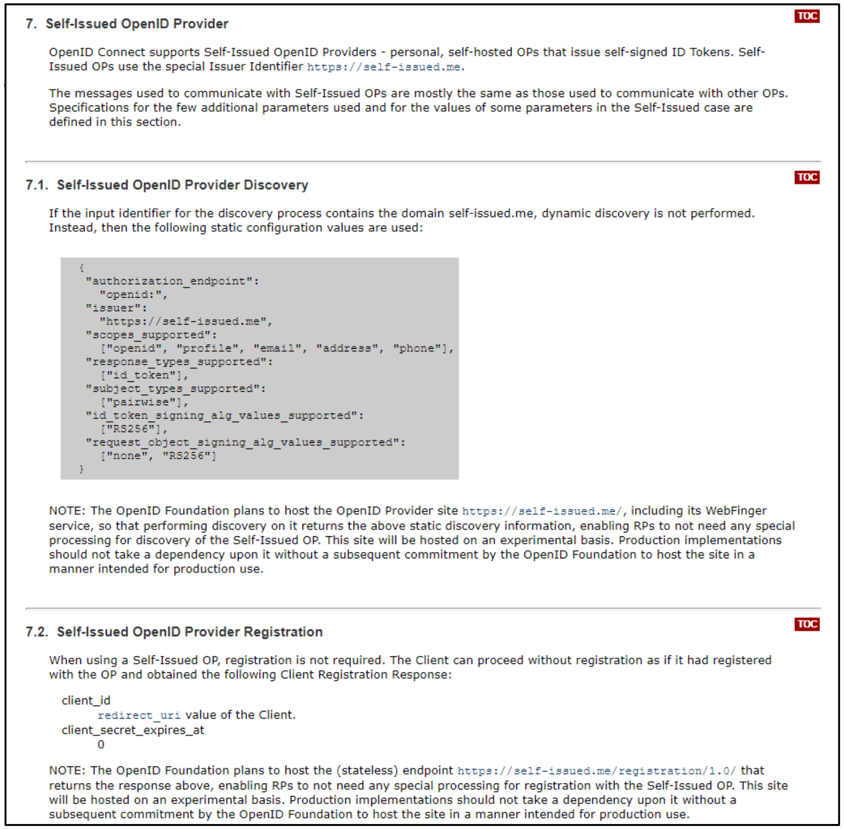
- In this section, an overview of the following specifications is summarized.
  Note that for A-2) OpenID Connect Claims Aggregation, the section on security considerations is TBD, and the issues are not described in this study.

#	Organization Name	Specification Name
A-1)	OIDF	OpenID Connect Core
A-2)	OIDF	OpenID Connect Claims Aggregation
B-1)	W3C	Decentralized Identifiers (DIDs) v1.0
B-2)	W3C	Verifiable Credentials Data Model 1.0
B-3)	W3C	Credential Handler API
B-4)	W3C, DIF	Confidential Storage 0.1
C-1)	DIF	Self-Issued DID Profile for OpenID v1.0
C-2)	DIF	Presentation Exchange
D-1)	Hyperledger	Aries RFC 0023: DID Exchange Protocol 1.0
D-2)	Hyperledger	Aries RFC 0036: Issue Credential Protocol 1.0
D-3)	Hyperledger	Aries RFC 0037:Present Proof Protocol

A-1) OpenID Connect Core

- OpenID Connect Core (hereinafter referred to as "OIDC") is a specification developed by the OpenID Foundation in 2014, which enables identity assertions based on OAuth 2.0.
- In this specification, a method called "Self-Issued OpenID Provider" (hereinafter referred to as "SIOP"), in which the user himself acts as an IdP, is mentioned.
  - OIDC Core Ch.7 Self-Issued OpenID Provider
    - SIOP behaves as a self-hosted OpenID Provider.
    - By using SIOP, it behaves as an OP and can manage the
    - This method is attracting attention as one of the means to a reduction in dependence on existing ID providers.

OpenID Connect Core 1.0 - SIOP



7. Self-Issued OpenID Provider

OpenID Connect supports Self-Issued OpenID Providers - personal, self-hosted OPs that issue self-signed ID Tokens. Self-Issued OPs use the special Issuer Identifier `https://self-issued.me`.

The messages used to communicate with Self-Issued OPs are mostly the same as those used to communicate with other OPs. Specifications for the few additional parameters used and for the values of some parameters in the Self-Issued case are defined in this section.

7.1. Self-Issued OpenID Provider Discovery

If the input identifier for the discovery process contains the domain self-issued.me, dynamic discovery is not performed. Instead, then the following static configuration values are used:

```
{
 "authorization_endpoint":
   "openid:",
 "issuer":
   "https://self-issued.me",
 "scopes_supported":
   ["openid", "profile", "email", "address", "phone"],
 "response_types_supported":
   ["id_token"],
 "subject_types_supported":
   ["pairwise"],
 "id_token_signing_alg_values_supported":
   ["RS256"],
 "request_object_signing_alg_values_supported":
   ["none", "RS256"]
}
```

NOTE: The OpenID Foundation plans to host the OpenID Provider site `https://self-issued.me/`, including its WebFinger service, so that performing discovery on it returns the above static discovery information, enabling RPs to not need any special processing for discovery of the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

7.2. Self-Issued OpenID Provider Registration

When using a Self-Issued OP, registration is not required. The Client can proceed without registration as if it had registered with the OP and obtained the following Client Registration Response:

client_id
`redirect_uri` value of the Client.
client_secret_expires_at
0

NOTE: The OpenID Foundation plans to host the (stateless) endpoint `https://self-issued.me/registration/1.0/` that returns the response above, enabling RPs to not need any special processing for registration with the Self-Issued OP. This site will be hosted on an experimental basis. Production implementations should not take a dependency upon it without a subsequent commitment by the OpenID Foundation to host the site in a manner intended for production use.

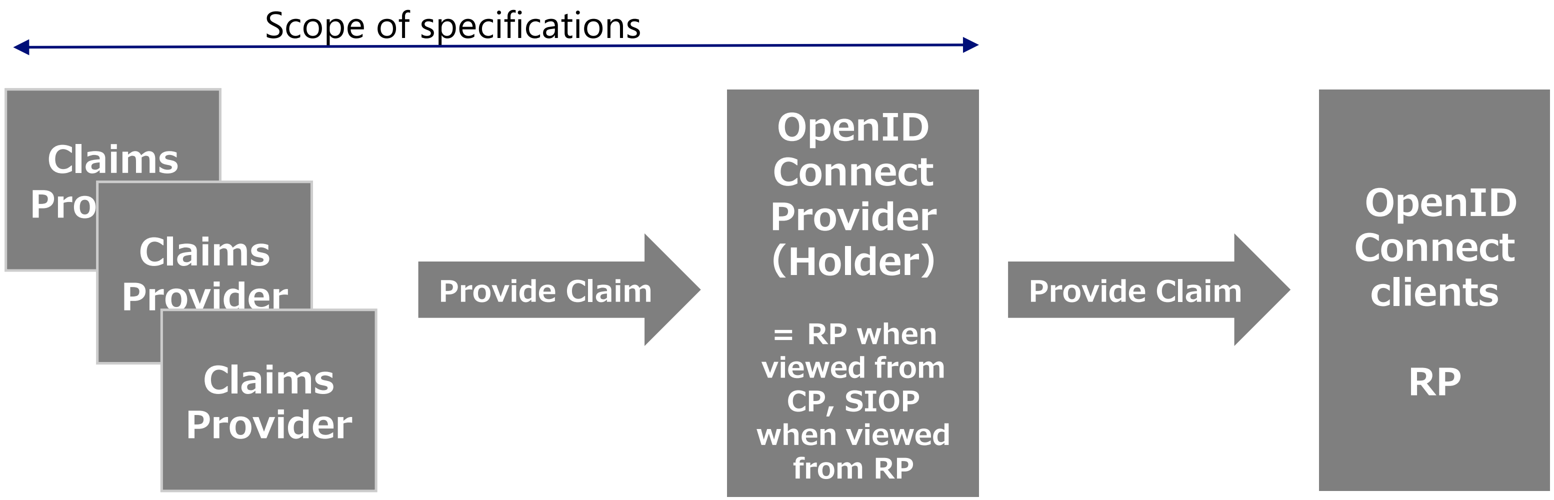
Source) OpenID Connect Core 1.0 incorporating errata set 1- 7, Self-Issued OpenID Provider
https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued

3-2-3. Consideration Specifications of each Standardization Organization

A-2) OpenID Connect Claims Aggregation

- This specification specifies the process for providing aggregated claims from a Claims Provider to an OpenID Connect client.
  - The OpenID Provider acts as a Relying Party ("RP") by registering as a client with the Claims Provider ("CP") and making an OIDC authentication request for the required user information.
  - In this specification, the scope of the specification is the processing until the claims are provided from the CP to the OpenID Connect Provider, and the provision of claims from the OpenID Connect Provider to the Relying Party is outside the scope of the specification.
  - Since the OpenID Provider can centrally collect all the claim information of the end user, there is no need for the Claims Provider and Relying Parties to directly exchange claims, and the user can share the claim information acquired through the OP with other service providers.

Overview of OpenID Connect Claims Aggregation

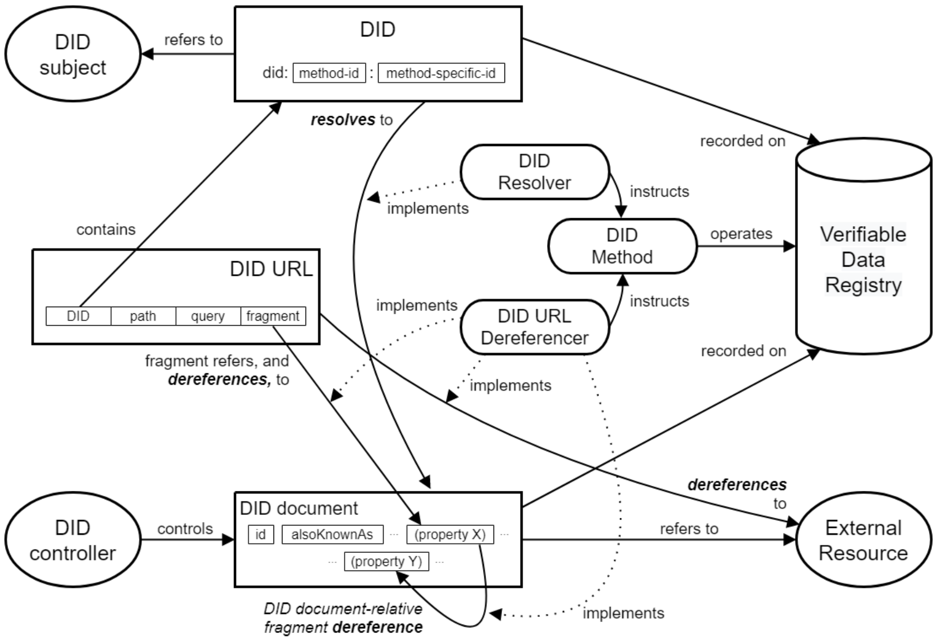


Source) OpenID Connect Claims Aggregation
https://bitbucket.org/openid/connect/src/master/openid-connect-claims-aggregation/openid-connect-claims-aggregation-1_0.md

B-1) Decentralized Identifiers (DIDs) v1.0

- DIDs v1.0 specifies the syntax, data model, properties, and serialized representation of DIDs, the operations on DIDs, and the process of resolving the resources that DIDs represent (refer the table below).
- The decentralized identifier (DID) is defined as a globally unique identifier that can be authenticated using cryptographic proofs (e.g., digital signatures, privacy-preserving biometric protocols) by generating its own identifier using a system that the individual or organization trusts.

Decentralized Identifiers (DIDs) v1.0



	Overview
DIDs and DID URLs	DID is a text string consisting of 3 parts. · Method-specific identifier DIDs generated from the Scheme (did) / method identifier / DID method are required to be permanent, immutable, and not reused after deactivation.
DID Subjects	It may be a DID Controller, or an entity identified by a DID. It can be people, groups, organizations, physical or logical
DID Documents	The controller of a DID is the entity (person, organization, or autonomous software) that has the capability—as defined by a DID method—to make changes to a DID document.
DID Methods	A distributed ledger, distributed file system, database, P2P network, or other forms of trusted storage that returns the data needed to record DIDs and generate DID documents.
DID Controllers	An abstract data model showing DID-related metadata, public key validation methods, and services related to interaction with DID subjects.
Verifiable Data Registries	Uses Verifiable Data Registries to specify how to generate, resolve, reverse, and deactivate DIDs and their associated DID Documents.
DID resolverと DID resolution	A DID resolver is a software and hardware component that receives DID as input and outputs DID Documents. This process is called DID resolution.
DID URL dereferencers と DID URL dereferencing	A DID URL dereferencer is a software or hardware component that takes a DID URL (and associated metadata) as input and produces a resource (and associated metadata) as output. This process is called DID URL dereferencing (dereferencing a reference).

Source) Decentralized Identifiers (DIDs) v1.0

B-1) Decentralized Identifiers (DIDs) v1.0

- The following points are listed as security considerations.

#	Overview (1/2)
DID resolver selection	The DID Method Registry is a list of DID method names and their corresponding DID method specifications. DID does not have a central authority to define them, but implementers can use the DID Method Registry to make informed decisions when choosing which DID resolver to use.
Proof of DID and DID Document	The signature and time stamp make the DID Document cryptographically verifiable. The signature verified on the self-signed DID Document does not prove control of the DID, and only shows that the DID Document has not been tampered with since it was time stamped, and that the DID controller controlled the private key used for signing.
Proof of public key control	There are two methods for proving control of the private key corresponding to a public key description in the DID document: static and dynamic. The static method is to sign the DID document with the private key. This proves control of the private key at the that the DID document was registered. If the DID Document is unsigned, the public key control described in the DID Document must be dynamically proven.
Authentication and Verifiable Claims	DIDs and DID Documents have essentially no PII (personally identifiable information).The process of binding a DID to a person, company, etc. using credentials in the real world, for example, with the same subject as the DID, is outside the scope of this specification.
Authentication service endpoint	If the DID Document exposes a service endpoint for the purpose of authenticating or authorizing the DID subject, it is the responsibility of the service endpoint provider, target audience, or requesting party to comply with the requirements of the authentication protocols supported by that service endpoint.
Prohibition of denial	Prohibiting denial of DID and DID Document updates is supported assuming that the target is monitoring unauthorized updates and that malicious updates can be undone according to the access control mechanism of the DID method.
DID Document change notification	One mitigation against unauthorized changes to the DID Document is to monitor and proactively notify the DID subject of changes. This is similar to supporting preventing traditional username / password account takeover by sending a password reset notification to an email address. For DIDs, there are no intermediary registrars or account providers that generate such notifications, if the verifiable data registry with which the DID is registered supports direct change notification, subscription services can be provided to the DID controller. If the DID controller relies on a third-party monitoring service, it will incorporate another attack vector.
Key and signature expiration date	In a decentralized identity architecture, there is no central authority to enforce a key or signature expiration policy. The DID resolver and the parties need to verify that the key has not expired when it was used.

B-1) Decentralized Identifiers (DIDs) v1.0

- The following points are listed as security considerations.

#	Overview (2/2)
Key revocation and recovery	It is up to the DID method to define the occurrence of cryptographic key revocation. In addition, the DID method specification is also expected to enable support for a quorum of trusted parties to facilitate key recovery. Access control and key recovery in the DID method specification can also include a time lock feature that protects against compromise of the key by retaining a second recovery procedure.
The role of human-friendly identifiers	The problem of mapping Human-Friendly identifiers to DIDs (and doing it in a validated and trusted way) is outside the scope of this specification.
Immutability	The idea that immutability brings cybersecurity benefits is especially relevant for caching. The DID method, which is tied to a true global source, is always searchable for the latest version of the DID Document. However, if a cache layer exists, it can be abused by believing that it actually exists even though the attributes of the object are actually different.
Encrypted data in DID Document	Encrypting all or part of a DID Document is not a good way to protect your data in the long run. Similarly, placing encrypted data in a DID Document is not an appropriate means of containing personally identifiable information. From this point, when encrypted data is included in the DID Document, it is important that the implementer does not encrypt it with the public key of the entity that does not want to be associated with the DID.

B-1) Decentralized Identifiers (DIDs) v1.0

- The following points are listed as privacy considerations.

#	Overview
Keeping personally identifiable information (PII) private	If a DID method specification is written for a public verifiable data registry where all DIDs and DID documents are publicly available, it is critical that DID documents contain no personal data. Personal data should instead be placed behind service endpoints under control of the DID subject. Personal data can be exchanged in private P2P using a secure communication channel identified by the public key description in the DID Document. This also enables DID subjects and requesting parties to implement the GDPR right to be forgotten, because no personal data is written to an immutable distributed ledger.
DID Correlation Risks and Pseudonymous DIDs	Since DIDs may be used for correlation, the DID controller can mitigate this privacy risk by using pairwise unique DIDs. In effect, each DID acts as a pseudonym.
DID Document Correlation Risks	The anti-correlation protection of the alias DID is easily broken if the data in the corresponding DID Document can be correlated. For example, using the same public key description or proprietary service endpoint in multiple DID Documents provides as much correlation information as using the same DID. A better strategy for endpoint privacy may be to share endpoints with thousands or millions of DIDs by many different subjects.
Assigning a type to the DID subject	It is dangerous to add properties to the DID Document that can be used to indicate the type and nature of the DID subject either explicitly or by inference. Not only do such properties potentially result in personal data or correlatable data being present in the DID document, but they can be used for grouping particular DIDs in such a way that they are included in or excluded from certain operations or functionalities. To minimize these risks, all properties in the DID Document should be meant to represent the cryptographic material, endpoint, or validation method associated with the use of DID.
Herd Privacy	When a DID subject is indistinguishable from others in the herd, privacy is available. To reduce digital fingerprints, share common settings across requesting party implementations, keep negotiated options to a minimum on wire protocols, use encrypted transport layers, and pad messages to standard lengths.

B-2) Verifiable Credentials Data Model 1.0

- At present, it is difficult to represent educational background qualifications, medical data, bank accounts, and various machine-readable personal information verified by other third parties on the Web. This specification provides a mechanism for expressing these types of credentials on the Web in a cryptographically secure, privacy-respecting, machine-readable way.

Verifiable Credentials Data Model 1.0

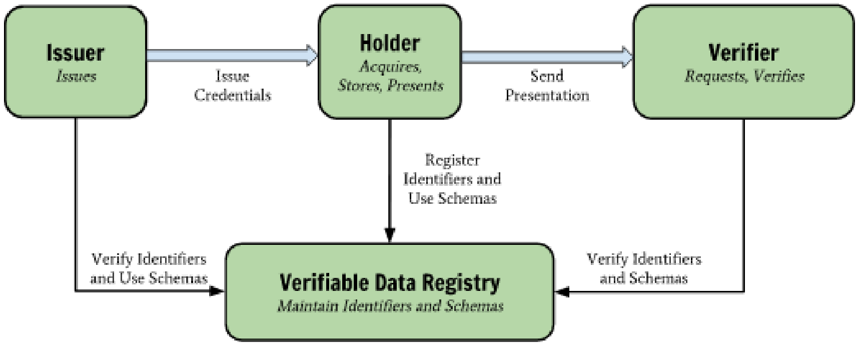

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

Figure 1 The roles and information flows forming the basis for this specification.

Actor	Overview
holder	The role played by an entity that holds one or more verifiable credentials and generates verifiable presentations from them. Examples: Students, employees, customers.
issuer	A role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Examples: Companies, nonprofits, industry associations, governments, and individuals.
subject	An entity about which claims are made. Examples: human beings, animals, and things. In many cases, the holder of a verifiable credential is the subject, but in some cases the parent (holder) possesses the verifiable credential of the child (subject) or the owner (holder) possesses the verifiable credential of the pet (subject).
verifier	The role played by an entity that receives one or more verifiable credentials, optionally inside a verifiable presentation. Examples: Employers, security officers, websites.
verifiable data registry	A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Examples: Trusted database, decentralized databases, government ID databases, decentralized ledgers.

Source) Verifiable Credentials Data Model 1.0
https://www.w3.org/TR/vc-data-model/

B-2) Verifiable Credentials Data Model 1.0

■ The following points are listed as security considerations.

#	Overview
Cryptography Suites and Libraries	Cryptography suites and libraries have a shelf life and eventually fall to new attacks and technology advances. Production quality systems need to take this into account and ensure mechanisms exist to easily and proactively upgrade expired or broken cryptography suites and libraries, and to invalidate and replace existing credentials. Regular monitoring is important to ensure the long term viability of systems processing credentials.
Content Integrity Protection	Verifiable credential often includes URLs to external data. Linked content that exists outside a verifiable credential are often not protected against tampering because the data resides outside of the protection of the proof on the verifiable credential. In order to protect the integrity of linked content, it is recommended to use a URL scheme that enforces the integrity of the content.
Unsigned Claims	This specification allows credentials to be produced that do not contain signatures or proofs of any kind. These types of credentials are often useful for intermediate storage, or self-asserted information, which is analogous to filling out a form on a web page. Implementers should be aware that these types of credentials are not verifiable because the authorship is either not known or cannot be trusted.
Token Binding	A verifier might need to ensure it is the intended recipient of a verifiable presentation and not the target of a man-in-the-middle attack. Approaches such as token binding [RFC8471], which ties the request for a verifiable presentation to the response, can secure the protocol. Any unsecured protocol is susceptible to man-in-the-middle attacks.
Bundling Dependent Claims	It is considered best practice for issuers to atomize information in a credential, or use a signature scheme that allows for selective disclosure. In the case of atomization, if it is not done securely by the issuer, the holder might bundle together different credentials in a way that was not intended by the issuer.
Highly Dynamic Information	When verifiable credentials are issued for highly dynamic information, implementers should ensure the expiration times are set appropriately. Expiration periods longer than the timeframe where the verifiable credential is valid might create exploitable security vulnerabilities. Expiration periods shorter than the timeframe where the information expressed by the verifiable credential is valid creates a burden on holders and verifiers. It is therefore important to set validity periods for verifiable credentials that are appropriate to the use case and the expected lifetime for the information contained in the verifiable credential.
Device Theft and Impersonation	When verifiable credentials are stored on a device and that device is lost or stolen, it might be possible for an attacker to gain access to systems using the victim's verifiable credentials. Ways to mitigate this type of attack include: ・Enabling password, pin, pattern, or biometric screen unlock protection on the device. ・Enabling password, biometric, or multi-factor authentication for the credential repository. ・Enabling password, biometric, or multi-factor authentication when accessing cryptographic keys. ・Using a separate hardware-based signature device. ・All or any combination of the above.

B-2) Verifiable Credentials Data Model 1.0

- The following points are listed as privacy considerations.

#	Overview (1/3)
Personally Identifiable Information	Data associated with verifiable credentials stored in the credential.credentialSubject field is susceptible to privacy violations when shared with verifiers. Personally identifiable data, such as a government-issued identifier, shipping address, and full name, can be easily used to determine, track, and correlate an entity. Even information that does not seem personally identifiable, such as the combination of a birthdate and a postal code, has very powerful correlation and de-anonymizing capabilities. Implementers are strongly advised to warn holders when they share data with these kinds of characteristics. Issuers are strongly advised to provide privacy-protecting verifiable credentials when possible. For example, issuing ageOver verifiable credentials instead of date of birth verifiable credentials when a verifier wants to determine if an entity is over the age of 18.
Identifier-Based Correlation	Subjects of verifiable credentials are identified using the credential.credentialSubject.id field. The identifiers used to identify a subject create a greater risk of correlation when the identifiers are long-lived or used across more than one web domain.
Signature-Based Correlation	The contents of verifiable credentials are secured using the credential.proof field. The properties in this field create a greater risk of correlation when the same values are used across more than one session or domain and the value does not change. Examples include the verificationMethod, created, proofPurpose, and jws fields. If strong anti-correlation properties are required, it is advised that signature values and metadata are regenerated each time using technologies like third-party pairwise signatures, zero-knowledge proofs, or group signatures.
Long-Lived Identifier-Based Correlation	Verifiable credentials might contain long-lived identifiers that could be used to correlate individuals. These include subject identifiers, email addresses, government-issued identifiers, organization-issued identifiers, addresses, healthcare vitals, verifiable credential-specific JSON-LD contexts and so on. Organizations providing software to holders are required to warn holders when this information is shared.
Device Fingerprinting	There are mechanisms external to verifiable credentials that are used to track and correlate individuals on the Internet and the Web. Some of these mechanisms include Internet protocol (IP) address tracking, web browser fingerprinting, evercookies, advertising network trackers, mobile network position information, and in-application Global Positioning System (GPS) APIs. Using verifiable credentials cannot prevent the use of these other tracking technologies. Also, when these technologies are used in conjunction with verifiable credentials, new correlatable information could be discovered. It is recommended that privacy-respecting systems prevent the use of these other tracking technologies when verifiable credentials are being used.
Favor Abstract Claims	To enable recipients of verifiable credentials to use them in a variety of circumstances without revealing more PII than necessary for transactions, issuers should consider limiting the information published in a credential to a minimal set needed for the expected purposes. One way to avoid placing PII in a credential is to use an abstract property that meets the needs of verifiers without providing specific information about a subject.

3-2-3. Consideration Specifications of each Standardization Organization

B-2) Verifiable Credentials Data Model 1.0

- The following points are listed as privacy considerations.

#	Overview (2/3)
The Principle of Data Minimization	Privacy violations occur when information divulged in one context leaks into another. Accepted best practice for preventing such violations is to limit the information requested, and received, to the absolute minimum necessary. With verifiable credentials, data minimization for issuers means limiting the content of a verifiable credential to the minimum required by potential verifiers. In addition, data minimization for verifiers means limiting the scope of the information requested or required for accessing services. Verifier is required to request only the information necessary for a particular transaction to occur.
Bearer Credentials	Bearer credentials are privacy-enhancing pieces of information, such as a concert ticket, which entitles the holder of the bearer credential to a specific resource without divulging sensitive information about the holder. Bearer credentials are often used in low-risk use cases where the sharing of the bearer credential is not a concern or would not result in large economic or reputational losses. Repeated use of the same bearer credential across multiple sites enables these sites to potentially collude to unduly track or correlate the holder. Similarly, information that might seem non-identifying, such as a birthdate and postal code, can be used to statistically identify an individual when used together in the same bearer credential or session. The bearer credential issuer must ensure that the bearer credential is single-use, does not contain personally identifiable information, and is not overly correlated.
Validity Checks	When processing verifiable credentials, verifiers are expected to perform validity checks including: ・The professional licensure status of the holder ・A date of license renewal or revocation. ・The sub-qualifications of an individual. ・If a relationship exists between the holder and the entity with whom the holder is attempting to interact. ･The geolocation information associated with the holder. The process of performing these checks might result in information leakage that leads to a privacy violation of the holder. For example, a simple operation such as checking a revocation list can notify the issuer that a specific business is likely interacting with the holder. This could enable issuers to collude and correlate individuals without their knowledge. Issuers are urged not to use mechanisms, such as credential revocation lists that are unique per credential, during the verification process that could lead to privacy violations.
Storage Providers and Data Mining	When a holder receives a verifiable credential from an issuer, the verifiable credential needs to be stored somewhere (for example, in a credential repository). Holders are warned that the information in a verifiable credential is sensitive in nature and highly individualized, making it a high value target for data mining. Services that advertise free storage of verifiable credentials might in fact be mining personal data and selling it to organizations wanting to build individualized profiles on people and organizations. Effective mitigations for data mining and profiling include: ・Service providers that do not sell customer information to third parties ・Software that encrypts the verifiable credential so that the service provider cannot view the contents of the credential ・Software that stores the verifiable credential locally on the customer management device and does not unexpectedly upload or analyze customer information.

3-2-3. Consideration Specifications of each Standardization Organization

B-2) Verifiable Credentials Data Model 1.0

- The following points are listed as privacy considerations.

#	Overview (3/3)
Aggregation of Credentials	Holding two pieces of information about the same subject almost always reveals more about the subject than just the sum of the two pieces, even when the information is delivered through different channels. The aggregation of verifiable credentials is a privacy risk and all participants in the ecosystem need to be aware of the risks of data aggregation. For example, if two bearer credentials, one for an email address and then one stating the holder is over the age of 21, are provided across multiple sessions, the verifier of the information now has a unique identifier as well as age-related information for that individual. It is now easy to create and build a profile for the holder such that more and more information is leaked over time. Aggregation of credentials can also be performed across multiple sites in collusion with each other, leading to privacy violations. Solutions tend to be through policies rather than technical approaches. If the holder does not want his or her information to be aggregated, the holder must state that information in the verifiable presentation he or she sends.
Usage Patterns	Despite the best efforts to assure privacy, actually using verifiable credentials can potentially lead to de-anonymization and a loss of privacy. If the same verifiable credential is presented to the same verifier more than once, the verifier could infer that the holder is the same individual. When the same verifiable credential is presented to different verifiers, those verifiers can collude or a third party can access the transaction records of both verifiers. An observer can infer that the individual presenting the verifiable credential is the same person in both services. In other words, it can be understood that the accounts are managed by the same person.
Sharing Information with the Wrong Party	When a holder chooses to share information with a verifier, it might be the case that the verifier is acting in bad faith and requests information that could be used to harm the holder. For example, a verifier might ask for a bank account number, which could then be used with other information to defraud the holder or the bank. Issuers should strive to tokenize as much information as possible such that if a holder accidentally transmits credentials to the wrong verifier, the situation is not catastrophic.
Frequency of Claim Issuance	Usage patterns can be correlated into certain types of behavior. Part of this correlation is mitigated when a holder uses a verifiable credential without the knowledge of the issuer. Issuers can defeat this protection however, by making their verifiable credentials short lived and renewal automatic. Organizations providing software to holders should warn them if they repeatedly use credentials with short lifespans, which could result in behavior correlation. Issuers should avoid issuing credentials in a way that enables them to correlate usage patterns.
Prefer Single-Use Credentials	Privacy-respecting systems would require only the information necessary for interaction with the verifier to be disclosed by the holder. The verifier would then record that the disclosure requirement was met and forget any sensitive information that was disclosed. Regulatory burdens and long-term storage identifiers can prevent this. The design of any verifiable credentials ecosystem, however, should strive to be as privacy-respecting as possible by preferring single-use verifiable credentials whenever possible.
Private Browsing	In an ideal private browsing scenario, no PII will be revealed. Different browser vendors handle private browsing differently, and some browsers may not have this feature at all. Because many credentials include PII, organizations providing software to holders should warn them about the possibility of revealing this information if they wish to use credentials and presentations while in private browsing mode.

B-3) Credential Handler API

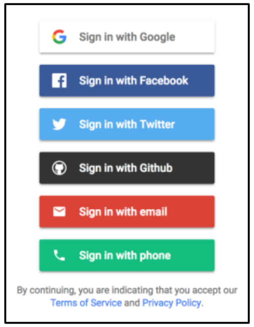
- The Credential Handler API (CHAPI) is an API for handling events related to credential requests and storage in the browser, and is based on two APIs: the Payment Handler API and the Credential Management API.
- This specification is intended to
  - Make it easier and more secure for users to use their credentials.
  - Allow users to choose their wallet provider.
  - Provide a standard wallet API for web app developers.
- In addition, the solution to the NASCAR problem in OAuth / OIDC is also specified.

Timeline for the development of the Credential Handler API

- Specifications released on W3C CCG (Credentials Community Group)
  - 2014 - Identity Credentials protocol proposed
  - 2017 - Web Payments Handler written by Dave Longley
  - 2017 - CHAPI Specification created by Dave Longley
  - 2017 - CHAPI adopted as W3C CCG Work Item

NASCAR problem

- The NASCAR issue is the problem of third-party icons and brands gathering on a website and becoming visual noise. Examples include the Payment UI and Sign-in UI.



By continuing, you are indicating that you accept our Terms of Service and Privacy Policy.

Source) INDIEWEBCAMP - NASCAR problem
https://indieweb.org/NASCAR_problem

B-3) Credential Handler API

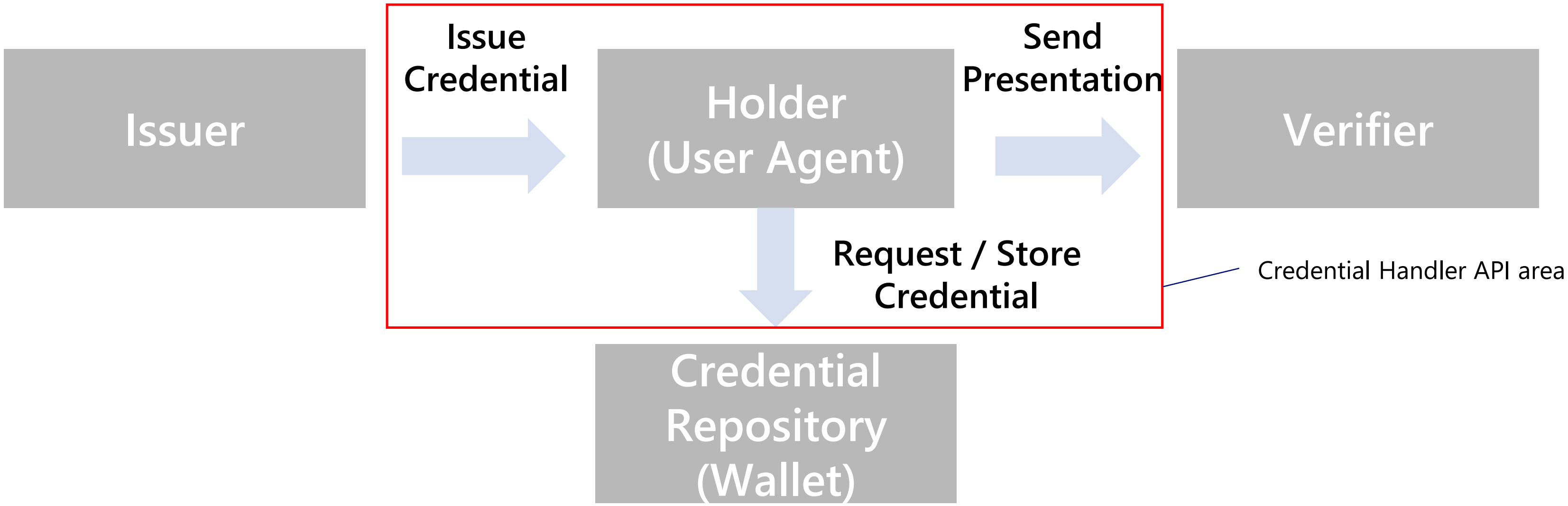
Process content

- Defines events related to Credential request and storage such as CredentialRequestEvent and CredentialStoreEvent
- Handles credential requests and storage events based on origins

Roles

- Credential Repository (Wallet): Stores user credentials and handle requests
- Credential Issuer (Issuer): Issues Credential to the user
- Credential Verifier (Verifier): Requests Credential from the user
- Mediator (User Agent): Mediates Credential storage and request

Overview of Credential Handler API


Issuer
Issue Credential
Holder (User Agent)
Send Presentation
Verifier
Request / Store Credential
Credential Handler API area
Credential Repository (Wallet)

Source)
https://github.com/w3c-ccg/credential-handler-api/#roles

3-2-3. Consideration Specifications of each Standardization Organization

B-3) Credential Handler API

- The following points are listed as privacy and security considerations.

#	Overview
Information about the User Environment	The API does not share information about the user's registered credential handlers. Information from origins is only shared with the relying party with the consent of the user.
User Consent Before Sending Credentials	One goal of this specification is to minimize the user interaction required to send credentials. At the same time, user agents must not permit combinations of configurations that would enable invoking Web sites to request credentials and receive them silently without any user consent.
Secure Communications	The Credential Handler is defined in the Service Worker code, which requires consideration of the Service Worker's Security Consideration. In addition, WebCredential security is outside the scope of this specification and is addressed by credential handlers that support managing them.
Credential Repository Authenticity	The user agent is not required to make available credential handlers that pose security issues. When a credential handler is unavailable for security reasons, the user agent should provide rationale to the credential handler developers (e.g., through console messages) and may also inform the user to help avoid confusion.
Data Validation	Relying parties should validate that the WebCredential data they have received through the Credential Management API is what they expect.
Private Browsing Mode	When the Credential Management API is invoked in a "private browsing mode," the user agent should launch credential handlers in a private context. This will generally prevent sites from accessing any previously-stored information. In turn, this is likely to require either that the user log in to the origin or re-enter details.

B-4) Confidential Storage 0.1

- Confidential Storage provides a privacy-respecting mechanism for storing, indexing, and retrieving encrypted data at the storage provider. This is useful when individuals or organizations want to protect their data so that storage providers cannot view, analyze, aggregate, or resell it. This approach ensures that application data is portable and protected from storage provider data breaches.

Overview Confidential Storage ecosystem

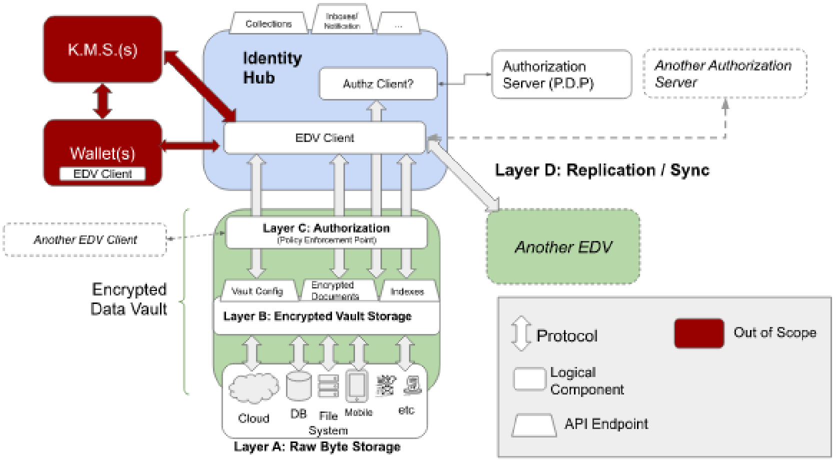


Figure 1 Confidential Storage layers

Requirement	Overview
Privacy and multi-party encryption	It must be encrypted both in transit (being sent over a network) and while it is at rest (on a storage system) to ensure the privacy of the entity's data and prevent unauthorized parties, including the storage provider, from accessing it. Since data could be shared with more than one entity, it is also necessary for the encryption mechanism to support encrypting data to multiple parties.
Sharing and authorization	The system is expected to specify one mandatory authorization scheme, but also allow other alternate authorization schemes.
Identifiers	The system should be identifier agnostic. In general, identifiers that are a form of URN or URL are preferred.
Versioning and replication	It is expected that information can be backed up on a continuous basis. For this reason, it is necessary for the system to support at least one mandatory versioning strategy and one mandatory replication strategy, but also allow other alternate versioning and replication strategies.
Metadata and searching	Large volumes of data are expected to be stored using this system, which then need to be efficiently and selectively retrieved. To that end, an encrypted search mechanism is a necessary feature of the system. It is important for clients to be able to associate metadata with the data such that it can be searched.
Protocols	At least one protocol is required because the system can reside in a variety of operating environments, but it is important that the other protocols are allowed by design.

Source)
https://identity.foundation/confidential-storage/

B-4) Confidential Storage 0.1 – Challenges and New Initiatives

- The following points are listed as security considerations.

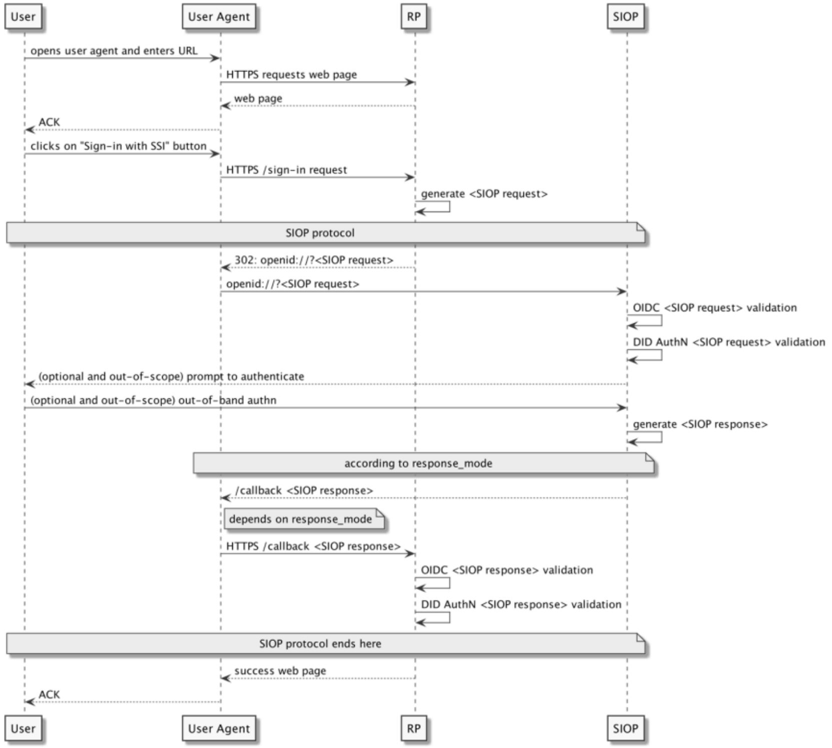
#	Overview
Malicious or accidental modification of data	While a service provider is not able to read data in an Encrypted Data Vault, it is possible for a service provider to delete, add, or modify encrypted data. The deletion, addition, or modification of encrypted data can be prevented by keeping a global manifest of data in the data vault.
Compromised vault	An Encrypted Data Vault can be compromised if the data controller (the entity who holds the decryption keys and appropriate authorization credentials) accidentally grants access to an attacker. For example, a victim might accidentally authorize an attacker to the entire vault or mishandle their encryption key. Once an attacker has access to the system, they may modify, remove, or change the vault's configuration.
Data access timing attacks	While it is normally difficult for a server to determine the identity of an entity as well as the purpose for which that entity is accessing the Encrypted Data Vault, there is always metadata related to access patterns, rough file sizes, and other information that is leaked when an entity accesses the vault.
Encrypted data on public networks	When protecting data, it is safe to assume that all encryption schemes will eventually be broken. For this reason, use any kind of public storage network as a storage strategy for servers to store encrypted data should be avoided.
Unencrypted data on server	There are a handful of fields that cannot be encrypted in this system. For example, a version number associated with data provides insight into how often the data is modified. The identifiers associated with encrypted content enables a server to gain knowledge by possibly correlating identifiers across documents. Implementations are advised to minimize the amount of information that is stored in an unencrypted fashion.
Partial matching on encrypted indexes	There are a number of operations that are common in search systems that are not available with encrypted indexes, such as partial matching on encrypted text fields or searches over a scalar range. These features might be added in the future through the use of zero-knowledge encryption schemes.
Threat model for malicious service provider	The following attacks by malicious service providers are possible. ・Correlation of entities accessing information in the vault ・Speculation about the types of files stored in a vault depending on file size and access patterns ・Addition, deletion, and modification of encrypted data ・Failure to enforce the authentication policy set on the encrypted data ・Exfiltrating encrypted data to an unknown external system.

C-1) Self-Issued DID Profile for OpenID v1.0

- Self-Issued DID Profile for OpenID (SIOP DID) is a specification for using OpenID Connect for DID AuthN as a generic way to integrate Identity Wallet into web applications.
- The RP is expected to be a web application, and the Identity Wallet application will be started from a mobile application or desktop browser.
- The overall processing flow is done in an implicit flow according to OIDC Core 7. Self-Issued OpenID Provide.

SIOP DID processing flow

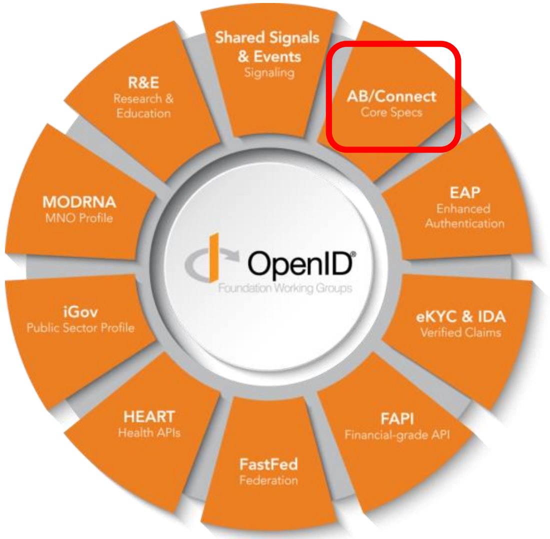
1. User accesses RP
2. The RP returns a "Sign-in with SSI" button, and when
 the User presses it, a SIOP Request is generated.
3. SIOP is activated by SIOP Request (openid://?<SIOP request>)
4. SIOP validates SIOP request according to OIDC / DID
AuthN and generates SIOP response.
5. SIOP Response is passed to RP according to the specification of response_mode.
6. The RP validates the SIOP response according to OIDC / DID AuthN.


User
User Agent
RP
SIOP
opens user agent and enters URL
HTTPS requests web page
web page
ACK
clicks on "Sign-in with SSI" button
HTTPS /sign-in request
generate <SIOP request>
SIOP protocol
302: openid://?<SIOP request>
openid://?<SIOP request>
OIDC <SIOP request> validation
DID AuthN <SIOP request> validation
(optional and out-of-scope) prompt to authenticate
(optional and out-of-scope) out-of-band authn
generate <SIOP response>
according to response_mode
/callback <SIOP response>
depends on response_mode
HTTPS /callback <SIOP response>
OIDC <SIOP response> validation
DID AuthN <SIOP response> validation
SIOP protocol ends here
success web page
ACK
User
User Agent
RP
SIOP

Source) Self-Issued OpenID Connect Provider DID Profile v0.1
https://identity.foundation/did-siop/

C-1) Self-Issued DID Profile for OpenID v1.0 – Challenges and New Initiatives

- On November 9, 2020, it was announced that SIOP DID work will be suspended due to the signing of the Liaison Agreement between OIDF and DIF.
  - In the future, the OIDF AB / Connect WG will proceed with the revision of 7. SIOP of OIDC Core.
  - After the AB / C WG completes the SIOP specification work, the DIF Authentication WG will resume work.



Discussions in OIDF

Discussions centered on the Scope described in Requirements for OIDC Self-Issued OpenID Provider

- **Scope**
  - A. SIOP request
  - B. SIOP response
  - C. Key recovery and key rotation
  - D. Trust model between RP and SIOP
  - E. Issuance of the claims
  - F. Privacy protection

Discussions in DIF

January 2021 Announced the status of the specification study at the DIF Face to Face community event

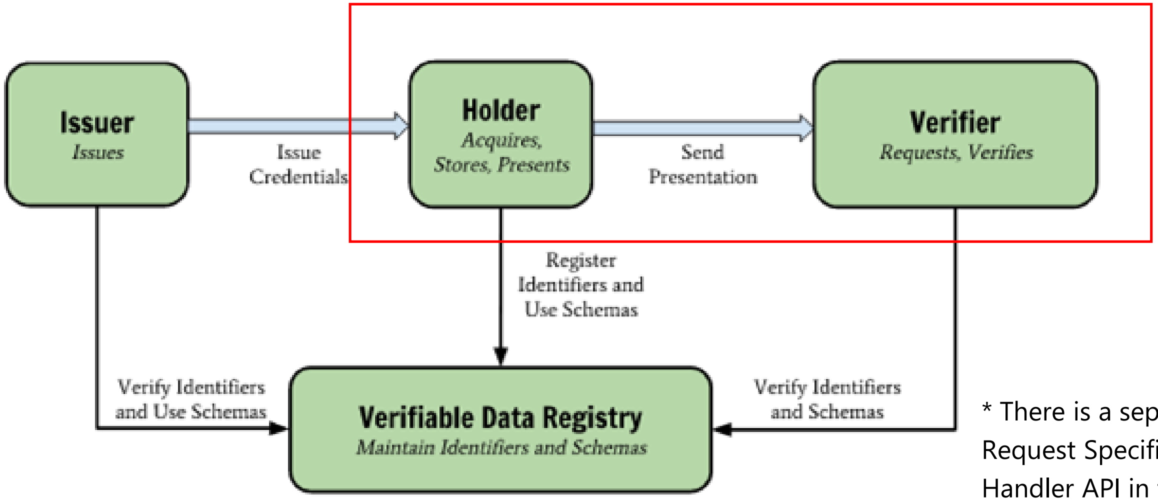
- **Current Draft**
  - OpenID Connect Claims aggregation (adopted)
  - OpenID Self Issued Identifiers (adopted)
  - Self-Issued OpenID Provider v2 draft01 (adopted)
  - OpenID Connect Credential Provider
  - Smart Credentials
  - Portable Identifiers: WIP

Source)
https://bitbucket.org/openid/connect/src/master/SIOP/siop-requirements.md

C-2) Presentation Exchange

- The Presentation Exchange defines a data format for Verifiers to clarify Proof requirements and for Holders to present Proofs according to the requirements.
- Presentation Exchange is a claim format- and transport protocol-independent mechanism that eliminates redundant processing, code, and effort.
- An example of supported Claim formats and transport protocols is as follows.
  - Claim Formats: JSON Web Token（JWT）、Verifiable Credential（VC）、JWT Verifiable Credential（JWT-VC）
  - Transport Protocols: OpenID Connect、DIDComm、Credential Handler API

Overview of Presentation Exchange


Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

* There is a separate Verifiable Presentation Request Specification for use with the Credential Handler API in the W3C Credential Community Group.

Source) Presentation Exchange
https://identity.foundation/presentation-exchange/

C-3) Presentation Exchange – Presentation Definition & Presentation Submission

- The request and presentation of Proof between Holder and Verifier are defined in the following terms.
  - **Presentation Definition**: Defines Proof required by the Verifier
  - **Presentation Request**: Defines how to transfer Presentation Definition from the Verifier to the Holder
  - **Presentation Submission**: Defines how to present a Proof according to the Presentation Definition specified by the Verifier

Example of a definition using the Presentation Definition object

```
{
  "comment": "Note: VP, OIDC, DIDComm, or CHAPI outer wrapper would be here.",
  "presentation_definition": {
    "id": "32f54163-7166-48f1-93d8-ff217bdb0653",
    "input_descriptors": [
      {
        "id": "wa_driver_license",
        "name": "Washington State Business License",
        "purpose": "We can only allow licensed Washington State business",
        "schema": [{
            "uri": "https://licenses.example.com/business-license.json"
        }]
      }
    ]
  }
}
```

Example of a definition using the Presentation Submission object

```
{
  // NOTE: VP, OIDC, DIDComm, or CHAPI outer wrapper properties would be here.
  "presentation_submission": {
    "id": "a30e3b91-fb77-4d22-95fa-871689c322e2",
    "definition_id": "32f54163-7166-48f1-93d8-ff217bdb0653",
    "descriptor_map": [
      {
        "id": "banking_input_2",
        "format": "jwt_vc",
        "path": "$.verifiableCredential[0]"
      },
      {
        "id": "employment_input",
        "format": "ldp_vc",
        "path": "$.verifiableCredential[1]"
      },
      {
        "id": "citizenship_input_1",
        "format": "ldp_vc",
        "path": "$.verifiableCredential[2]"
      }
    ]
  }
}
```

Source) Presentation Exchange - 4. Presentation Definition, 5. Presentation Submission
https://identity.foundation/presentation-exchange/

3-2-3. Consideration Specifications of each Standardization Organization

C-2) Presentation Exchange – Challenges and New Initiatives

■ Security considerations

- There are currently no security considerations listed in this specification. The addition of a section on security considerations has been discussed in an Issue on GitHub. *1)
- There is also a concern in the Issue that if a Holder automatically responds to a request from a Verifier, the Verifier may be able to profile the Holder by running Presentation Exchange multiple times, defeating the purpose of privacy protection. *1)

■ Initiatives for the future

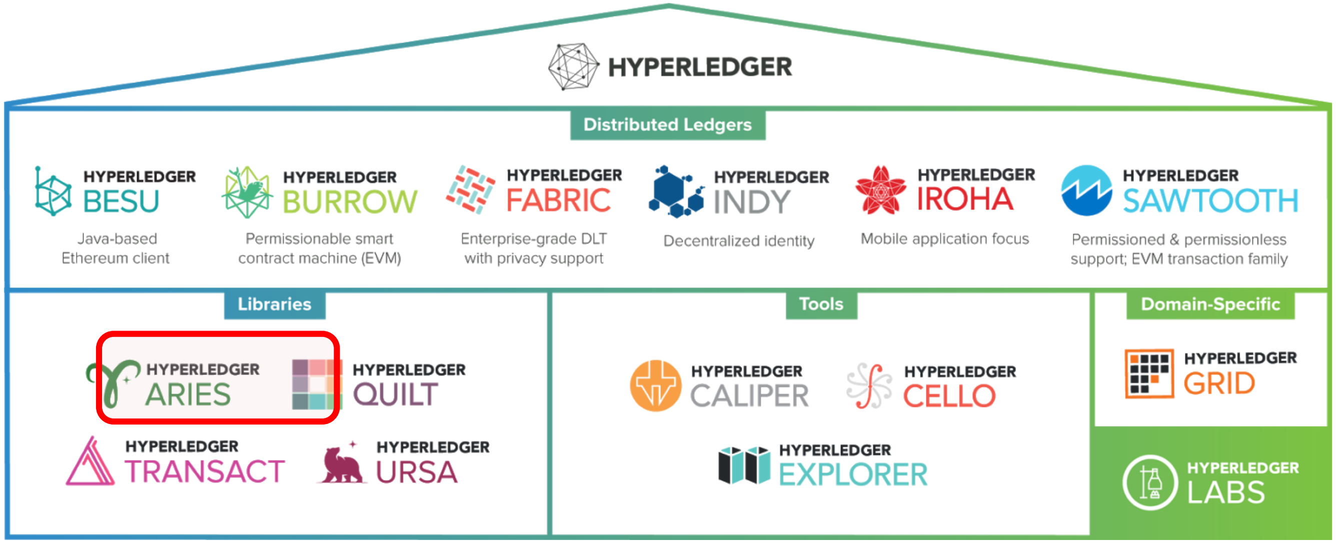
- A very similar specification to Presentation Exchange, the Verifiable Presentation Request Specification, has been published by the W3C CCG and is being considered for integration or coexistence. *2)
- On GitHub, there are some questions about the process flow when using OpenID Connect, which is a transport protocol supported by Presentation Exchange. *3) *4)

Sources) *1) Security Considerations, https://github.com/decentralized-identity/presentation-exchange/issues/204
*2) IIW30 CHAPI and DID Comm 101, https://docs.google.com/presentation/d/1qPbwx9IXwPlgsZgS2XPXeGgstxrixnC8n0E2I4cxVc8/edit
*3) What does PE look like within OpenID Connect? #101, https://github.com/decentralized-identity/presentation-exchange/issues/101
*4) Examples that show support for regular OIDC flow, https://github.com/decentralized-identity/presentation-exchange/issues/92

D) Aries RFC

- Hyperledger is a project to build a blockchain supported by the Linux Foundation
- The Hyperledger Aries project aims to define and share the message exchange protocol, agent architecture and tests
  - The concepts and features that make up the Aries project are documented in the Hyperledger aries-rfcs GitHub repository.
  - The Aries RFC is defined into two groups: concepts (background information across all protocols) and features (specification of a particular protocol).
  - Hyper Ledger Indy has a separate repository called indy-hipe that corresponds to aries-rfc.

The position of the Hyperledger Aries project in the Hyperledger project



Source)
https://www.hyperledger.org/

D-1) Aries RFC 0023: DID Exchange Protocol 1.0

■ This specification specifies a protocol for exchanging DIDs between Agents.

■ The following two roles are specified:

- Requester

  A party that initiates this protocol after receiving an invitation message or using an implicit invitation from the Public DID.

- Responder

  The sender of the invitation or the issuer of the DID with an implicit invitation. You need to be able to interact with other agents via DIDComm.

■ The outline of the process flow is as follows:

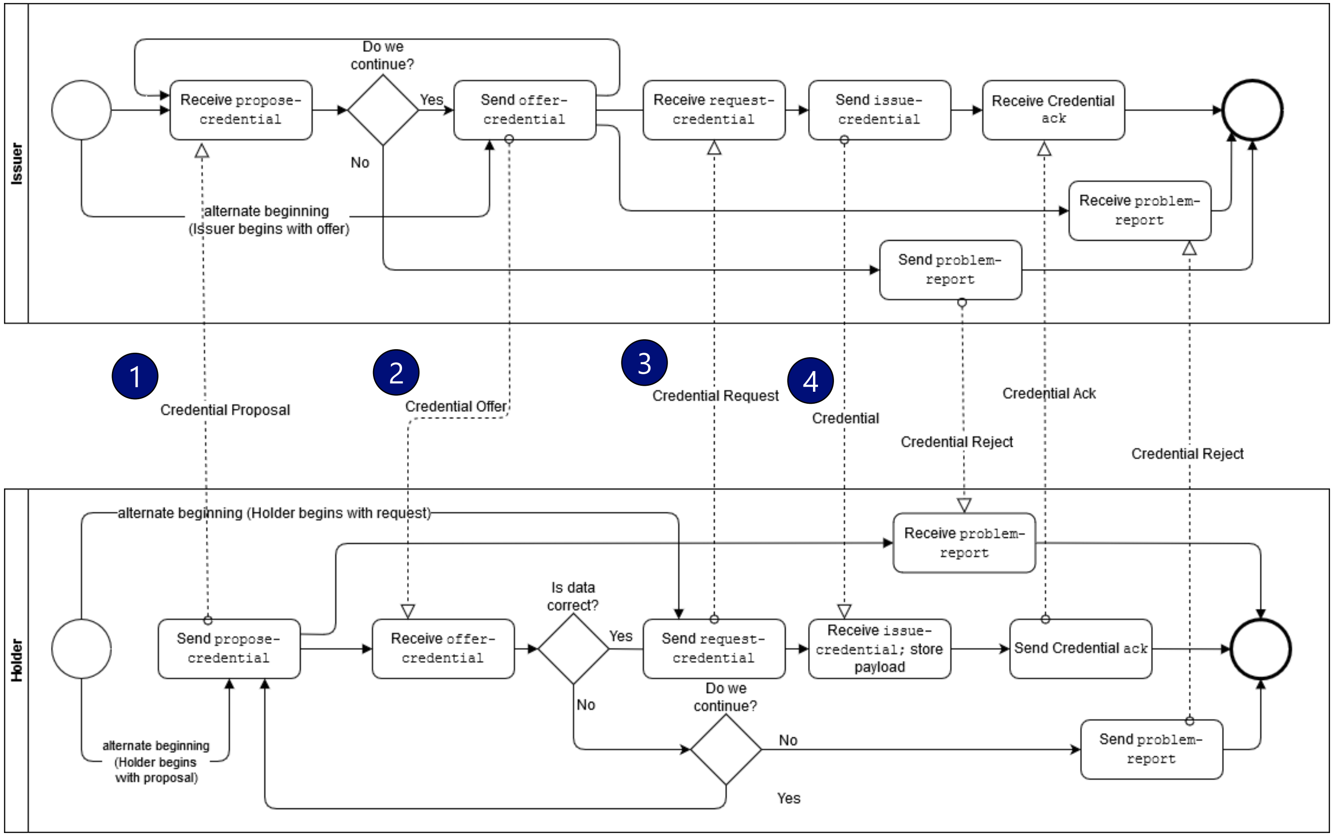
1. The Responder provides its information to the Requester using invitation messages from the out-of-band protocol and invitation messages contained in the Responder's Public DID.
2. The Requester sends the DID and DID Document as request message to the Responder based on the received information.
3. The Responder sends the DID and DID Document as a response message to the Requester using the information contained in the sent DID Document.
4. The Requester sends a message to the Responder notifying that it has received a response message.

Source) Aries RFC 0023, Aries RFC 0434
https://github.com/hyperledger/aries-rfcs/blob/master/features/0023-did-exchange/README.md
https://github.com/hyperledger/aries-rfcs/blob/master/features/0434-outofband/README.md

D-2) Aries RFC 0036: Issue Credential Protocol 1.0

- The Issue Credential Protocol formalizes the messages that are used to issue credentials. This protocol is not dependent on any particular credential format. Examples of supported credential formats include JWT, JSON-LD, and ZKP. Also, if a credential format that does not fit into this protocol to be used, an issue can be submitted through GitHub..
- This protocol deals with two roles, the Issuer and the Holder

1. A request to initiate a protocol sent by the Holder to Issuer. Or a request that specifies the credentials that the Holder requires from the Issuer.
2. Information about the credentials and the value that the Issuer will send to the Holder.
3. Requests for credentials sent by the Holder to the Issuer.
4. The response with credentials to the Credential Request.

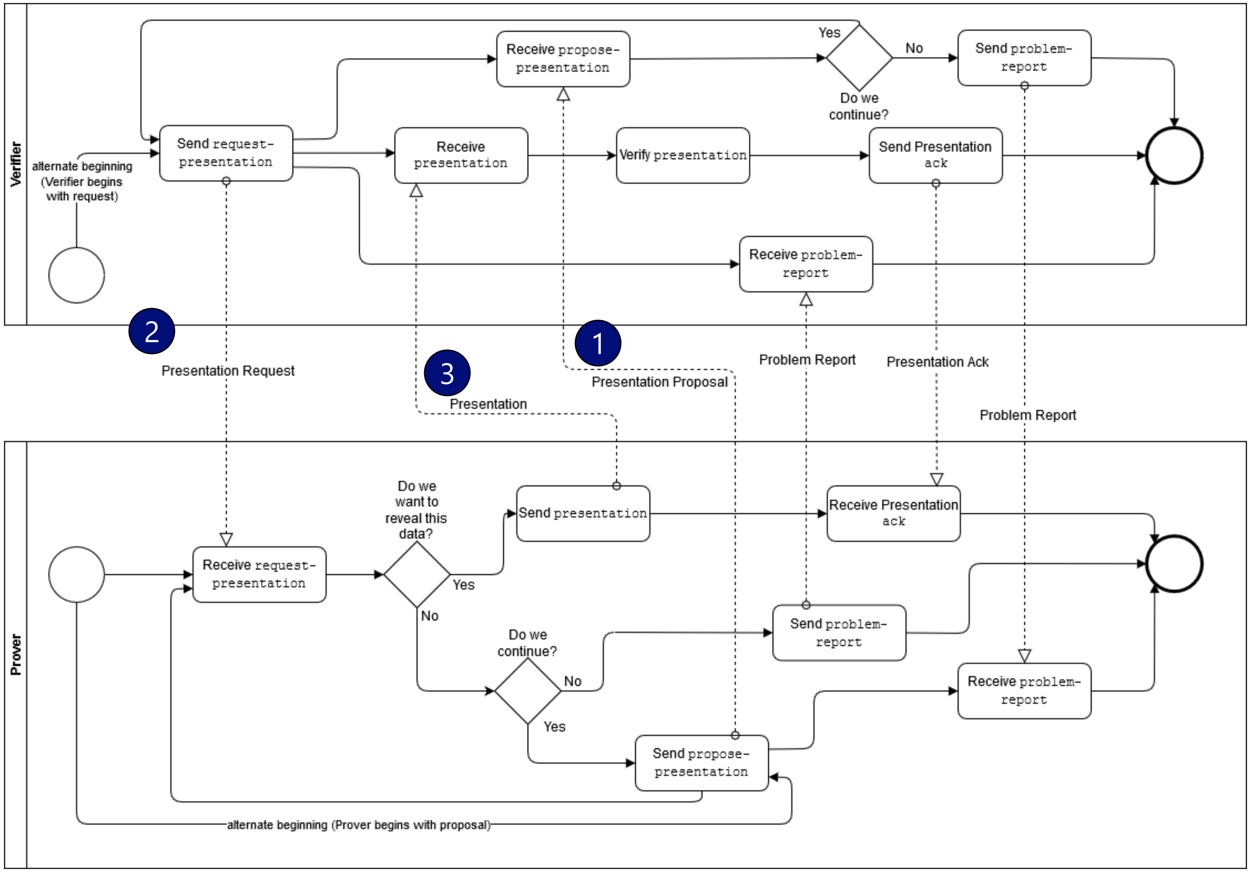


Source) https://github.com/hyperledger/aries-rfcs/blob/master/features/0036-issue-credential/README.md

D-3) Aries RFC 0037: Present Proof Protocol

- The Present Proof Protocol formalizes the message used to present a Proof. This protocol is for messages used to present verifiable claims, and is not dependent on any particular presentation mechanism. However, as of version 1.0, the only supported presentation mechanism is Hyperledger Indy.
- This protocol handles two roles, the Verifier and the Prover

1. The message sent by the Prover to the Verifier to start the Proof Presentation. Or a response to a Presentation Request when the Prover wants to use a different Presentation format.
2. The request for credentials sent by the Holder to the Issuer.
3. The response to a Presentation Request containing a signed Presentation sent by the Verifier to the Prover.



Source) https://github.com/hyperledger/aries-rfcs/blob/master/features/0037-present-proof/README.md

D) Aries RFC – Challenges and New Initiatives

- Aries and DIF jointly host the DID Communication working group and participate in the specification of the communication protocol not only for the ecosystem built around Aries, but also for the entire distributed identity community. *1)
- Aries has its own Conformance Test profile called the Aries interoperability profile. However, this is only to show that the Aries protocols and architecture have been successfully implemented. Interoperability here means interoperability with other Aries systems and conformance with Aries' common interpretation of the standard VC data model and the protocols defined by the community based on that interpretation. The W3C CCG is working on the VC-HTTP-API Test Suite and the DID core Test Suite as test suites for the W3C core specifications. The Aries interoperability profile is focused on its own infrastructure, with a focus on the blockchain-based ZKP system privacy assurance. This focus does not replace the W3C test suite, but complements it. *2)

Sources)
*1) Drilling down: Co-development, https://medium.com/decentralized-identity/drilling-down-co-development-in-the-open-765a86ab153f
*2) Setting Interoperability Targets, https://blog.identity.foundation/setting-interoperability-targets/

3-2-4. Overview of Control Components

Governance Framework of Digital Identity (Trust Framework)

- ■ The Open Identity Exchange (OIX) Trust Framework, introduced in Chapter 1, proposes a Framework that does not rely on specific technical elements, but builds on the lessons learned from existing major Trust Frameworks. It is also a guide for regulators to understand the relevance of the Trust Framework in defining appropriate regulations in areas such as AML. It is also expected to be applied to SSI.
- ■ Based on these characteristics, this study summarizes the components of governance based on the items specified in the framework. At the same time, the governance considerations in the SSI model are summarized.

Components specified in the OIX trust framework

Components	Items
Principles	
Trustmark(s) and UX	
Roles and Obligations	
General Rules	Record Keeping and Audit Trail
	Fraud and Cyber Controls
User Services	Choosing a Digital Identity
	Creation and Management of a Digital Identity
	Achieving and Presenting Trust
	Consent
	Help and Support

Components	Items
Relying Party Services	User Access to Identity Service
	Requests and Responses (API)
	Relying party Based Identity Assurance
	Liability
	Service Levels
	Help & Support
Trust Rules	Proofing
	Identity Assurance
	Authentication
	Eligibility Assurance

Components	Items
Security and Technical Requirements	Security Rules
	Trust Registry of eco-system participants
	Recording and Presentation of evidence Proofs
	Request and Response Schemas
Interoperability Requirements	Internal Interoperability
	External Interoperability
Governance of the Trust Framework	Creation and Management of a Trust Framework
	Enforceability of a Trust Framework
	Certification to a Trust Framework
	Operation of a Trust Framework

Source) OIX," OIX Guide to Trust Frameworks(version 0.1 Beta)"

Overview of Elements Required in Trust framework

Element		Overview
1. Principle		• Defines priorities for considering the needs of multi-stakeholders. 1.User, 2. RP, 3.Framework • 1. Defines four principles (4Cs) for User （Convenience, Choice, Control, Confidence）
2. Trustmark(s) and UX		• A signal that makes it possible for User, RP, and Evidence Issuer to recognize that the Trust Framework is in operation. (Symbols, phrases, etc.) • It is also possible to show interoperability between frameworks by creating a comprehensive trust mark or by listing the comprehensive agreements between frameworks when displaying the trust mark. (Examples: phrases, words, symbols, etc. In similar cases, the Visa brand, etc. in payments）
3. Roles and Obligations		-
4. General Rules	Record Keeping and Audit Trail	• To ensure the integrity of data tracking and Trust Framework, it is necessary to keep audit records regarding the following: ➢ Data generation, update, deletion, evidence collection / presentation, warranty evaluation (assessment), credential issuance and use.
	Fraud and Cyber Controls	• The entire identity ecosystem in the trust framework needs to be protected against cyber attacks and identity fraud. • In addition, entities participating in the trust framework have some responsibility for fraud and cyber risk management, depending on their role ➢ Defending against fraud, detecting fraud, informing and reporting to the parties involved, sharing attack information among organizations engaged in fraud prevention activities, localizing the impact and closing the target ID, handling and recovering from the attack, obtaining evidence, and presenting evidence for prosecution and investigation.

Source) Created by NRI based on OIX Governance framework

3-2-4. Overview of Control Components

Overview of Elements Required in Trust framework

Element		Overview
5. User Service	Choosing a Digital Identity	• IDP search, existing ID search, CI / CDD of RP in On-Going, Authentication requirements
	Create & Manage ID	• Identity lifecycle management. Especially credential, Account Recovery, notification to RP when attribute information is updated, etc.
	Achieving and Presenting Trust	• Evidence retention, fulfillment of the guarantee level required by RP. Ideally, the user should be able to use it without being aware of the guarantee level.
	Consent	• It is possible to link the original attribute information of user consent. The user has the right to review the sharing / usage history and the right to delete the data.
	Help and Support	• The Identity Provider can be changed at any time and has the portability of Identity Proofing information. • It is possible to notify the RP and restore the credential when the credential is compromised.
6. Relying Party Services	User Access to Identity Service	• Trustmark can be selected by RP
	Requests and Responses(API)	• Interface definition and request / response definition that are not restricted by Identity Provider / verifier selection.
	RP Based ID Assurance	• Defines the Identity Assurance Model, acts as a guide for RP users (to complete the guarantee level without being aware of it).
	Liability	• Responsibility model, liability in case of failure, liability imposed when framework rules deviate, litigation, need for mediator / arbitrator.
	Service Levels	• Differentiation / competitiveness by Trust scheme and Differentiation / competitiveness by Trust scheme and Broker.
	Help and Support	• Realization of IDP portability and freedom of choice, compliance and grievance handling while maintaining continuous access to RP accounts. • Differentiation by guarantee mechanism

Source) Created by NRI based on OIX Governance framework

Overview of Elements Required in Trust framework

Element		Overview
7. Trust Rules	Proofing	• Validation, Verification, and Identity Risk Assessment are defined as technical elements of ID Proofing. Also mentions Proofing Score assignment to Identity Assurance Assessment. • Interoperability between frameworks may be achieved by matching / equivalence judgment of Proofing Score.
	Identity Assurance	• In the Identity Assurance Process, it is necessary to consider the definition of the guarantee level, the guarantee level of identity verification / personal authentication, and the binding process. • Interoperability between frameworks may be achieved by guarantee level matching / equivalence judgment.
	Authentication	• In order to present the level of reliability / evidence / eligibility to the RP and to maintain the Digital Identity, it is necessary to perform personal authentication processing using credentials. • Continuous trust verification (Evidence validation and reverified) should be considered.
	Eligibility Assurance	• Validation / Verification of Eligibility Evidence to guarantee eligibility.

Source) Created by NRI based on OIX Governance framework

Overview of Elements Required in Trust framework

Element		Overview
8. Technical and Security Requirements	Security Rules	• Definition of rules that apply to the parties in the framework and compliance with them is required (It is necessary to establish rules regarding data during hibernation, data during transit, and operational security management).
	Trust Registry of eco-system participants	• Registry implementation / recording / checking required to manage participating parties.
	Recording and Presentation of evidence Proofs	• Define how evidence proof history is recorded during the evidence collection, generation, and presentation phases. It is also necessary to consider cryptographic technology so that the history will not be tampered with. • Consider whether to support zero-knowledge proof.
	Request and Response Schemas	• Request / response schema definition is required so that Identity Evidence and identity information are presented to the RP in a consistent manner. （Especially important for Trust Frameworks that support multiple Evidence Issuers） • Globally defined schemas such as OIDF / W3C should be considered. • Necessity of requirement for localization depending on the Evidence Type, but the framework should prepare for it and implement a curator for a locally applicable schema.

Source) Created by NRI based on OIX Governance framework

Overview of Elements Required in Trust framework

Element		Overview
9. Interoperability	Internal Interoperability	Achieved by complying with rule settings at the Trust framework level or by having the parties comply with multiple individual schemes to achieve interoperability between use case sectors. The following are stated as rules that should be set at the Trust framework level. ➢ Application of Principles ➢ Trustmark Rules ➢ Trust Rules and model, but perhaps leave the setting of acceptable scores within the model for particular use cases to the trust scheme. ➢ Technical Rules such as used of common levels of Security and common Schemas
	External Interoperability	The following three points are mentioned as means for realizing external interoperability with other Trust frameworks. 1) Mutual agreement. Mutual recognition of trust guaranteed by framework 2) Through the node approach *, many agents independently evaluate the integrity and compatibility of many frameworks, and multiple trust frameworks trust each other. 3) Compliance with multiple trust frameworks of parties such as IDP and evidence verifier *The node approach only requires each framework to follow commonly agreed rules, making it an efficient means of achieving a large amount of interoperability between frameworks. So-called "Framework of frameworks") The following are stated as design / implementation points to be considered for interoperability. ➢ Application of Framework Principles ➢ Trustmark Rules ➢ Trust Rules ➢ Record Keeping ➢ Fraud Controls ➢ Response Schema ➢ Security Standards

Source) Created by NRI based on OIX Governance framework

Overview of Elements Required in Trust framework

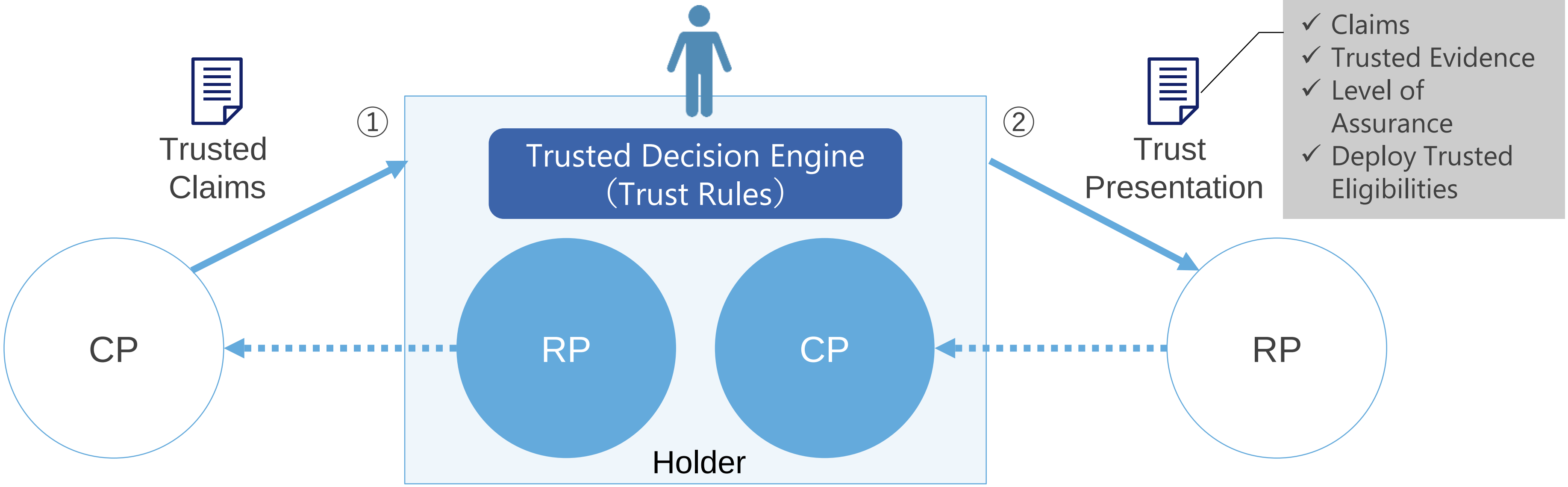
Element		Overview	
10. Governance	Creation and Management of a Trust Framework	• Defines 5 models for the Trust framework generator. 1）Independent Governing Entity 2）Consortium of Participating Entities 3）Single Participant Governing Entity 4）Non-Governing Standards or Certification Organization 5）Mutual Agreement Among All	（Example cases） 1）DIACC 2）CA/Browser Forum 3）Single ID Provider, GOV.UK Verify 4）Kantara Initiative ID Assurance framework, tScheme tScheme Approval Profile 5）- (There is no individual management entity)
	Enforceability of a Trust Framework	• The following three cases are described as the compulsory force for compliance with the rules: 1）Private Sector: Enforcement by Contract Mechanism. 2）Government Sector / Government Sponsor: Enforcement by laws and regulations. 3）Public-private partnership: Hybrid (main principles are legal compliance, specific requirements are enforced by contract, etc.).	
	Certification to a Trust Framework	• Authentication of entities participating in the trust framework. (As a trail fulfilling the obligations defined by the Trust Framework) • The certification method is as follows (each level is detailed in the attached sheet). ➢ Self-Assessment ➢ Verified Self-Assessment ➢ Approved ➢ Certified	
	Operation of a Trust Framework	• A Trust Framework Provider is required to take responsibility for the development and maintenance of the Trust Framework and fix it when problems occur. • The following are mentioned as examples of control functions (details of each level difference are given in a separate sheet). ➢ Governance and Policy Development ➢ Policy Enforcement ➢ Participating Entity Management ➢ Network Evolvement ➢ Trust Framework Operations	

Source) Created by NRI based on OIX Governance framework

Image of Applying the Trust framework in the SSI Model

- In the Trust Framework of the Open Identity Exchange (OIX), the Trust framework approach in the SSI model is mentioned. A unique point is that the Holder has two roles.
  - ① As a “RP", Holder receives Claims from the CP
  - ② As an “CP", Holder deploys the claims obtained in ①
- In the trust framework, the responsibilities are assigned according to the roles. If the holder takes on the above two roles, it is necessary to realize most of the governance requirements described above. Therefore, there are some challenges to be overcome in terms of actual operation, such as dealing with audits, managing credentials, and organizing liability. The details are described in detail in Chapter 3-4.

Image of Holder's role



Source) Created by NRI based on “OIX Quarterly Workshop - 15th Dec 2020”

3-3. Major SSI/DID Preceding and PoC Projects

3-3. Major SSI/DID Preceding and PoC Projects

Main Points of this Section

- Currently, various demonstration experiments using SSI/DID involving financial institutions are underway in Japan and other countries.
- It was found that financial institutions are interested in SSI/DID mainly to improve the efficiency of customer registration procedures and to prevent AML.

- However, many of these initiatives are currently at the demonstration level, and only a few, such as Canada's Verified.Me, is deployed as actual services.
  - Verified.Me started as a consortium model, and at the time of its launch, only financial institutions as IdP, and government agencies and some life insurance companies as service providers participated in the model. Therefore, the concept of SSI is realized by limiting the usage scenarios of users to a certain extent.
  - In terms of governance compliance, the model is unique in that it complies with the PCTF established by DIACC.

- One of the initiatives that is attracting attention in the EU, especially for its practical application in the future, is the project using Alastria_ID, which is being proceeded mainly in Spain, and is represented by the project Dalion promoted by Santander.
  - Alastria states its compliance with the EU's GDPR and eIDAS, and it is positioned as a solution that can comply with the EU's strict regulations.
  - However, Alastria itself only develops and provides the technical framework for Alastria_ID, and the actual use cases are being considered in individual projects such as Dalion. It is not clear at this point how the participating stakeholders in each project will divide their responsibilities to build the business model, and this is considered to be an issue for the future.

3-3-1. Major Cases of Projects Involving Financial Institutions

- At present, various initiatives related to SSI/DID are underway, particularly overseas, but most of them are at the trial phase, and few of them have been applied to actual services.
- The following are some of the major SSI/DID-related initiatives in which financial institutions are involved.

Country	Financial Institution	Use Case	Partner	Roles of Financial Institution	Overview
Canada	Seven major Canadian banks	Government, life insurance, etc.	SecureKey Technologies	Banks participate as IdPs	Seven major Canadian banks have formed a consortium to launch a service called Verified.Me in May 2019, the service that will be available from May 2019. Identity verification information is asserted to life insurance companies.
Spain	Banco Santander	Application for car rental, insurance and loans, and application to the government	CaxiaBank、MAPFRE(Insurance company), Repsol(fossil fuel company)Alastria (Non-profit blockchain consortium)	Joint venture acts as identity platform. The bank itself acts IdP	A secure and reliable identity platform that gives users more control over their personal information, thereby protecting their privacy and providing them with once-only convenience. The system is currently in the trial phase and is due to be released in May 2021.
Spain	Veridas (Joint venture between BBVA and das-Nano)	Finance	BBVA/Bankia/ Renta 4 Banko	Provide advanced biometric features (face, voice, fingerprint, etc.) Security protection	It provides features such as opening bank accounts and biometric authentication for online transactions to various financial institutions, including BBVA.
		Administration	Government of Navarra (Spain)		It provides the government of Navarra with the ability to carry out administrative procedures online, control borders using facial recognition technology, and provide secure and fast identification.
Germany	Deutsche Bank	Administration, banks, health care, etc.	Deutsche Bahn, Daimler, Lufthansa	Joint venture acts as identity platform. The bank itself acts IdP	Verimi, which is a company established with investments from other companies, will provide a single point of contact for IDs as a digital ID platform and use cases for digital IDs in banks, government, healthcare, mobility and online games.

Source) Created by NRI based on press releases from various companies, etc.

3-3. Major SSI/DID Preceding and PoC Projects

3-3-1. Major Cases of Projects Involving Financial Institutions

Country	Financial Institution	Use Case	Partner	Roles of Financial Institution	Overview
UK	Barclays	Administration (e.g. receipt of national pension)	UK Government	Connect to GOV.UK identity	As part of the Government's GOV.UK Authentication Initiative, it is accredited as an IdP and identity assertion is conducted, making it easy to verify identity when accessing UK Government services.
Global	MasterCard	Customer identity management for telecoms companies	Optus (telecoms companies)	Provide a digital identity platform	Optus introduces MasterCard's ID service to its nearly six million customers who download the MyOptus app. It provides a secure and portable digital ID that can be used to purchase devices, change accounts and purchase additional services.
		Identification in university examinations	・Postal Service ・Deakin University		Using the Post Office ID application and the Deakin University portal, it is possible to verify the identity of students taking exams online.
		Digital ID assertion in administration	Republic of North Macedonia		The aim is to provide a local digital identity and related trust services that Macedonian citizens can use in a variety of everyday activities. Among the first applications are an e-KYC feature to support the remote opening of new accounts for banks and mobile phone.
Japan	JCB	Identity verification, attribute change procedures, etc.	Fujitsu	Provide knowledge of payment and authentication features and operational schemes such as inter-operator fund settlement.	In October 2019, the companies started to consider the joint development of a platform that enables the assertion and use of user ID information, and new services and business models using the platform.

Source) Created by NRI based on press releases from each company.

3-3. Major SSI/DID Preceding and PoC Projects

3-3-1. Major Cases of Projects Involving Financial Institutions

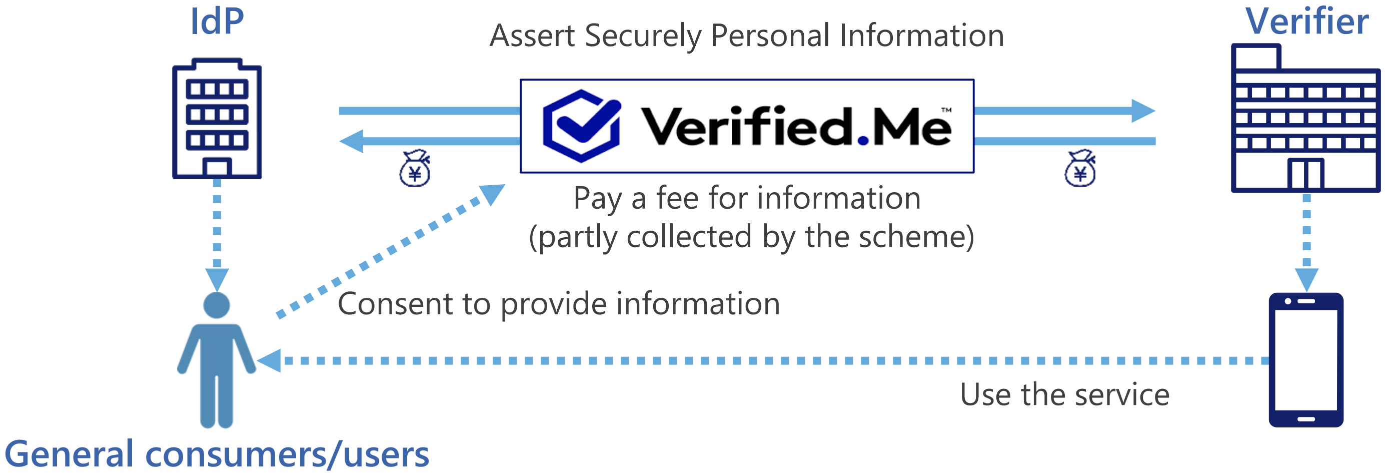
- Of the major initiatives mentioned in the previous section, the following two cases, which were often mentioned as examples of SSI/DID in the financial sector in hearings with experts in Japan and overseas, are described in detail.

Country	Financial Institution	Use Case	Partner	Roles of Financial Institution	Country	Reasons for selection*
Canada	Seven major Canadian banks	Government, life insurance, etc.	SecureKey Technologies	Banks participates as IdPs	Seven major Canadian banks have formed a consortium to launch a service called Verified.me in May 2019, the service that will be available from May 2019. Identity verification information is asserted to life insurance companies.	It is already available as a service and is recognized globally as a leading example of an SSI/DID use case in the financial sector.
Spain	Banco Santander	Application for car rental, insurance and loans, and application to the government	・CaxiaBank, MAPFRE (Insurance company), ・Repsol (fossil fuel company) ・Alastria (Non-profit blockchain consortium)	Joint venture acts as identity platform. The bank itself acts IdP	A secure and reliable identity platform that gives users more control over their personal information, thereby protecting their privacy and providing them with once-only convenience. The system is currently in the trial phase and is due to be released in May 2021.	It is positioned as a leading SSI/DID initiative in the EU.

3-3. Major SSI/DID Preceding and PoC Projects

3-3-2. Canada: Verified.Me

- Verified.Me is a service (live and in production as of May 1, 2019) offered by SecureKey Technologies Inc., in conjunction with a consortium of seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD.
  - Verified.Me is a privacy-respecting digital identity and attribute sharing network. The service simplifies identity verification processes by allowing individuals (subjects) to share identity and attribute information from trusted sources (including financial institutions, mobile operators, credit bureau, and government) to access services.
  - The network is based on permission-based distributed ledgers operated by the consortium. It is built using the IBM Blockchain Platform which is based on Linux Foundation's open source Hyperledger Fabric and is aligning with W3C decentralized identity standards1, to enable interoperability with other networks.
  - The service is free for consumers to use. (downloaded the mobile app through the App Store or Google Play.)

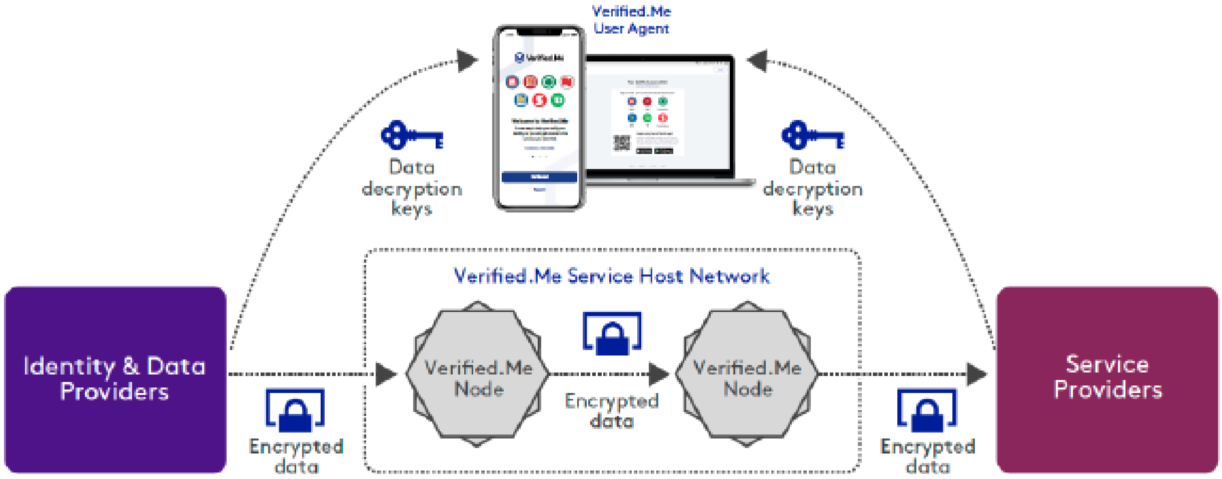

IdP
Assert Securely Personal Information
Verifier
Verified.Me™
¥
¥
Pay a fee for information
(partly collected by the scheme)
Consent to provide information
Use the service
General consumers/users

https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

3-3-2. Canada: Verified.Me

- A basic overview of the service is as follows.

Mechanism of Verified.Me



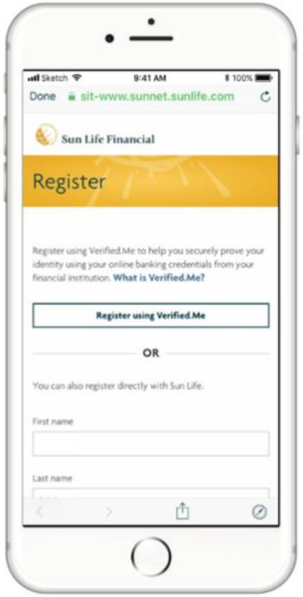
- Identity & Data Providers (IDPs)
  - Eligible organizations in Canada that participate in Verified.Me that generate or hold certain information about the subject. Examples of IDPs include financial institutions, credit bureaus, telecommunications providers and other eligible trusted sources.
- Relying Parties (RPs), or Service Providers
  - These are eligible organizations in Canada that participate in Verified.Me that ask subjects to provide certain information through Verified.Me. Verified.Me helps verify the subject's identity and/or eligibility for product or service offerings.
- Financial Institution Identity & Data Providers (Financial Institutions, or Service Hosts)
  - Seven of Canada's major financial institutions that are responsible for authenticating subjects wishing to access the Verified.Me service, and also for hosting the core components of the Network.
- Verified.Me User Agent
  - The tool provided to the subject to interact with the Verified.Me Network and consent to the sharing of their attributes via the network (via mobile app or web browser).

Source: https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

3-3-2. Canada: Verified.Me

■ Below is an image of the use of the life insurance company (Sun Life Financial) contract in conjunction with the bank (RBC) identification information.

Image of the use of Verified.Me



Done sit-www.sunnet.sunlife.com

Sun Life Financial

Register

Register using Verified.Me to help you securely prove your identity using your online banking credentials from your financial institution. What is Verified.Me?

Register using Verified.Me

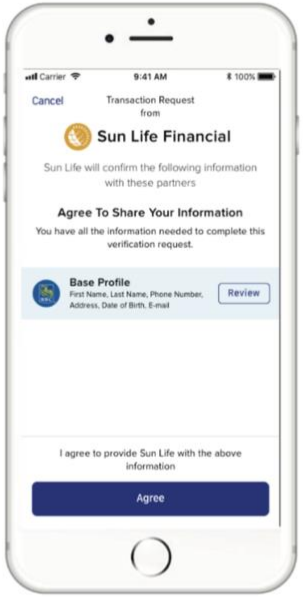
OR

You can also register directly with Sun Life.

First name

Last name

- Select "Register using Verified.Me" from the life insurance company's website



Cancel Transaction Request from

Sun Life Financial

Sun Life will confirm the following information with these partners

Agree To Share Your Information

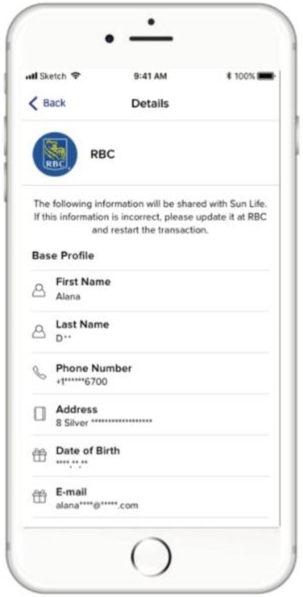
You have all the information needed to complete this verification request.

Base Profile
First Name, Last Name, Phone Number, Address, Date of Birth, E-mail — Review

I agree to provide Sun Life with the above information

Agree

- Select the identity information registered in Verified.Me (in this case RBC)



Back Details

RBC

The following information will be shared with Sun Life. If this information is incorrect, please update it at RBC and restart the transaction.

Base Profile

First Name: Alana

Last Name: D**

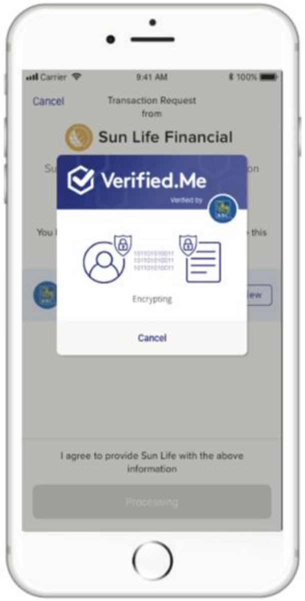
Phone Number: +1******6700

Address: 8 Silver ******************

Date of Birth: ****.**.**

E-mail: alana****@*****.com

- Check the identity information registered in RBC.



Cancel Transaction Request from

Sun Life Financial

Verified.Me

Verified by

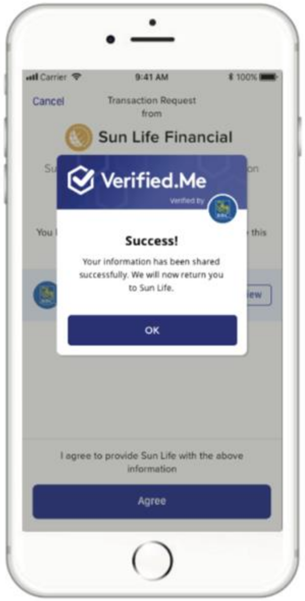
Encrypting

Cancel

I agree to provide Sun Life with the above information

Processing

- Click "Agree" to share the information



Cancel Transaction Request from

Sun Life Financial

Verified.Me

Verified by

Success!

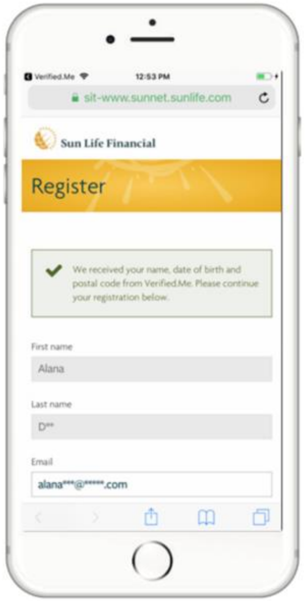
Your information has been shared successfully. We will now return you to Sun Life.

OK

I agree to provide Sun Life with the above information

Agree

- Successful sharing of RBC identity information



sit-www.sunnet.sunlife.com

Sun Life Financial

Register

✓ We received your name, date of birth and postal code from Verified.Me. Please continue your registration below.

First name: Alana

Last name: D**

Email: alana***@*****.com

- The information is shared to the life insurance company and registration is completed.

Source: https://www.iphoneincanada.ca/news/verifiedme-launch-canada/

3-3-2. Canada: Verified.Me

■ The main features of Verified.Me are as follows

【 Background to the creation of the service 】

- In Canada, banks are required to verify the identity of customers in person at the time of account opening, and if KYC information is not updated, the account will be frozen. As a result, the bank's identity verification information is both fresh and accurate, and the bank had the idea to make good use of this KYC information.

【 Features as SSI/DID 】

- This service model is based on SSI but is more stringent than SSI in general. SecureKey calls it "Triple Blind". meaning that none of the three parties involved in the service model (Identity & Data Provider, Service Provider and Network Operator) can see where the information users are sharing to is coming from or where it is being presented. In general, the SSI model is a more robust privacy design in this respect, as the Service Provider has no control over which Identity information is used.

【Use case】

- The main service users (service providers) are limited to government agencies and life insurance companies, but the aim is to become a Nationwide ID infrastructure.

Appendix: Digital Identity in Canada

- In Canada, the Digital Identity & Authentication Council of Canada (DIACC), a group of government and private sector organizations, is working to develop a digital identity and authentication framework.
- The establishment of DIACC was prompted by a report produced in December 2011 by the Payment Systems Review Task Force, set up by the Canadian Department of Finance to review the financial system in the digital age.

Task Force for the Payments System Review
Moving Canada into the Digital Age
DECEMBER 2011

"In order to significantly modernize Canada's payments system, changes are needed in a number of fields, from consumer behavior to accounting solutions to the procedures that governments rely on to deliver services. Industries has not implemented change, in part due to uncertainty and lack of coordination. Therefore, the Government of Canada needs to lead the change by taking the following actions.

- Implement electronic invoicing and payments (EIP) for all government suppliers and benefit recipients
- Partner with the private sector to create a mobile ecosystem
- Propel the build of a digital identification and authentication (DIA) regime to underpin a modernized payments system and protect Canadians' privacy"

➢ Based on the third of the above recommendations, the DIACC was established in 2012 as a non-profit public-private organization as a review body.

Source: https://www.canada.ca/content/dam/fin/migration/n12/data/12-030_1-0_eng.pdf

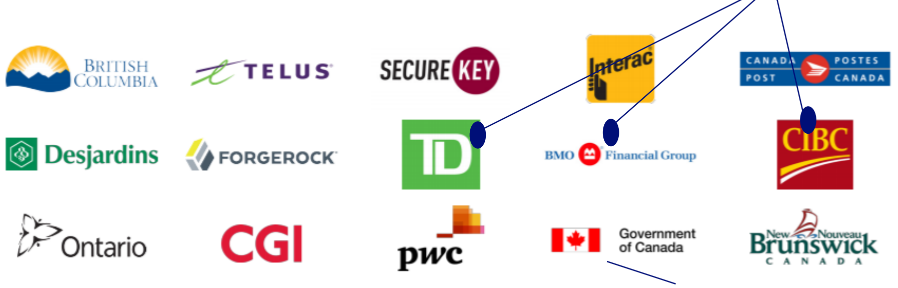
Appendix: DIACC（Digital ID & Authentication Council of Canada）

■ DIACC's members and their main activities are as follows

■ Due to the recommendations of the Ministry of Finance's Task Force, many of the member companies are financial institutions.

DIACC's main members

Major domestic banks participated



The Government participated

DIACC's initiatives in the public and private sectors

Outreach: Gather and share information

- Connect, develop, and strengthen outreach that informs Canadian and global trends.
- Gain early input and view into local and international efforts including GDPR, PSD2, UNCITRAL, and more.
- Provincial members are first to be considered as venues for DIACC and IdentityNORTH events.

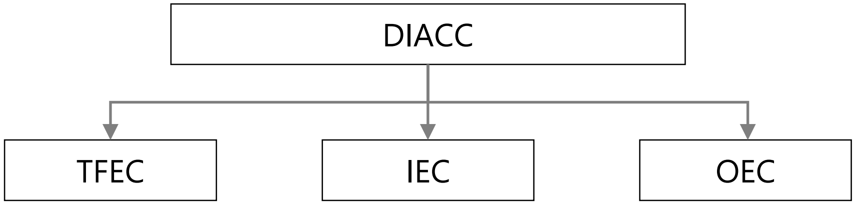
Innovation Plan use cases and conduct PoC

- Connect, share, develop, and strengthen service and product strategies.
- Drive use cases to gain visibility, input, and recognition.
- Test viabilities and accelerate innovation via design challenges, proofs of concepts, applied research, and more.

Interoperability: Interoperability, export best practices

- Connect, influence, and deliver public/private sector collaborative standards, agreements, and programs to secure interoperability.
- Map impactful use cases to evolving standards and practices to secure Canadian digital identity.
- Lead and gain early insights and strategic opportunities for interoperability.
- Share Canadian standards globally and bring best global practises to our community.

Committees in DIACC.



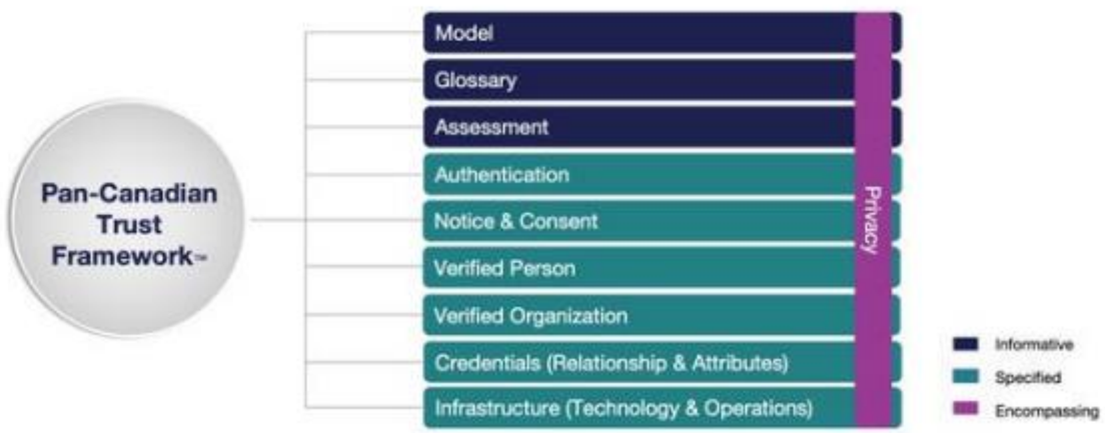
TFEC：Trust Framework Expert Committee
IEC：Innovation Expert Committee
OEC：Outreach Expert Committee

3-2. Major SSI/DID Preceding and PoC Projects

Appendix: Support for PCTF(Pan-Canadian Trust Framework) and SSI/DID

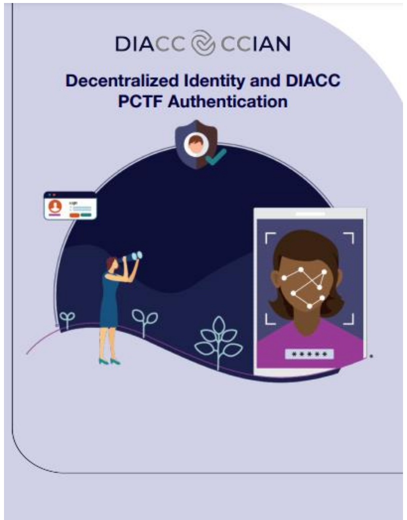
- DIACC developed the PCTF as a governance model for Canadian public and private sector organizations to use digital identities securely and launched PCTF 1.0 alpha in November 2020.
- The PCTF was developed to establish the basic principles and standards required when migrating identity management from existing analogue to digital, and to provide a reference architecture for government agencies and businesses to refer to.
- While it is not legally enforceable and compliance is voluntary, it is attracting attention both in Canada and globally as a trust framework for digital identities.
- It has also published guidelines on how distributed identities can comply with the PCTF in February 2021.

【Components of the PCTF】



Source: https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf

【 Guidelines on DID 】

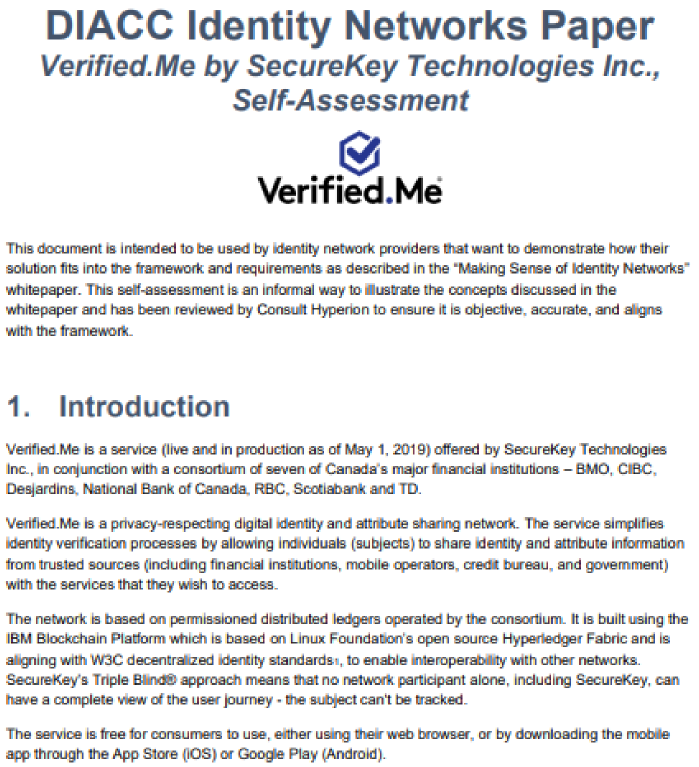

DIACC CCIAN

Decentralized Identity and DIACC PCTF Authentication

Source: https://diacc.ca/wp-content/uploads/2021/02/Decentralized-Identity-and-DIACC-PCTF-Authentication.pdf

Appendix: Self-Assessment of PCTF Compliance Status

- Providers of digital identity services are required to self-assess their compliance with the PCTF and publish the results in order to demonstrate their accountability to users.
- For example, SecureKey has published the following self-assessment results for Verified.Me.



DIACC Identity Networks Paper

Verified.Me by SecureKey Technologies Inc., Self-Assessment

Verified.Me

This document is intended to be used by identity network providers that want to demonstrate how their solution fits into the framework and requirements as described in the "Making Sense of Identity Networks" whitepaper. This self-assessment is an informal way to illustrate the concepts discussed in the whitepaper and has been reviewed by Consult Hyperion to ensure it is objective, accurate, and aligns with the framework.

1. Introduction

Verified.Me is a service (live and in production as of May 1, 2019) offered by SecureKey Technologies Inc., in conjunction with a consortium of seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD.

Verified.Me is a privacy-respecting digital identity and attribute sharing network. The service simplifies identity verification processes by allowing individuals (subjects) to share identity and attribute information from trusted sources (including financial institutions, mobile operators, credit bureau, and government) with the services that they wish to access.

The network is based on permissioned distributed ledgers operated by the consortium. It is built using the IBM Blockchain Platform which is based on Linux Foundation's open source Hyperledger Fabric and is aligning with W3C decentralized identity standards[1], to enable interoperability with other networks. SecureKey's Triple Blind® approach means that no network participant alone, including SecureKey, can have a complete view of the user journey - the subject can't be tracked.

The service is free for consumers to use, either using their web browser, or by downloading the mobile app through the App Store (iOS) or Google Play (Android).

Source: https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

3-3-3. Spain: Alastria_ID/Dalion

- Alastria_ID is the model for digital identity in SSI, and Dalion is the name of a project based on Alastria_ID that is being serviced by Spanish financial institutions.
- Dalion participants' industries:
  - Alastria, banks insurance, stock exchange, energy, and IT service
- Project overview
  - Launched in 2019 PoC begun in 2020, and planned to roll out in May 2021
  - Run on Alastria's Ethereum-Quorum blockchain (as of development)
- Benefit for individual users
  - Self manage own information
  - Improve efficiency of registration (including identity verification)
  - Identity theft prevention
- Benefit for participating organizations
  - Improve efficiency of registration (including identity verification)
  - Fraud prevention
  - Develop new business models and improve user experiences

Dalion Project Participants

(According to the press release by Santander)

ALASTRIA

Banks

Santander

Bankia

Liberbank

CaixaBank

Insurance

linea directa

MAPFRE

Energy

Naturgy

REPSOL

Stock Exchange

BME SPANISH EXCHANGES

IT Service

inetum. Positive digital flow

Source: Santander's press release about Dalion project https://www.santander.com/en/press-room/press-releases/2020/11/ten-spanish-companies-join-forces-to-promote-digital-identity-using-blockchain-technology

3-3-3. Spain: Alastria_ID/Dalion

- The digital identity initiatives related to Spain are as follows.
- DNI (Documento National de Identidad) 3.0 ※1
  - Issued by the Spanish government (National Police Corps) since 2015
  - Electronic chip and NFC are included to be used
    - Contained data: Personal information (such as name), photograph, fingerprint, signature image, electronic certificates to authenticate and sign electronically…etc.
  - Can be used to prove personal identity and digitally sign electronic documents

Sample of DNI 3.0 Card

Source：https://www.dnielectronico.es/PDFs/uso_nfc.pdf

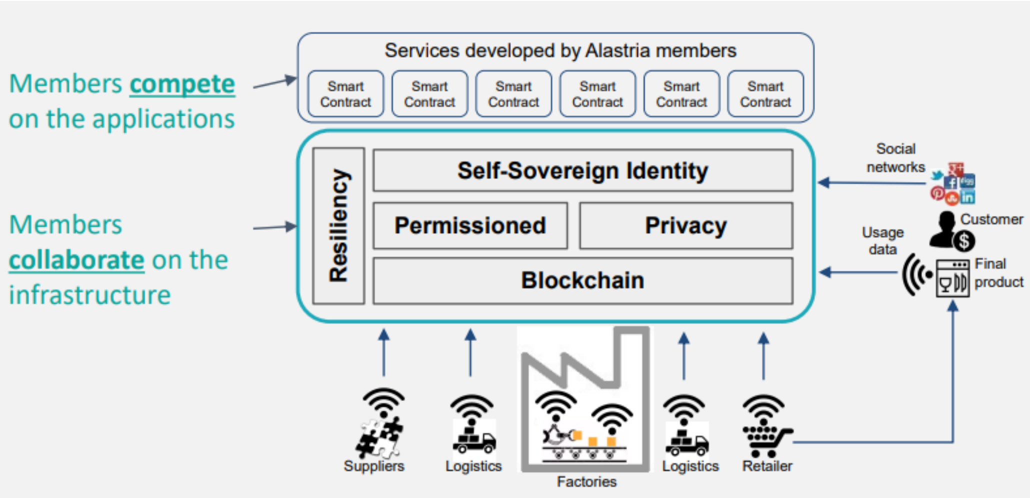
- Alastria_ID
  - SSI digital identity model begun in 2018 by Alastria, a nonprofit association founded in 2017 ※2
    - Alastria participant member is counted to nearly 550, mainly from Spain (some from Italy and Germany). There are companies, including some from financial sector, public sector organizations, universities…etc.
  - Open-source SSI model deployed on blockchain infrastructure operated by Alastira participants※3
  - To provide SSI digital identity infrastructure and development framework with full legal validity in Europe zone ※3
    - Presented to UNE (Spanish Standardisation Association), submitted to CEN/CENELEC, and gave inspiration for ESSIF (European Commission's Self-Sovereign Identity Initiative). ※4
- Dalion ※4
  - Project based on Alastria_ID launched in 2019, PoC begun in 2020, and planned to roll out in May 2021
  - Banks, insurance, and stock exchange are participating. Local public authority and university are observing.
  - To improve the efficiency in processes by enabling reuse of verified identity by other participants

※1 Spain National Police Corps https://www.dnielectronico.es
※2 Alastria https://alastria.io/
※3 Alastria_ID GitHub https://github.com/alastria/alastria-identity/wiki
※4 Press release by Santander about Dalion Project https://www.santander.com/en/press-room/press-releases/2020/11/ten-spanish-companies-join-forces-to-promote-digital-identity-using-blockchain-technology

3-3-3. Spain: Alastria_ID/Dalion

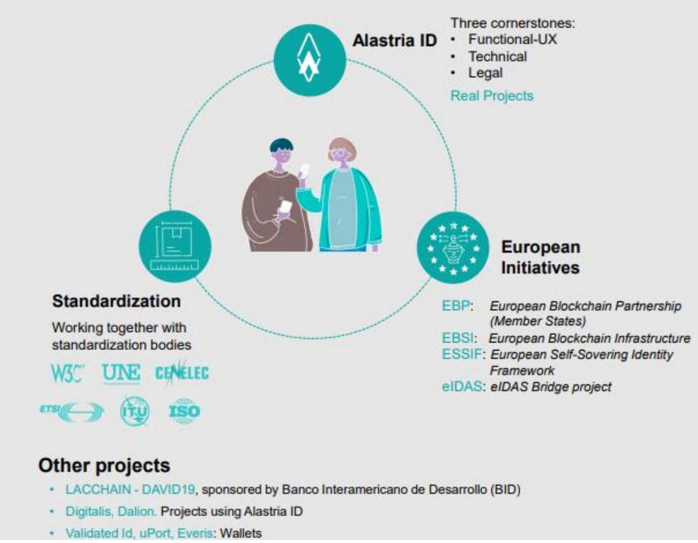
- Alastria_ID is digital identity project of the Alastira's Identity Commission
  - SSI/DID model run on the blockchain operated by Alastria participants
  - To provide SSI digital identity infrastructure and development framework with full legal validity in Europe zone
- Following premises below
  - SSI eIDAS Legal Report by European Council for to enable a framework for make use of SSI with Blockchain
  - e-Identity Workshop Report from EUBOF (EU Blockchain Observatory and Forum)
  - Recommendations described in the report about blockchain and GDPR from EUBOF and European Parliamentary
  - eIDAS Regulation

Alastria_ID roles



Source: "Alastria Digital Identity An ongoing project"
https://portal.r2docuo.com/alastria/document?L3110FC15F

Alastria_ID specifications



Three cornerstones:
- Functional-UX
- Technical
- Legal

Real Projects

Working together with standardization bodies

EBP: European Blockchain Partnership (Member States)
EBSI: European Blockchain Infrastructure
ESSIF: European Self-Sovering Identity Framework
eIDAS: eIDAS Bridge project

Other projects

- LACCHAIN - DAVID19, sponsored by Banco Interamericano de Desarrollo (BID)
- Digitalis, Dalion. Projects using Alastria ID
- Validated Id, uPort, Everis: Wallets

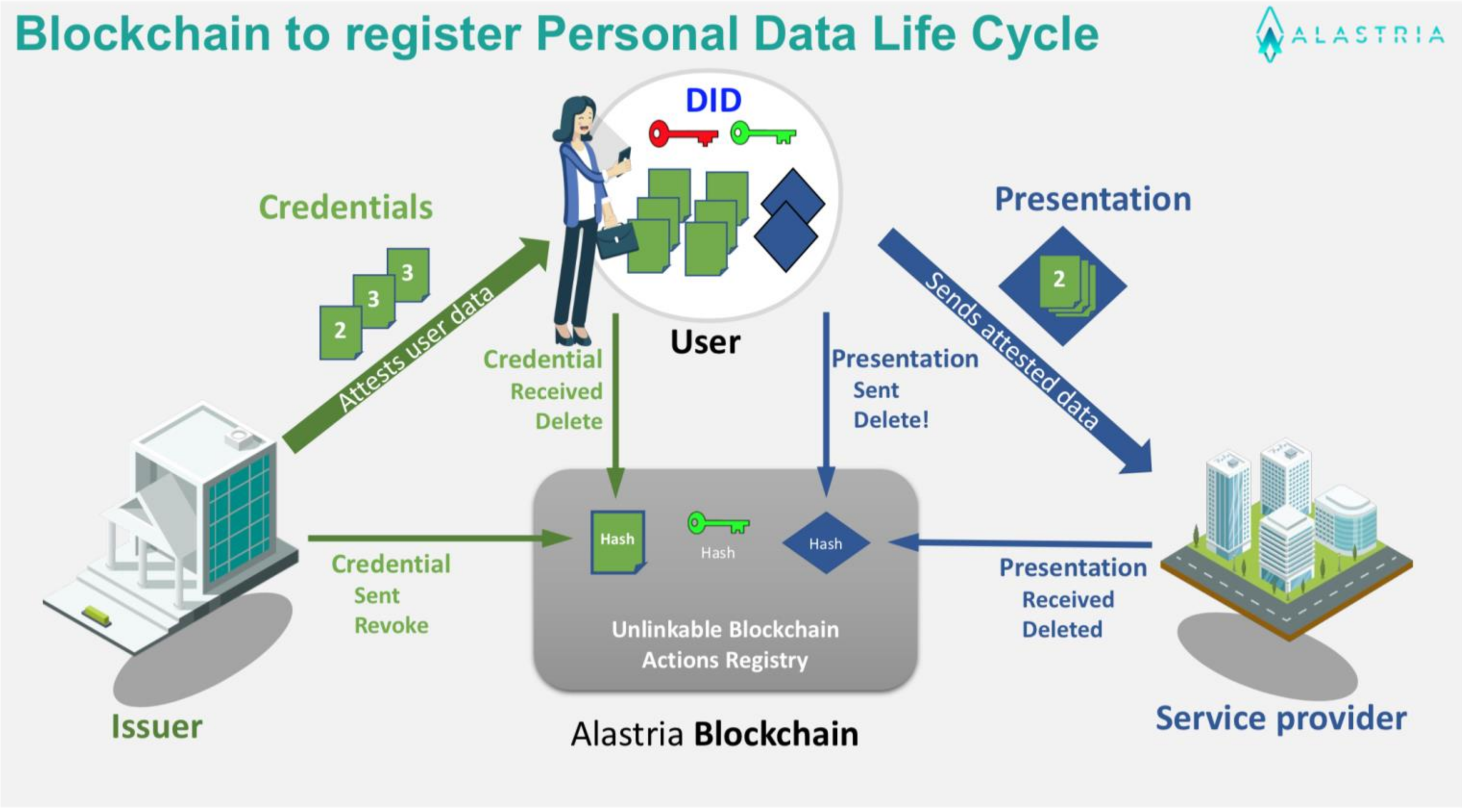
Source: "Alastria ID Compatibility and interoperability"
https://portal.r2docuo.com/alastria/document?L097EBB43D

Source: Alastria_ID GitHub https://github.com/alastria/alastria-identity/wiki

3-3-3. Spain: Alastria_ID/Dalion

- Alastira_ID, similar to general SSI/DID, is divided into roles of credential issuers (Issuers), users (Users), and credential recipients (Service Providers), and operations related to credentials are written to the Alastria blockchain. Operations on the credential are written to the Alastria blockchain, and the authenticity of the credential can be verified using the records on the blockchain.

Alastria_ID usage overview



Source: https://alastria-es.medium.com/la-identidad-digital-de-alastria-presenta-su-primer-mvp-696750d687ac

3-4. Advantages of SSI / DID and Issues toward Realization

3-4. Advantages of SSI / DID and Issues toward Realization

Main Points of this Section

■ The advantages of the SSI model and the issues for the model’s realization are as follows.

- For the advantages, it is possible to achieve self-control and privacy by reducing the dependency on ID providers. In addition, by adopting a topology that links multiple claim providers with the user's wallet as a hub, it is expected to contribute to reducing the onboarding cost of the entire industry.
- For the issues toward realization, it is necessary to overcome new technical, legal, public system, and operational issues arising from the new model, as well as to consider the overhead of new business initiatives and to search for suitable use cases.

Advantages of SSI model

Types	Overview
Self-sovereignty acquisition	• Avoiding lockout restrictions by ID providers • Avoiding tampering with claims after issuance by ID providers
Privacy consideration	• Minimizing processing within existing ID providers • Clear consent management for data assertion, and data minimization, as well as the exercise of the "right to be forgotten" by deleting claims held at will. • Confidentiality of the complainant to the claims provider (enabling compliance with the "need to know" principle)
Improvement of convenience and cost control for the entire industry	• Deployment to multiple relying parties using obtained claims (increased convenience) • Reduction of onboarding costs across the industry by enabling data assertion from multiple claim providers

Issues of SSI model toward realization

Types	Overview
Technical	• Organization and implementation of trust anchors in each layer of SSI/DID • Consideration of interoperability when multiple specifications coexist • Ensuring security implementation for newly developed protocols
Legal/ Public system	• Engagements of governments and policymakers • Data protection systems • Privacy measures
Operational	• Understanding of technology by regulators, lawyers and notaries • Promotion of standardization • Maintenance/development of trust frameworks • Clarification of liability
Business	• Adaptation of current IT/digital systems • Individual adoption/use case considerations

3-4-1. Advantage of Using SSI/DID

Advantages of the SSI Model

- In the SSI model, the following advantages are expected (underlined are the issues in accelerating digitization mentioned in Chapter 2.
- The four characteristics of SSI/DID are essential to obtain each benefit.

Advantages of SSI model

Advantages	Overview	Correspondence with SSI/DID characteristics			
		Separation of Authentication and Attributes	Utilizing and Selectively Presentation of Distributed Attribute Information	Confidentiality of Presentation Destination	Long-term Storage and Usage
Self-sovereignty acquisition	• No lockout of identifiers by malicious IdPs • Become independent of the dynamics of the claim provider by realizing the following／Claims can be retained without being subject to unintended updates (tampering) by the user ✓ Obtaining claims in their own Wallet ✓ Long-term storage of the claim provider's signature verification key (required for claim authenticity verification) in a distributed repository that is tamper-proof and can be maintained in a reliable manner	●	●		●
Privacy consideration	• Minimize processing within existing IdPs (limited to recognition processing) • Utilization as a measure to realize clear consent management and data minimization in data assertion • Utilization as a measure to realize the exercise of the "right to be forgotten" by deleting claims that are retained at will	●	●	●	
Improvement of convenience and cost control for the entire industry	• Enabling the deployment of claims once obtained to multiple service providers (contributing to customer convenience) • Enabling data assertion from multiple claim providers, contributing to lower onboarding costs across the industry	●	●		

3-4-1. Advantage of Using SSI/DID

Advantages of the SSI Model in Preceding Cases

- As for the advantages of the SSI model, the following is considered to be the response status in Canada's Verified.Me, covered in 3-3.

Examples in the preceding case

Advantages	Correspondence with SSI/DID characteristics				Examples in the Preceding Case (Canada Verified.Me) Note: Consideration by NRI based on public information, etc.
	Separation of Authentication And Attributes	Utilizing and Selectively Presentation of Distributed Attribute Information	Confidentiality of Presentation Destination	Long-term Storage and Usage	
Self-sovereignty acquisition	●	●		●	• For the separation of authentication and attributes, the attributes stored in the user agent are under the control of the user, and are outside the control of the CP. • For utilizing and selectively presentation of distributed attribute information, the user agent has been implemented to enable selective presentation, the user agent has been implemented to enable selective presentation. • For long-term storage and usage, the details are unknown, including whether or not it will be implemented. As for other cases with this characteristic, for example, in the use case of "online ID card" that Keio University is working on with JCB and others, "permanently verifiable attribute provision infrastructure" is positioned as one of the characteristics.
Privacy consideration	●	●	●		• For the separation of authentication and attributes, a feature has been implemented to minimize the processing within the existing IdP (limited to authentication processing). • For utilizing and selectively presentation of distributed attribute information, a user agent has been implemented to enable selective presentation, and processing based on user consent has been realized. • For confidentiality of presentation destination, a feature has been implemented to realize anonymous processing so that the RP does not know from which IdP the attributes were obtained.
Improvement of convenience and cost control for the entire industry	●	●			• For the separation of authentication and attributes, the obtained claims are stored in the user agent, and the implementation is capable of claim deployment to multiple RPs. • For utilizing and selectively presentation of distributed attribute information, the cost of identity verification at the RP side can be greatly reduced by enabling data assertion from multiple CPs.

Technical Issues

■ Technical issues in the layers that constitute SSI/DID

- This section summarizes the issues in terms of trust, interoperability, and security at each layer that constitutes DID.

Technical issues in SSI model by layer

*Also involved in the reliability of the wallet application

Layer		Trust Anchor	Interoperability			Security	
Claim Presentation Layer		Ensuring Validation/Verification/Transparency	Unifying Data Format Common Schema	Interoperability between Models and Methods, Consideration for Scalability	Verification of Protocol Certification Conformance to Standards (Certificate, Conformance Test)	Cryptographic Agility	Formally Provable
Claim Issuance Layer							
Wallet Layer	Local Storage	Reliability of Wallet Applications Credential Management					
	WebApp						
	Cloud						
Transport/ Communication Layer		Ensuring trust in DID Cryptographic Private keys*					
Discovery Layer		Universal Resolver's Traceability, Transparency, and Trust Anchor Guarantee					
Utility Layer		Authority Model of the identity Generation Schema					

(Reference) Target specifications for technical issues accompanied by the realization method

- Each standardization organization has a different method for implementing each layer. It is necessary to consider countermeasures for technical issues in terms of both issues in utilizing and developing existing methods and issues in considering new methods.
- The implementation methods are not limited to the following combinations, and each standardization organization is also discussing stack recombination (e.g., OIDF/DIF liaison agreement described in Section 3-2).

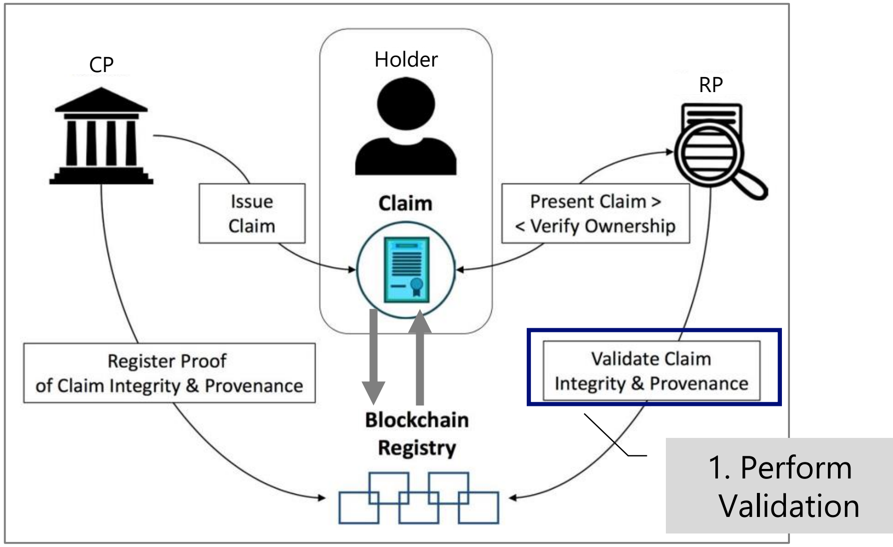
Layer		Model			
		OIDC	DID/VC		
Claim Presentation Layer		OpenID Connect	OpenID Connect	Presntation Exchange VP Requeset Spec	Aries : Present Proof Protocol 1.0
		JWT Also supported as JSON-LD and ZKP format methods)	VC Data Model (VC / VP / ZKP)	VC Data Model (VC / VP / ZKP)	
Claim Issuance Layer		OIDC4IDA Claims Aggregation			Aries：Issue Credential Protocol 2.0
Wallet Layer	Local Storage	Depends on vendor implementation	Depends on vendor implementation	Confidential Storage	Depends on ndor implementation
	WebApp			Depends on vendor implementation	
Transport/ Communication Layer		REST http(s) OIDC SIOP	REST http(s) OIDC SIOP	DID Comm/ CHAPI	Aries : DID Exchange Protocol 1.0
				NFC/BLE/QR/http(s)	
Discovery Layer		OIDC Discovery WebFinger .well-known	OIDC Discovery WebFinger .well-known	DID Resolution	
Utility Layer		DNS/Domain	DNS/Domain	DIDs	

Validation/verification/transparency for claims

- It is important for SSI/DID to ensure that claims are: 1. validation to ensure that they are valid (not revoked), 2. verification to ensure not tampering, and 3. transparency to ensure a compliant trust framework when generated. Possible realization methods are:
  1. to deploy claim expiration information on a distributed repository such as a blockchain, and refer to it on the RP side. On the other hand, it is necessary to consider the implementation of a method with immutable characteristics, such as blockchain, to deal with the enlargement of the size of the CRL*, which excludes expired information.
  2. the CP to sign the claim and the RP to verify the signature.
  3. to use a transparent specification such as the "OpenID Connect for Identity Assurance" protocol, in which the claim itself describes the legal requirements, trust framework, commercial agreements, etc. that the CP complied with at the time of generation, and the RP can verify the content.

*) CRL: Certificate Revocation List (RFC5280)

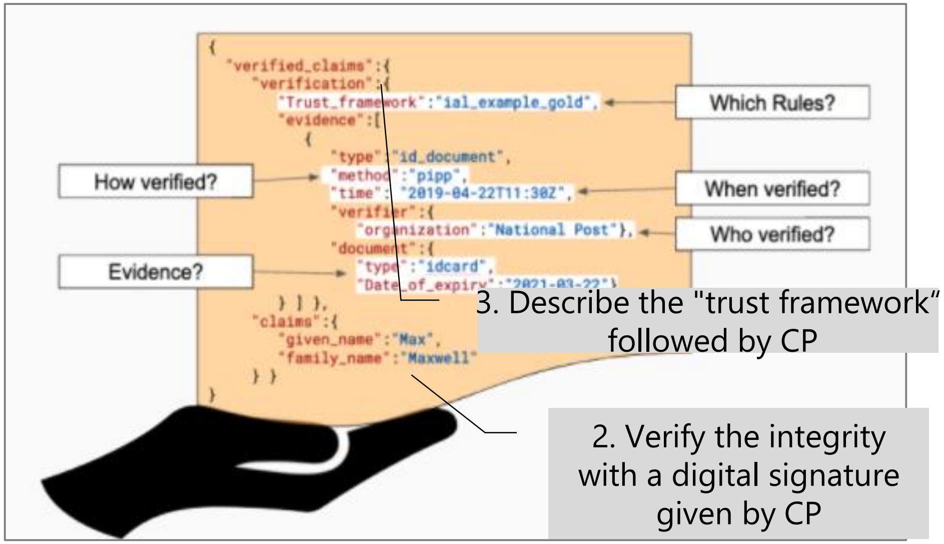
Perform validation to distributed repositories


CP
Holder
RP
Issue Claim
Claim
Present Claim >
< Verify Ownership
Register Proof of Claim Integrity & Provenance
Validate Claim Integrity & Provenance
Blockchain Registry

1. Perform Validation

Source) decentralized-id.com

Verify claims and ensuring transparency using OIDC4IDA



```
{
  "verified_claims":{
    "verification":{
      "Trust_framework":"ial_example_gold",
      "evidence":[
        {
          "type":"id_document",
          "method":"pipp",
          "time": "2019-04-22T11:30Z",
          "verifier":{
            "organization":"National Post"},
          "document":{
            "type":"idcard",
            "Date_of_expiry":"2021-03-22"}
      } ] },
    "claims":{
      "given_name":"Max",
      "family_name":"Maxwell"
  } }
}
```

3. Describe the "trust framework“ followed by CP

2. Verify the integrity with a digital signature given by CP

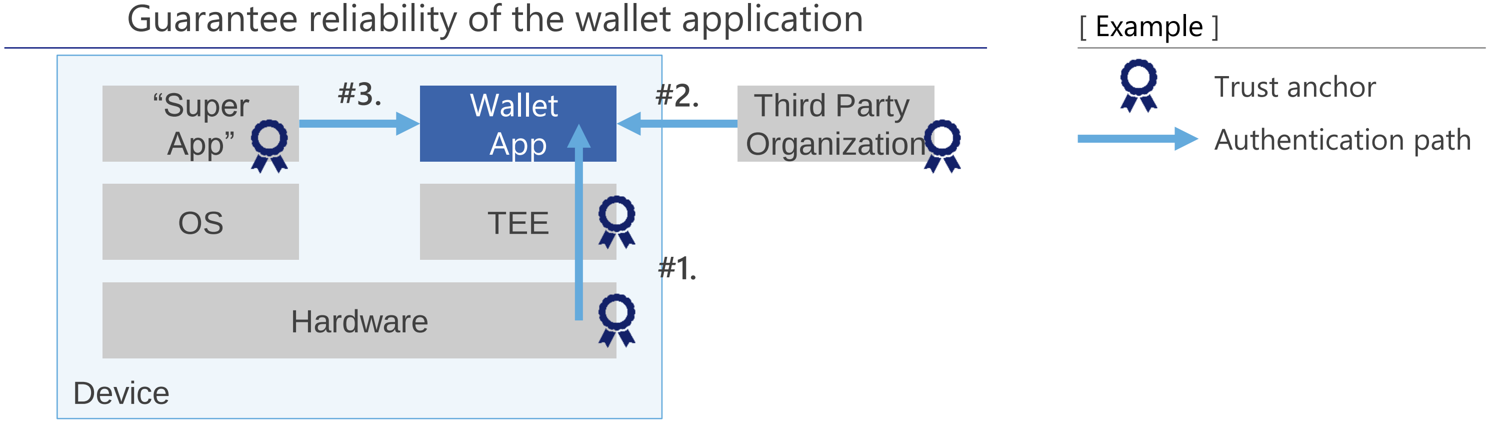
Source) OpenID Foundation “eKYC & Identity Assurance WG”

3-4-2. Issues of SSI/DID - (1) Technical Issues

Guarantee Reliability of the Wallet Application

- In order to ensure (guarantee) the reliability of the application, it is necessary to secure the trust chain from one of the trust anchors. For example, the following are possible trust anchor options.
- In view of providing the system as an ecosystem, it is preferable to 1) secure the chain from lower layers. On the other hand, to realize this specification, the cooperation of platformers such as hardware and OS vendors will be essential.

Guarantee reliability of the wallet application



#	Method	Overview	Issue
1.	Building validation path chains from lower layers in devices	Perform signature and signature verification and validation on processing results using signature keys stored in secure elements such as OS/TEE to build trust from lower layers.	• Dependence on specific models/products • Difficulties in ensuring portability • Cooperation from HW/OS vendors is required
2.	Evaluation through a third-party evaluation program	Third party organizations verify apps, such as the App Store for iOS and Google Play Store for Android.	• Dependence on third-party verification programs • Able to bypass by obtain from another channel • Exclusion of Wallet apps at the behest of third parties
3.	Launch from "super app" (Deeplink, etc.)	Call the wallet as a mini-app from a trusted "super app".	• Pre-installation of the "super app" is required (in the case of post-installation, the same consideration as for Method 2 is required)

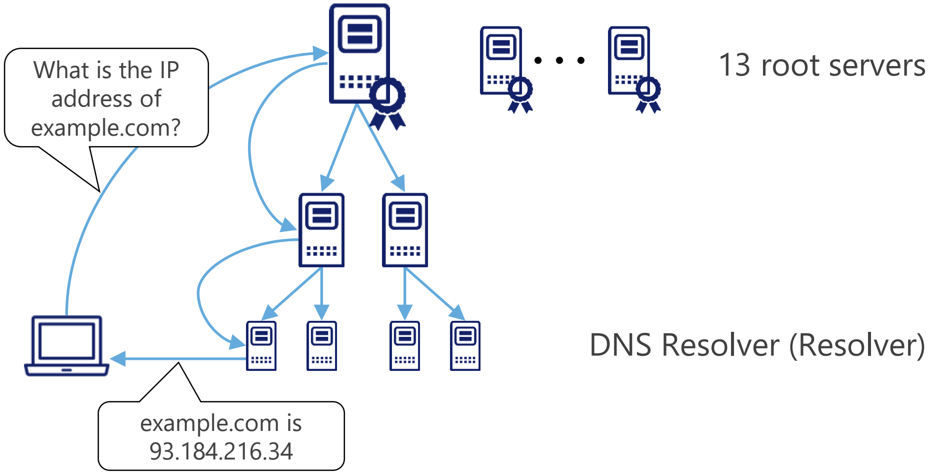
Source) Created by NRI based on https://www.jnsa.org/seminar/pki-day/2021/data/0415okuda.pdf

3-4-2. Issues of SSI/DID - (1) Technical Issues

Universal Resolver’s Trackability, Transparency, and Guarantee Trust Anchor

- It could be an issue to guarantee the trust anchor of SSI/DID's Universal Resolver and to ensure traceability and transparency.
  - Discussion could occur on how to guarantee trust anchors in Resolver similar to DNS resolution from DNS root servers.
    - Consideration must be given to maintaining availability and ensuring reliability as an ecosystem.
    - Similar operational and management requirements to those of ICANN, such as management at the time of domain acquisition, are expected.

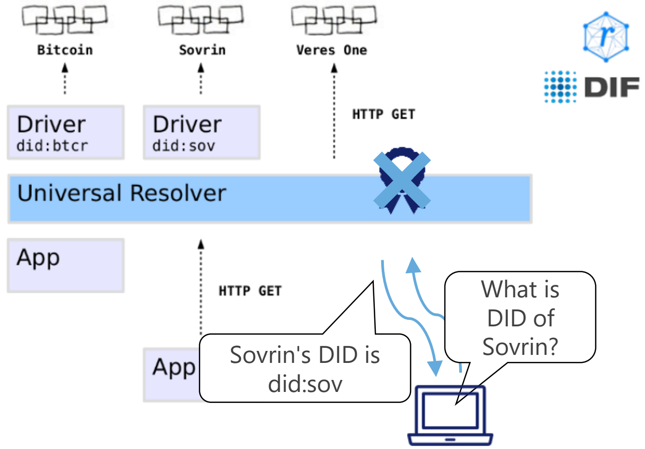
DNS resolution (Resolve) overview


What is the IP address of example.com?
13 root servers
DNS Resolver (Resolver)
example.com is 93.184.216.34

The root server acts as a trust anchor for the lower DNS resolvers (Resolver)

Source) Created by NRI

Universal Resolver overview



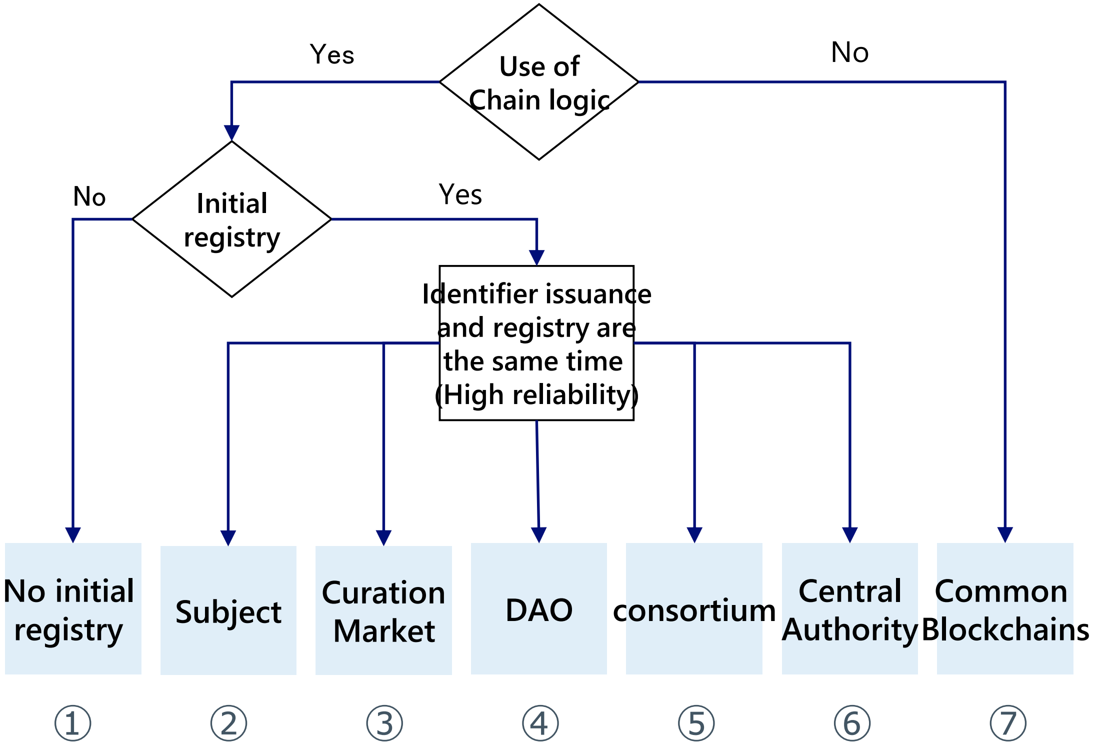
Universal Resolver needs to act as a trust anchor

Source) https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

Schema Authority Model in Identifier Generation

- A subjective consensus between the Authority Model and the SSI philosophy may occur.
  - At the time of identity generation by existing IdPs, there are multiple Authority Models.
  - Even in the case of self-sovereignty in SSI/DID, it may be necessary to consider how much authority and control should be given to the registry.

Registry model for identifier



#	Category	Characteristics
①	No initial registry	Register identifiers in the ledger only under certain circumstances
②	Subject	Self-registration, with the registry managed by the Subject, the entity that receives credentials issued by the Issuer
③	Curation market	③ through⑤ may vary depending on the degree of control participants have over the implementation of permits. • Curation market: Participants vote on registry decisions • DAO: Self-sustainable organizational structure in which no single entity manages a chain of registries and logic • Consortium: Entities other than governments, companies, and individuals (themselves) are responsible for registry decisions
④	DAO (Decentralized Autonomous Organization)	
⑤	Consortium	
⑥	Central Authority	A single or combined entity manages the registry.
⑦	Common Blockchain (no chain logic))	Identity registration using a common blockchain without chain logic (e.g. smart contracts)

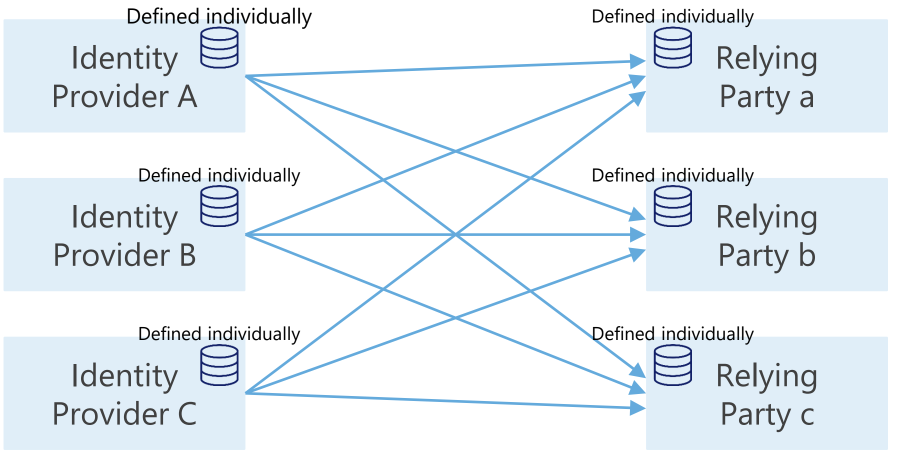
Source) NIST "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems"

3-4-2. Issues of SSI/DID - (1) Technical Issues

Standardization and Unification of Formats, Schemas, Properties, etc.

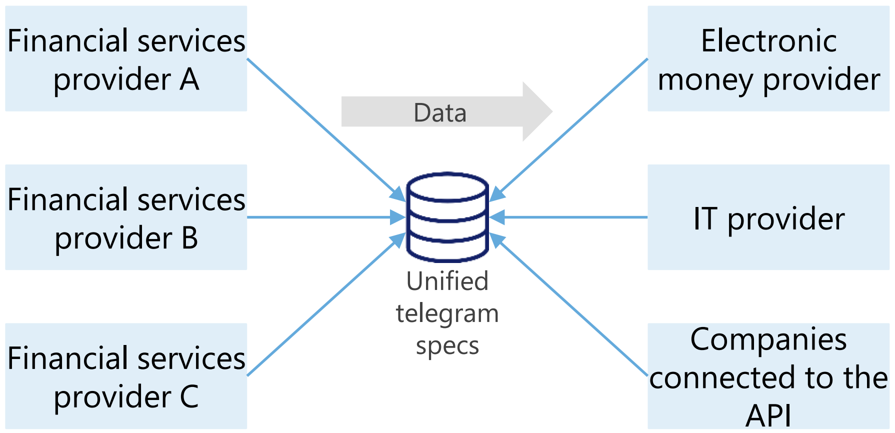
- If there is no unification of formats, schemas, properties, etc., development will become inefficient due to the need to refer to individual schemas and implement unique parsing processes when assertion data. Therefore, it is preferable to make specifications as common and unified as possible.
  - For commonization and unification, it is necessary to discuss the scope of formulation taking into account the boundary between the scope of formulation as a standard technical specification and the scope defined by related organizations according to the use cases such as industries and sectors.
- OpenID Connect, financial APIs, etc. share a common format and schema, making it easier to pass data.
  - The JWT (JSON Web Token), which is widely used in the exchange of claims in OpenID Connect, has been formulated as RFC7519 and defines the format of various data and handling methods for identity information as a schema to maintain interoperability.
  - In Japan, the "Telegram Specification Standard for Open APIs in the Electronic Money Field" was formulated to promote the use of data by connected businesses.

Data assertion with individual formats, schemas, etc. defined



Different schemas, formats, properties, parameters, etc. make development for data exchange inefficient (separate development occurs)

Data assertion with unified format and schema defined


Financial services provider A
Financial services provider B
Financial services provider C
Data
Unified telegram specs
Electronic money provider
IT provider
Companies connected to the API

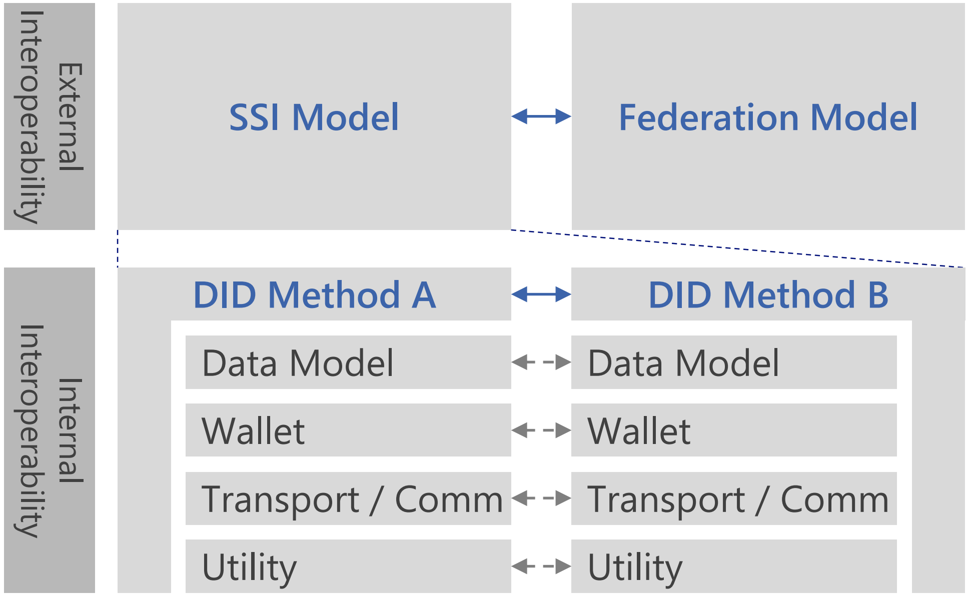
Standardize specifications for data exchange by unifying telegram specifications

Source) Created by NRI

Considerations for Interoperability and Scalability between Models and Methods

- In claim assertion, it is necessary to ensure interoperability between different models, and even between different methods in SSI models, taking into account the different methods..
  - If interoperability of the federation model SSI/DID is to be considered at the interface of existing operators, supporting SSI/DID may be an additional investment.
  - In SSI/DID, each DID method has its own DID scheme, and methods for generating, resolving, updating, and invalidating DIDs and DID documents, and if the schemes and methods are different, the assertion process becomes difficult.
- To have compatibility between the SSI model and the federation model, it is necessary to consider the conversion process such as switching by modules with Gateway features. On the other hand, many specifications are being formulated for the SSI model, and depending on the number of methods to be supported, the cost of developing switching features and operating costs may be enormous.

Examples of targets for consideration for overall operability



External Interoperability

SSI Model ↔ Federation Model

Internal Interoperability

DID Method A ↔ DID Method B

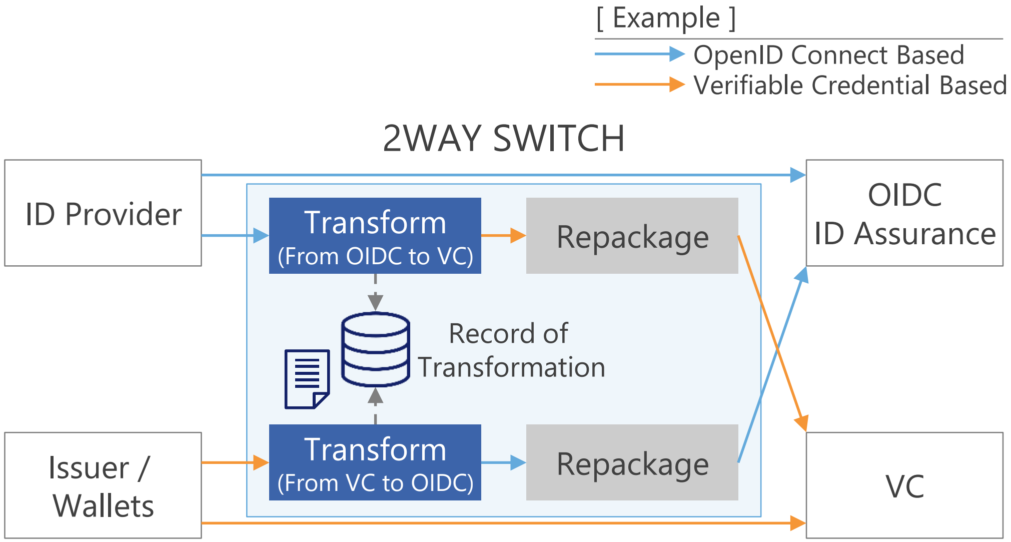
Data Model ↔ Data Model

Wallet ↔ Wallet

Transport / Comm ↔ Transport / Comm

Utility ↔ Utility

Example image of model switching



[Example]

OpenID Connect Based

Verifiable Credential Based

2WAY SWITCH

ID Provider

Issuer / Wallets

Transform (From OIDC to VC)

Repackage

Record of Transformation

Transform (From VC to OIDC)

Repackage

OIDC ID Assurance

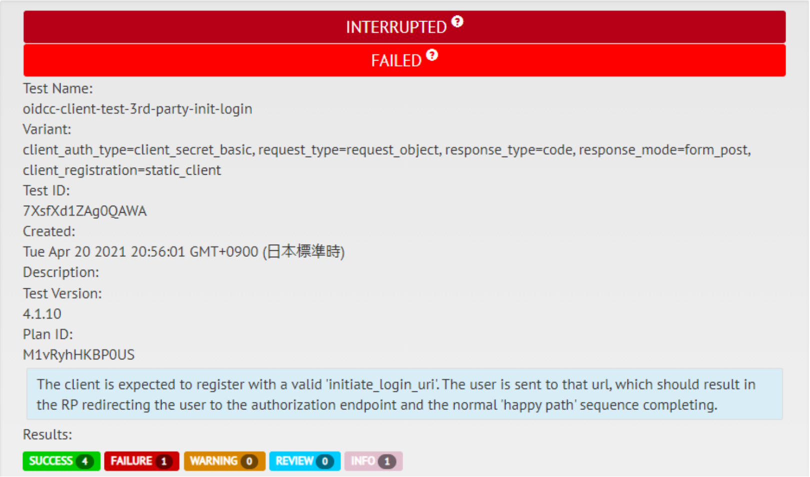
VC

Source) Created by NRI based on OIX Quarterly Workshop - 15th Dec 2020

DID Certification and Standards Compliance

- As with initiatives in existing standard technologies, it is recommended to consider the provision of certification systems and standard conformance tests that provide transparency and reduce the implementation burden, such as interoperability and specification fulfillment, as measures to promote standardization.
  - Examples of standard certification and confirmation standard conformance
    - The FIDO UAF, U2F and FIDO2 described in Chapter 1 are provided with a certification program by the FIDO Alliance for conformance, interoperability and security features. As part of the certification program, a test tool for self-assessment is provided to confirm that the implementation complies with the specifications. The certification program ensures interoperability, for example, a FIDO2 certified server can use any FIDO2 authenticator manufactured and certified by a different vendor.
    - As for OpenID Connect and FAPI (Financial-grade API), which have been developed by the OpenID Foundation, standards conformance tests are provided and certification programs are conducted in order to ensure interoperability in implementations. In the conformance testing, the operation of HTTP requests and responses, server settings, and keys are checked against the specifications.

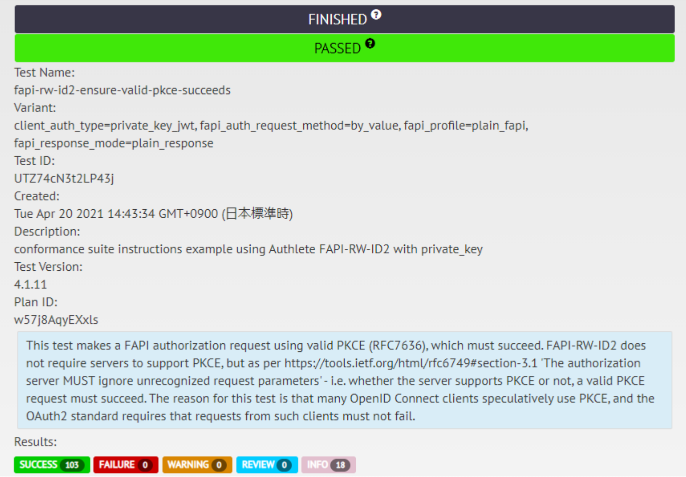
Standards conformance test images provided by the OpenID Foundation



INTERRUPTED
FAILED
Test Name:
oidcc-client-test-3rd-party-init-login
Variant:
client_auth_type=client_secret_basic, request_type=request_object, response_type=code, response_mode=form_post, client_registration=static_client
Test ID:
7XsfXd1ZAg0QAWA
Created:
Tue Apr 20 2021 20:56:01 GMT+0900 (日本標準時)
Description:
Test Version:
4.1.10
Plan ID:
M1vRyhHKBP0US

The client is expected to register with a valid 'initiate_login_uri'. The user is sent to that url, which should result in the RP redirecting the user to the authorization endpoint and the normal 'happy path' sequence completing.

Results:
SUCCESS 4 FAILURE 1 WARNING 0 REVIEW 0 INFO 1



FINISHED
PASSED
Test Name:
fapi-rw-id2-ensure-valid-pkce-succeeds
Variant:
client_auth_type=private_key_jwt, fapi_auth_request_method=by_value, fapi_profile=plain_fapi, fapi_response_mode=plain_response
Test ID:
UTZ74cN3t2LP43j
Created:
Tue Apr 20 2021 14:43:34 GMT+0900 (日本標準時)
Description:
conformance suite instructions example using Authlete FAPI-RW-ID2 with private_key
Test Version:
4.1.11
Plan ID:
w57j8AqyEXxls

This test makes a FAPI authorization request using valid PKCE (RFC7636), which must succeed. FAPI-RW-ID2 does not require servers to support PKCE, but as per https://tools.ietf.org/html/rfc6749#section-3.1 'The authorization server MUST ignore unrecognized request parameters' - i.e. whether the server supports PKCE or not, a valid PKCE request must succeed. The reason for this test is that many OpenID Connect clients speculatively use PKCE, and the OAuth2 standard requires that requests from such clients must not fail.

Results:
SUCCESS 103 FAILURE 0 WARNING 0 REVIEW 0 INFO 18

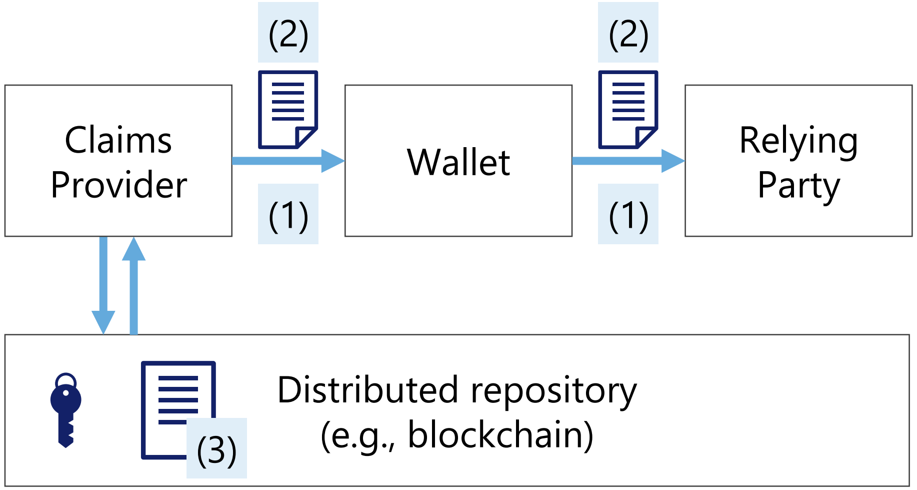
Source) OpenID Foundation “OpenID Foundation conformance suite” https://www.certification.openid.net/

3-4-2. Issues of SSI/DID - (1) Technical Issues

Considerations for Cryptographic Agility

- ■ In general, the risk of algorithm compromise increases over time. Therefore, in the use case of long-term claim usage, it is necessary to consider the possibility of algorithm compromise and to migrate to a secure algorithm.
- ■ In order to realize the " Long-term Storage and Use of Digital Identity" described in section 3-1-2, a mechanism that takes into account the situation where there is no claim provider is necessary.

Consideration targets for Cryptographic Agility



(1) Communication route
    (oncoming authentication and route encryption)
(2) Claims
(3) Information for claim verification
    (eg, DID, DID Doc, etc.)

- ● Based on the process flow described in Section 3-2, it is necessary to consider the compromise of the algorithms used in at least three areas: (1) oncoming authentication and route encryption, (2) claims, and (3) information necessary for claim verification.
  - ● (1) is a dynamic request-based process, and the parties' responses (e.g., switching to a new cryptographic algorithm) need to be organized under the assumption that there is a claim provider/holder/relinquishing party who is the main party to handle the transition.
  - ● On the other hand, (2) and (3) also cover information that was generated in the past. It is necessary to take into account the possibility that the claim provider, which is one of the entities responsible for responding to a compromise, may no longer exist.
    - ●For example, in (3), a method is proposed for public blockchains that can cope with the compromise of a hash algorithm without the presence of a trusted third party (by generating a new block with a new algorithm and extending the validity of the block generated in the past using the compromised algorithm).

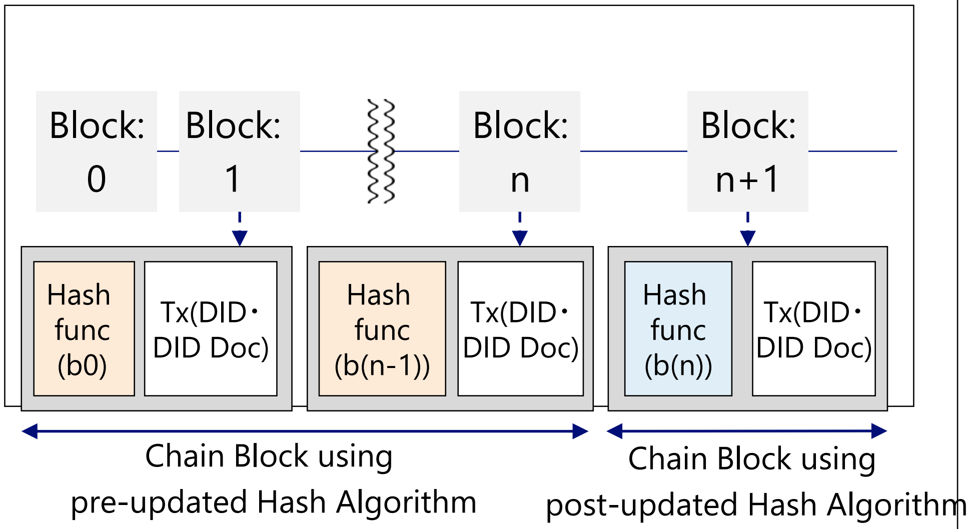
*) Long-term public blockchain: Resilience against Compromise of Underlying Cryptography – Masashi Sato, Shin'ichiro Matsuo

3-4-2. Issues of SSI/DID - (1) Technical Issues

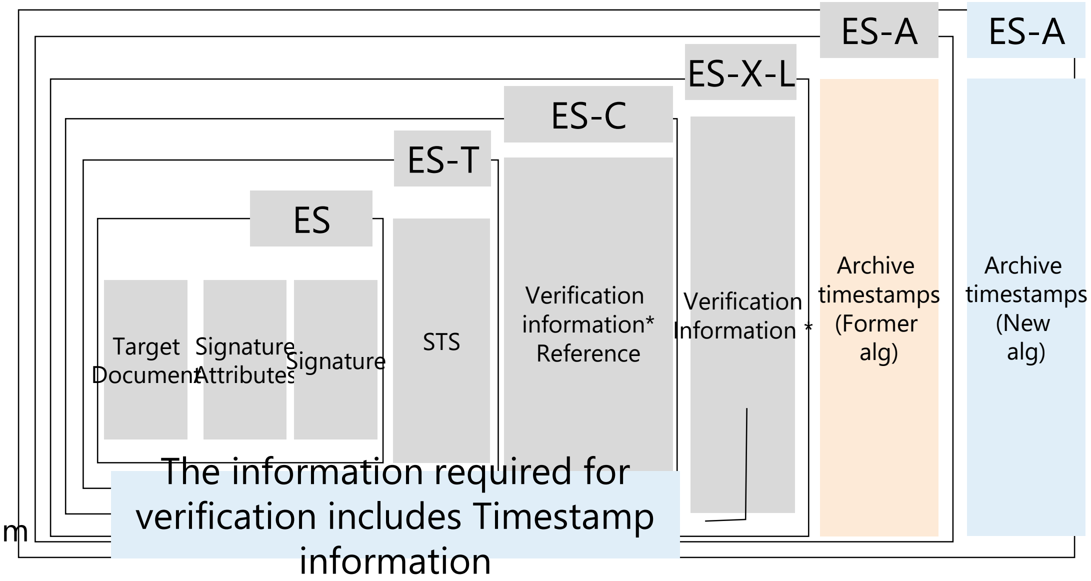
(Reference) Migration Method when Hash Algorithm is Compromised (Blockchain Method, Long-term Signature Method)

- When using a blockchain, even if a hash algorithm is compromised, it is possible to generate a block using a new hash algorithm (Hash(n)) to prove the authenticity of the past block in a form that includes the authenticity of the previous block.
- When DID is realized, it is expected to be implemented not only in blockchains but also in distributed repositories using long-term signature schemes. In the scheme, a method of re-archiving using a new hash algorithm is specified. On the other hand, it should be noted that this method requires accurate time information in light of the expiration date of the public key certificate and the issuance time of the revocation information list (CRL).

Algorithm migration methods in blockchain



Long-term signature scheme (example of cades)


ES-A
ES-A
ES-X-L
ES-C
ES-T
ES
Target Document
Signature Attributes
Signature
STS
Verification information* Reference
Verification Information *
Archive timestamps (Former alg)
Archive timestamps (New alg)
The information required for verification includes Timestamp information

Source)
Left: Created by NRIS based on Long-term public blockchain: Resilience against Compromise of Underlying Cryptography – Masashi Sato, Shin'ichiro Matsuo
Right: Created by NRIS based on 'RFC5126 - CMS Advanced Electronic Signatures (CAdES)'

3-4-2. Issues of SSI/DID - (1) Technical Issues

Guarantee Security by Formal Verification

- Protocol specification is a very complex task, and it is expected to be supported by vulnerability detection methods using mathematical proofs. Formal Verification is a method for detecting vulnerabilities in various possible attack scenarios within a given threat model, and has been used in various scenarios such as ISO/IEC9798 vulnerability detection and Finaicial-Grade API evaluation. It has been used in various scenarios such as ISO/IEC9798 vulnerability detection and Finaicial-Grade API evaluation.
- Related protocols of SSI/DID, which are currently under specification, are also expected to be applied and verified in the future.

Example of formal verification conformance and detection threats to ISO/IEC 9798

Target for verification ISO/IEC 9798 Series

- ISO/IEC 9798-1:2010
- ISO/IEC 9798-2:2008
- ISO/IEC 9798-3:1998
- ISO/IEC 9798-4:1999
- ISO/IEC 9798-2:2008/Cor 1:2010
- ISO/IEC 9798-3:1998/Cor 1:2009
- ISO/IEC 9798-3:1998/Amd 1:2010
- ISO/IEC 9798-4:1999/Cor 1:2009

Thread Model to be considered as mentioned in ISO/IEC 9798

1. Man-in-the-middle attacks
2. Replay attacks
3. Reflection attacks
4. Forced delay attacks

Adapt formal verification

Threats detected

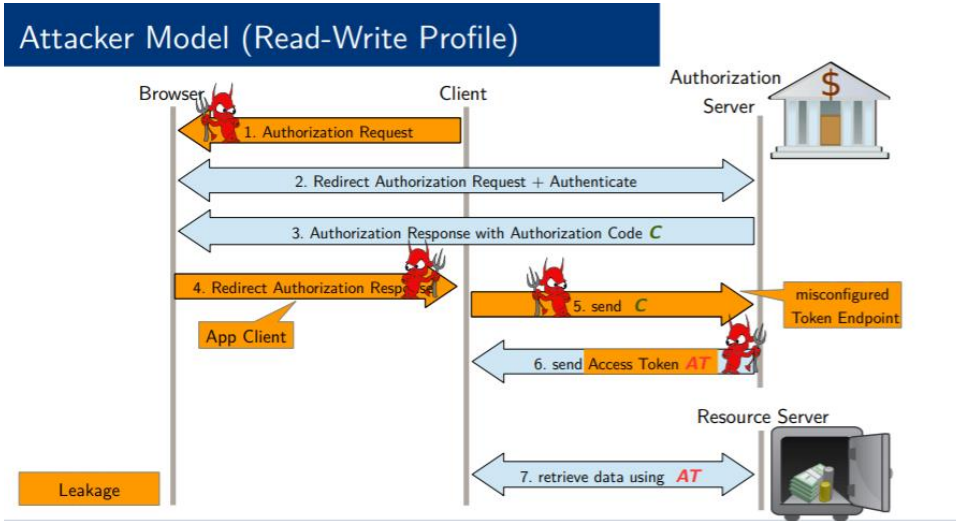
1. Role-mixup attacks
2. Type flaw attacks
3. Reflection attacks

Fix

1. Tagging
2. Removing ambiguity of optional fields
3. Explicitly stating assumptions on Spec

- Verified against the ISO/IEC 9798 series based on the Thread Model mentioned in the specification.
- The concerns of Role-mixup attacks, Type flaw attacks, and Reflection attacks are extracted. In addition, fixes are proposed to solve the problem, such as tagging the protected object to be encrypted, disambiguation of Option Field, and clarification of preconditions.

Overview of formal verification and examples of verification in FAPI


Attacker Model (Read-Write Profile)
Browser
Client
Authorization Server
1. Authorization Request
2. Redirect Authorization Request + Authenticate
3. Authorization Response with Authorization Code C
4. Redirect Authorization Response
5. send C
misconfigured Token Endpoint
App Client
6. send Access Token AT
Resource Server
7. retrieve data using AT
Leakage

- After defining the model to be verified, the Attacker model was defined and verified.
- Formal methods were deployed for both Read and Read-Write profiles.
- The Attacker model is defined as Authorization Request/Authorization Response leakage for Read and Token Endpoint Control/AT leakage by Attacker for Read-Write.

Source:
Evaluation of ISO/IEC 9798 Protocols Version 2.0 David Basin and Cas Cremers April 7, 2011
Formal Security Analysis of the OpenID Financial-grade API - Daniel Fett, Pedram Hosseyni, Ralf Küsters 2019-03-20

3-4-2. Issues of SSI/DID - (2) Non-Technical Issues

Non-Technical Issues of SSI/DID (1/2)

■ The following are possible non-technical issues for SSI/DID

Category	Perspective	Overview
Legal and public system	Engaging government and policymakers	• Public system issues need to be responded to in order to make the technical and legal framework for providing national ID documents that are supported for SSI. • For example, regulation of electronic signatures and electronic transactions that are supported for SSI/DID, and positioning them as certifications to be verifiable for electronic documents, etc.
	Data Protection	• There is a need to review and, if necessary, revise the existing system for data protection regulations to protect the data, rights, and privacy of those who promote and direct SSI. For example, consider the right to protect private keys for wallet operations. • When distributed ledgers or blockchain networks are used for SSI/DID, there is a risk that personal/confidential data may be registered in the distributed ledger. A review of regulations and the establishment of operational guidelines, etc. for their use will be required as necessary.
Operational	Trust Framework	• It is necessary to develop national and regional public and private frameworks to establish certification of qualified IdPs, such as the European Union's eIDAS.
	Liability	• In the SSI model, the user who controls the wallet acts as the IdP, and the user itself is required to fulfill the responsibilities that should be fulfilled by the government, company, or organization in the past. Therefore, it is important to provide support to the user, but it is unclear who will be responsible, how they will be responsible, the boundaries of responsibility, and how they will be handled in case of emergency.

3-4-2. Issues of SSI/DID - (2) Non-Technical Issues

Non-Technical Issues of SSI/DID (2/2)

■ The following are possible non-technical issues for SSI/DID

Category	Perspective	Overview
Business	Adaptation to current IT/digital systems	• To enable SSI/DID, credential issuance and validation, current IT systems may need to be migrated or new systems may need to be built, but in many cases the investment is not yet worth it.
	Individual implementation /consideration for use case	• Currently, SSI/DID is not widely used, and it is necessary for companies and governments to continue to propose easy-to-use solutions to individuals. In addition, it is very important to develop the market for applications suitable for SSI.

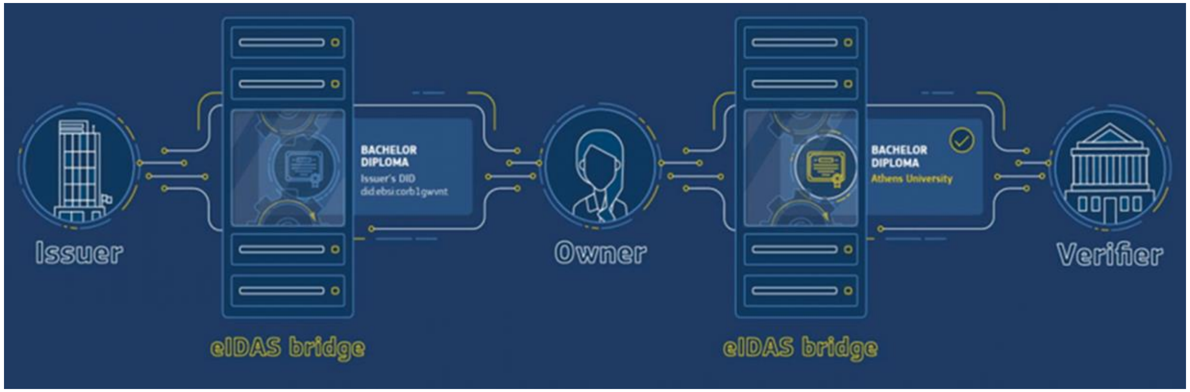
3-4-2. Issues of SSI/DID - (2) Non-Technical Issues

Issues of SSI/DID on Legal and Public Systems: Legal Status of Digital Certificates, etc.

- ■ One of the legal/public system issues that is currently being considered and discussed the most, both domestically and internationally, is considered to be positioned as a verifiable certificate for electronic signatures, electronic transactions regulations, and electronic documents that support SSI/DID.
- ■ For example, in the EU, consideration is underway to make SSI/DID to be supported to the eIDAS regulation adopted in 2014.
  - In eIDAS, the legal validity of trust services and eID, including digital signatures, will be approved, and the results of eID certification can be accepted by each EU member state, therfore whether SSI/DID is applicable to this eIDAS has become a point of discussion.
  - This point is being considered in detail in the eIDAS Bridge*1, which positions eIDAS as a trust framework for the SSI ecosystem, and in the EBSI ESSIF*2, which is a European SSI framework.

Case: eIDAS Bridge

- The European Commission has developed the eIDAS Bridge to promote eIDAS as a trust framework for the SSI ecosystem.
- The eIDAS Bridge assists in the process of signing Verifiable credentials for the Issuer, and for the Verifier, assists in identifying the Issuer (legal entity within the scope of this project) behind the Issuer's DID in the credential verification process. eIDAS By "crossing" the Bridge, the Verifiable credential becomes trustworthy.



Note 1: For more information about eIDAS Bridge, refer to the following
https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about
Note 2: For more information on ESSIF, refer to EBSI's
https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505360

Issues of SSI/DID on Legal and Public Systems: Data Protection System

- One of the reasons for the growing attention to SSI/DID is the strengthening of data protection laws and regulations in various countries, and the growing importance of personal data management in organizations. In order to promote SSI/DID, a system that encourages the promotion of such ideas and architectures will be necessary.
- For example, in SSI/DID, it is most important to protect the private key that enables the operation of the wallet, and if this key is unnecessarily disclosed or presented, it will cause the same human rights damage as a personal data leak. From this perspective, it may be necessary to consider the need for a legal and public system review.

Case: Wyoming, USA legislation

- The U.S. state of Wyoming is well known as one of the states actively encouraging blockchain-related businesses, and has enacted a number of blockchain-related laws.
- Among them, a proposed article (34-29-107) on "disclosure of private keys" is presented as an additional article (34-29-107) to the Act on Digital Assets (Section 34-29), which is attracting attention as it guarantees the right of individuals to protect their "private keys".
- This bill was rejected in April 2021, but it is assumed that similar bills will be considered in other countries around the world in the future for private keys.

“Disclosure of private cryptographic keys”

34-29-107. Production of private keys; prohibition

No person shall be compelled to produce a private key or make a private key known to any other person in any civil, administrative, legislative or other proceeding in this state that relates to a digital asset, other interest or right to which the private key provides access unless a public key is unavailable or unable to disclose the requisite information with respect to the digital asset, other interest or right. This paragraph shall not be interpreted to prohibit any lawful proceeding that compels a person to produce or disclose a digital asset, other interest or right to which a private key provides access, or to disclose information about the digital asset, other interest or right, provided that the proceeding does not require production or disclosure of the private key.

Source) Wyoming Senate Bill 105
https://legiscan.com/WY/text/SF0105/2021

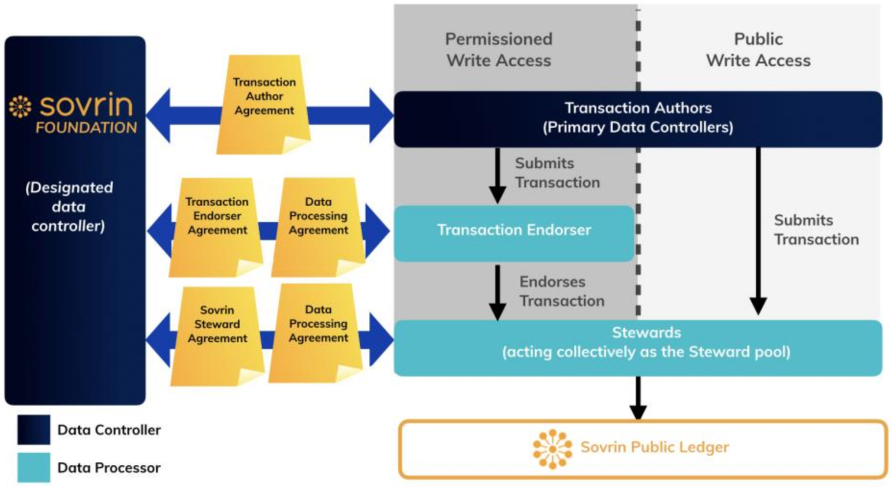
Issues of SSI/DID on Legal and Public Systems: Privacy

- ■ SSI is attracting attention as a possible solution to many existing privacy problems. For example, to address the right to be forgotten as stipulated in Article 17 of the EU's General Personal Data Protection Regulation (GDPR), SSI/DID allows individuals to control their own information linked to digital information, which can be beneficial for users and data controllers as it eliminates the need to manage unnecessary personal data.
- ■ However, when blockchain is used for SSI/DID, it is necessary to ensure that registration of personal data and PII in the ledger is avoided. It is assumed that this point will need to be better clarified and clarified depending on the use cases of SSI/DID.

Case: Sovrin Foundation's innitiatives

- Sovrin organizes the roles of key actors in a legal framework for complying with data protection laws in anticipation of the GDPR as shown in the figure on the right. Among them, with respect to Transaction Authors who write to Sovrin Leger, the current Permissioned Write Access polices allow only legal entities to write, not individuals. Sovrin mentioned the following as one of the reasons for this.

"This will reduce the risk of personal data being written to the Sovrin Ledger. This is currently prohibited by Permissioned Write Access polices, and Sovrin Foundation believes this protection is necessary under the current regulatory uncertainty regarding personal data on immutable public ledgers."


sovrin FOUNDATION
(Designated data controller)
Transaction Author Agreement
Transaction Endorser Agreement
Data Processing Agreement
Sovrin Steward Agreement
Data Processing Agreement
Permissioned Write Access
Public Write Access
Transaction Authors (Primary Data Controllers)
Submits Transaction
Transaction Endorser
Submits Transaction
Endorses Transaction
Stewards (acting collectively as the Steward pool)
Sovrin Public Ledger
Data Controller
Data Processor

Source) ：https://sovrin.org/data-protection/

3-4-2. Issues of SSI/DID - (2) Non-Technical Issues

Issues of SSI/DID on Operations and Business: Liability

- Among the operational and business issues of SSI/DID, the issue of liability has been pointed out as one that is unique to SSI/DID. In other words, in the services based on the SSI model, it is unclear at present how to organize the division of responsibility when problems occur.
  - In the conventional centralized and federation-type IMS model, liability issues are resolved through direct coordination and negotiation between IdPs/RPs. In the SSI model, the user who controls the wallet acts as the IdP itself, which means that the user must fulfill the responsibilities of the conventional IdPs, such as the government, companies, and organizations.
  - In fact, it is impossible to expect all users to coordinate their own activities, and some kind of support is needed from the perspective of financial inclusion. However, it is unclear who and how to provide such support, as well as their responsibilities, demarcation points, and how to handle contingencies. Unless this issue is resolved, users will not use SSI model services with confidence, and RPs will not provide services with unclear responsibilities, therefore, it is important from an operational and business perspective to consider the direction of resolution of this issue.

Case: OIX Trust Framework

- OIX suggests the creation and use of trust frameworks as one tool to solve such issues and points out the following features for the effective use and operation of trust frameworks.

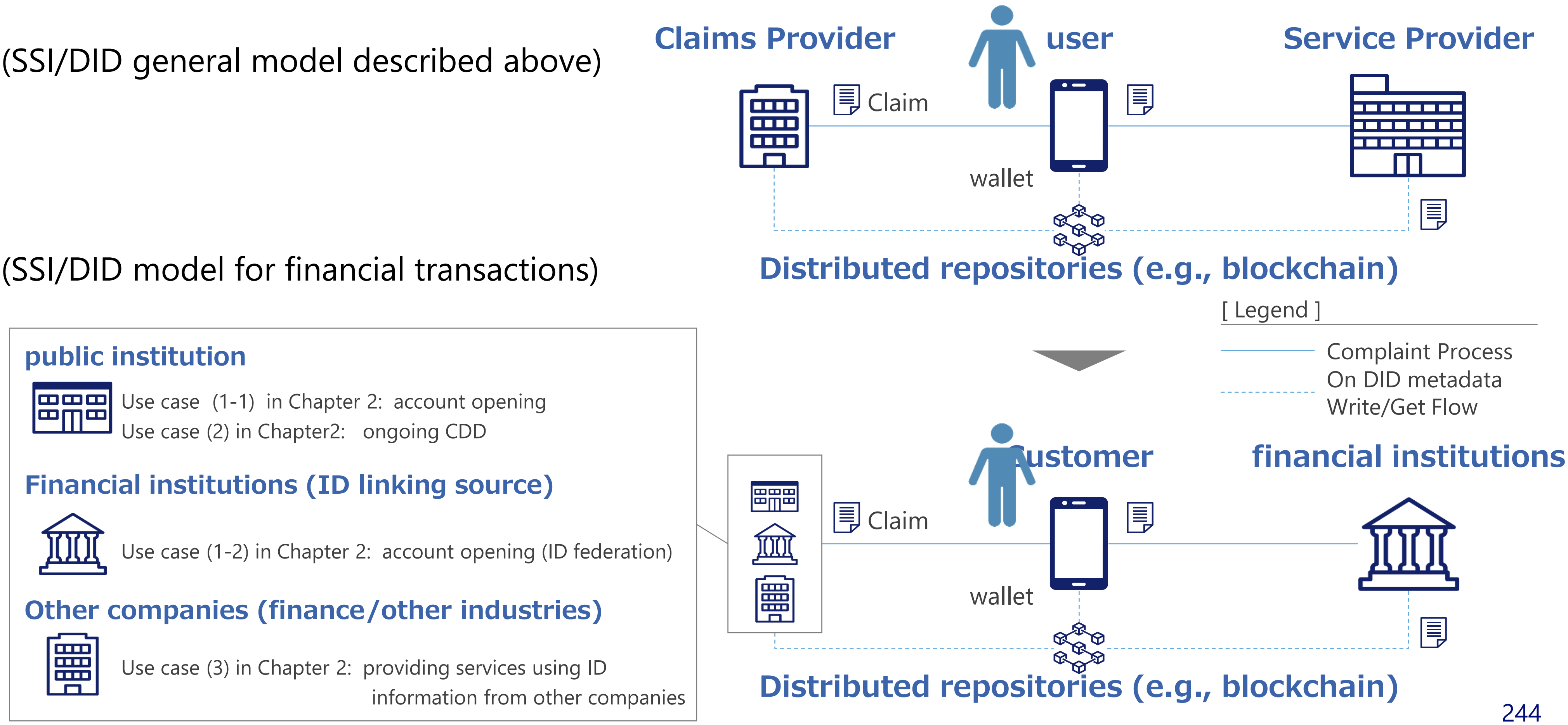
Items	Overview
Governance and Policy Development	• Developing and amending policies; decision making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
Policy Enforcement	• Ensuring compliance with existing policies; enforcement mechanisms; performing assessments or audits; managing changes and releases.
Participating Entity Management	• Administration and enrolment of participating entities; certification and trust marks; support; dispute resolution; billing.
Network Evolvement	• Growing and supporting the network; marketing; communication and; developing strategy
Trust Framework Operations	• Offering central services to the participating entities and/or public, e.g. fraud management, information and discovery services.

Source) ：OIX,” Guide to Trust framework”

3-5. Financial Regulatory Issues in the Use of SSI/DID

Assumptions of identity management using SSI/DID in considering financial regulatory issues

- Applying the financial transaction entities to the SSI/DID model described above, the model in the lower part is assumed for consideration.
- It is assumed that the financial institution can store and use the claim received from the customer.



(SSI/DID general model described above)

(SSI/DID model for financial transactions)

public institution

Use case (1-1) in Chapter 2: account opening
Use case (2) in Chapter2: ongoing CDD

Financial institutions (ID linking source)

Use case (1-2) in Chapter 2: account opening (ID federation)

Other companies (finance/other industries)

Use case (3) in Chapter 2: providing services using ID information from other companies

[Legend]

Complaint Process

On DID metadata Write/Get Flow

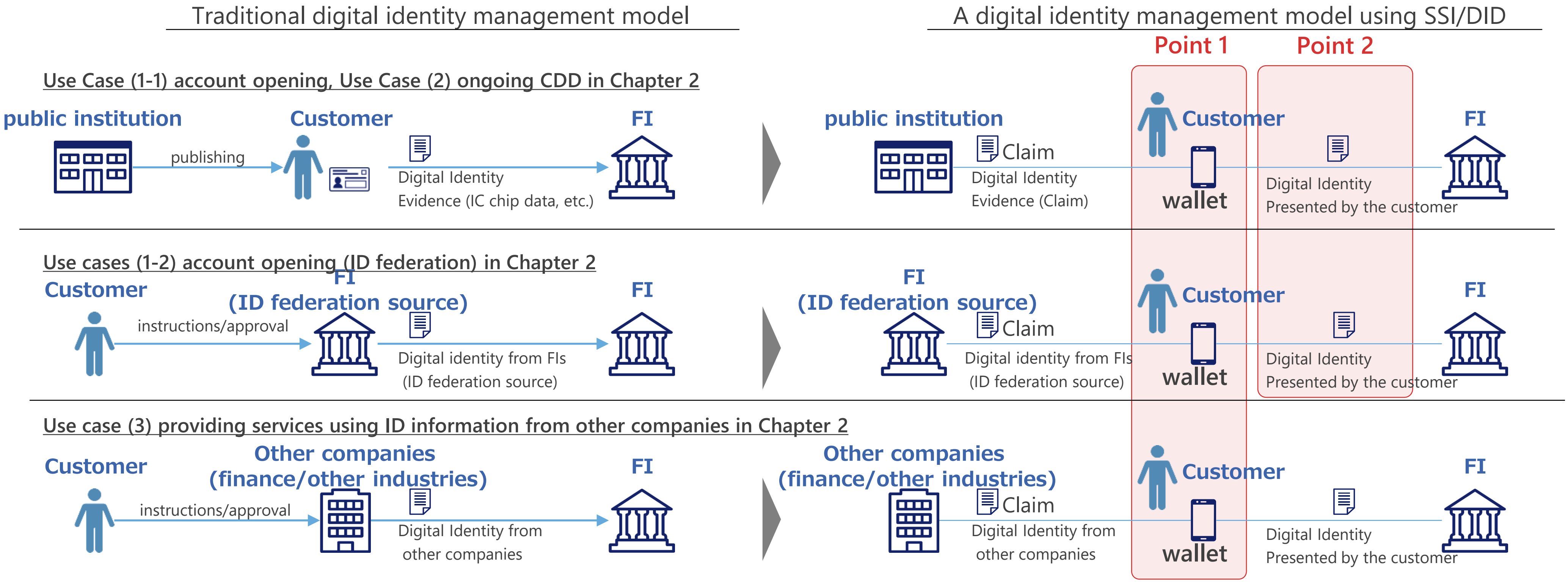
3-5. Financial Regulatory Issues in the Use of SSI/DID

Approaches to Financial Regulatory Issues in the SSI/DID Utilization Model

- There are two major differences from the traditional digital identity management model.
  1) All claims linked to a financial institution (FI) originate from the customer's Wallet.
  2) The data linked to the financial institution will be the claim presented by the customer.
- We will examine the points that are newly subject to financial regulation due to the above two points as the discussion points.

Discussion point 1) **Approach to financial regulation of Wallet**

Discussion point 2) **Legal treatment of new identification information**



Traditional digital identity management model

A digital identity management model using SSI/DID

Point 1

Point 2

Use Case (1-1) account opening, Use Case (2) ongoing CDD in Chapter 2

public institution → publishing → Customer → Digital Identity Evidence (IC chip data, etc.) → FI

public institution → Claim Digital Identity Evidence (Claim) → Customer wallet → Digital Identity Presented by the customer → FI

Use cases (1-2) account opening (ID federation) in Chapter 2

Customer → instructions/approval → FI (ID federation source) → Digital identity from FIs (ID federation source) → FI

FI (ID federation source) → Claim Digital identity from FIs (ID federation source) → Customer wallet → Digital Identity Presented by the customer → FI

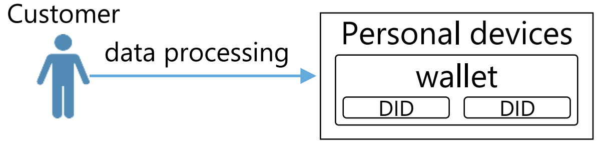
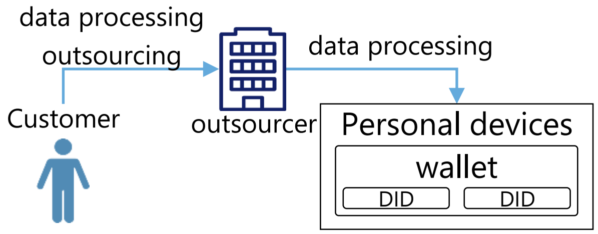
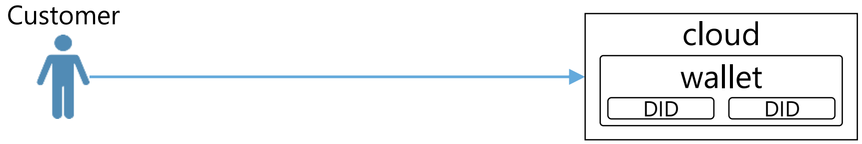
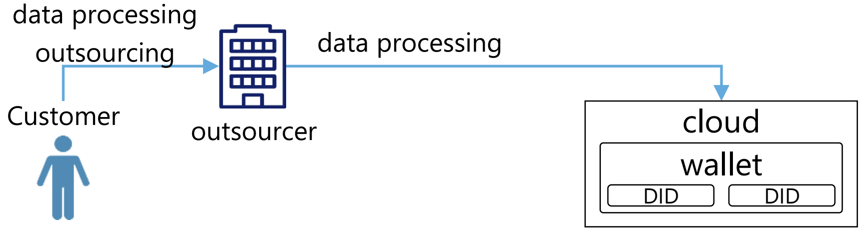
Use case (3) providing services using ID information from other companies in Chapter 2

Customer → instructions/approval → Other companies (finance/other industries) → Digital Identity from other companies → FI

Other companies (finance/other industries) → Claim Digital Identity from other companies → Customer wallet → Digital Identity Presented by the customer → FI

Assumptions and methods for consideration
(1) Patterns of Wallet operation patterns

- The following four patterns of wallet operations are categorized based on the two axes of "data operation and management entity" and "data storage environment".
- We will examine the impact of different types of wallet operations on financial regulations.

No.	Data operation and management entity		Data storage environment	Image of Wallet Operation Form
	manager	operator		
1	Self (Customer)	self	local	 Customer data processing Personal devices wallet DID DID
2 3		Contractor (Wallet Provider)	local	 data processing outsourcing data processing Customer outsourcer Personal devices wallet DID DID
4		self	cloud	
		Contractor (Wallet Provider)	cloud	 data processing outsourcing data processing Customer outsourcer cloud wallet DID DID

Assumptions and methods for consideration
(2) Evaluation items regarding the feasibility of financial regulations

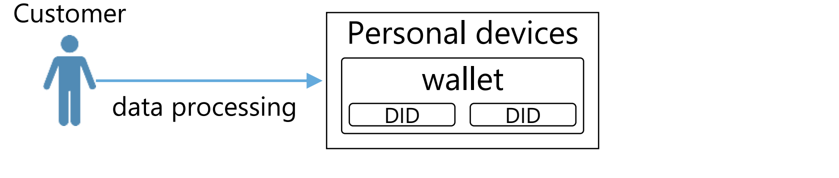
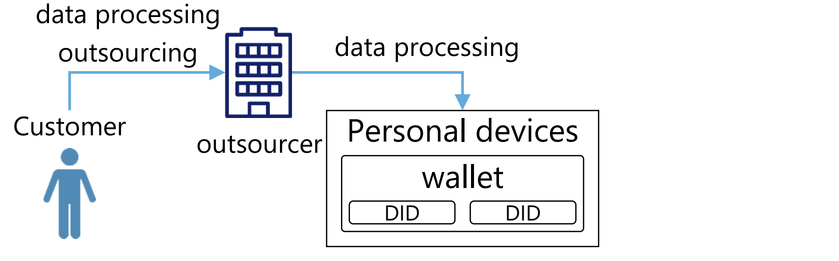
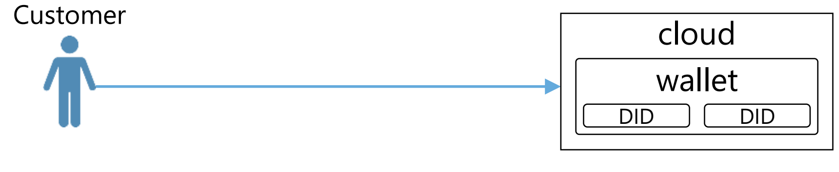
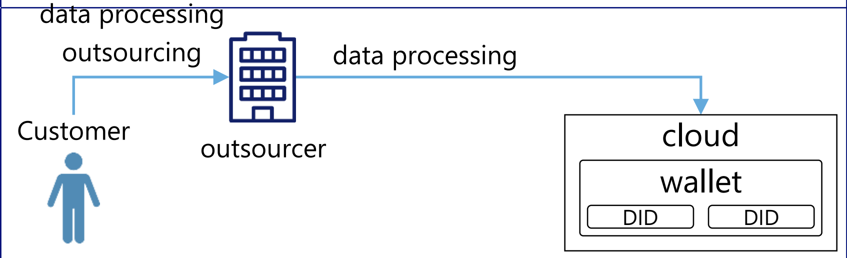
- Since all claims linked to financial institutions originate from the customer's Wallet, it is necessary to ensure the security of claims transmitted from the Wallet and the channels for investigation and accountability in order to stabilize the financial system.
- To this end, we will evaluate the following three financial regulatory issues with respect to Wallet, and examine their implications for financial regulation.

1)	Wallet operation reliability	Whether the binding of the customer's ID and the claim of the cooperation source is performed correctly, and the correct claim of the customer can be linked to the financial institution.
2)	Pursuing responsibility and responding when problems occur	Whether the customer, who is the source and ultimate responsible party of the claim, can be held accountable and asked to take action in the event of unauthorized use such as identity theft.
3)	Disclosure of data in Wallet during financial crime investigation	Whether investigators can examine data in the Wallet that is not stored by the financial institution during a financial crime investigation.

3-5. Financial regulatory issues when using SSI/DID Discussion Point 1) Financial regulatory approach to Wallet

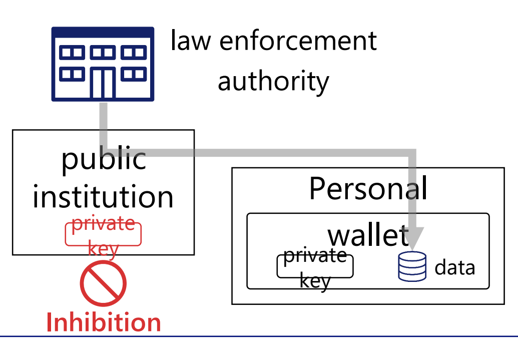
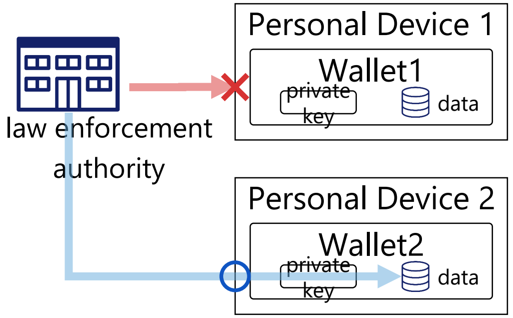
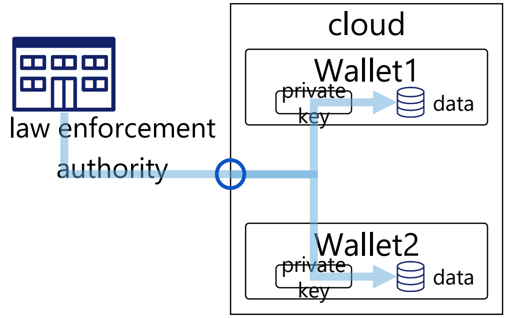
Results of the feasibility assessment of regulations for Wallet

- For financial regulatory purposes, the outsourced/cloud-based Wallet operation is currently preferred.

Regulation feasibility			Patterns in Wallet Operation Types	Assessment of the feasibility of financial regulation		
				1) Wallet operation Reliability	2) Pursuing responsibility and responding when problems occur	3) Disclosure of data in Wallet during financial crime investigation
	1	self/local	 Customer data processing Personal devices wallet DID DID	low (Concerns from the perspective of fraudulent use such as identity theft due to low operational reliability)	difficult (It is difficult to ask individuals to take responsibility for managing and responding to problems when they occur.)	difficult (Mandatory data disclosure to customers during financial crime investigations is difficult.)
	2	Outsourced/Local	 data processing outsourcing data processing Customer outsourcer Personal devices wallet DID DID	high (Concerns are reduced when compared to self-management because the data is processed by a contractor.)	acceptable (There is room to hold the trustee accountable to a certain extent, and stable management is expected compared to self-management.)	difficult (Mandatory data disclosure to customers during financial crime investigations is difficult.)
	3	Self/Cloud		low (Concerns from the perspective of fraudulent use such as identity theft due to low operational reliability)	difficult (It is difficult to ask individuals to take responsibility for managing and responding to problems when they occur.)	acceptable (More feasible than personal devices, depending on the disclosure policy of the cloud vendor)
	4	Outsourced/Cloud	 data processing outsourcing data processing Customer outsourcer cloud wallet DID DID	high (Concerns are reduced when compared to self-management because the data is processed by a contractor.)	acceptable (There is room to hold the trustee accountable to a certain extent, and stable management is expected compared to self-management.)	acceptable (More feasible than personal devices, depending on the disclosure policy of the cloud vendor)

(Supplemental) Differences in the disclosability of data in the wallet during financial crime investigations, etc., depending on the data storage environment

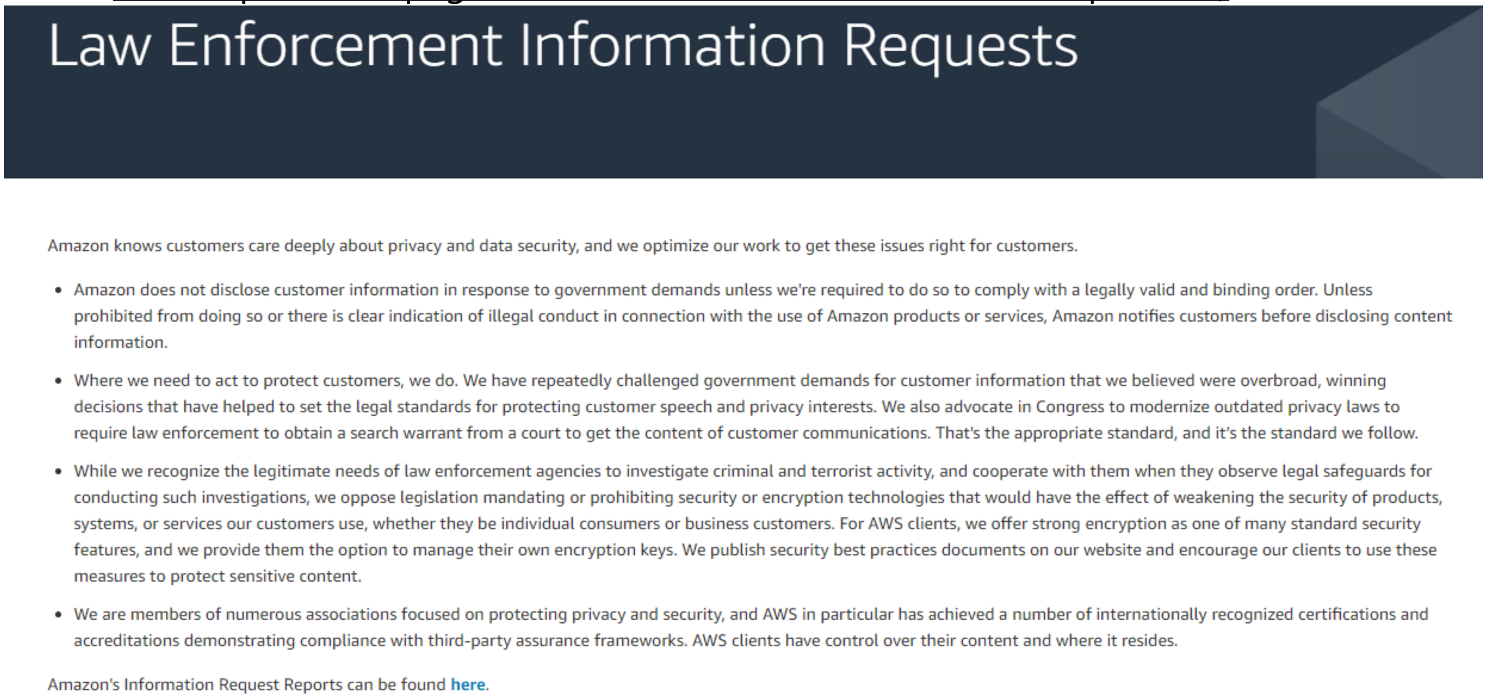
- Due to the way SSI/DID works, it is basically impossible to disclose data in the Wallet without the Wallet's private key.
- However, data necessary for criminal investigations, etc., must be compulsorily disclosed even when the customer refuses to provide the private key.
- Wallet should be managed in the cloud rather than in a local device, as authorities need special access to private keys during criminal investigations.

Pattern No.	1	2	3
Private key storage environment	Except Customer's Wallet	Customer's Wallet	
Wallet Storage Environment	-	local	cloud
Disclosure of data in wallet during financial crime investigation, etc. Disclosure of data in wallet	not allowed	difficult	acceptable
	The principle of not allowing others to manage private keys for any reason is in line with basic human rights. (This has been pointed out by foreign experts.)	Since the customer is the one in control of the device, depending on the type and configuration of the device, they may not be able to access the data needed for criminal investigations even if they try to obtain it through the backdoor.	Depending on the policy of cloud vendors in dealing with data disclosure during financial crimes, data disclosure via cloud vendors can be expected.
	 law enforcement authority public institution private key Inhibition Personal wallet private key data	 law enforcement authority Personal Device 1 Wallet1 private key data Personal Device 2 Wallet2 private key data	 law enforcement authority cloud Wallet1 private key data Wallet2 private key data

(Reference) Amazon Web Service's (AWS) approach to law enforcement information requests

- AWS will disclose necessary customer information in response to a government request when necessary to comply with a legally valid and binding order.
  - Disclose customer information in response to a government request when necessary to comply with a legally valid and binding order (red line below)
  - In response to the government's request, the company has indicated its intention to disclose only the necessary information in writing and only upon formal request. (Blue line below)

AWS explanation page for law enforcement information requests*1)



Law Enforcement Information Requests

Amazon knows customers care deeply about privacy and data security, and we optimize our work to get these issues right for customers.

- Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.
- Where we need to act to protect customers, we do. We have repeatedly challenged government demands for customer information that we believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests. We also advocate in Congress to modernize outdated privacy laws to require law enforcement to obtain a search warrant from a court to get the content of customer communications. That's the appropriate standard, and it's the standard we follow.
- While we recognize the legitimate needs of law enforcement agencies to investigate criminal and terrorist activity, and cooperate with them when they observe legal safeguards for conducting such investigations, we oppose legislation mandating or prohibiting security or encryption technologies that would have the effect of weakening the security of products, systems, or services our customers use, whether they be individual consumers or business customers. For AWS clients, we offer strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and encourage our clients to use these measures to protect sensitive content.
- We are members of numerous associations focused on protecting privacy and security, and AWS in particular has achieved a number of internationally recognized certifications and accreditations demonstrating compliance with third-party assurance frameworks. AWS clients have control over their content and where it resides.

Amazon's Information Request Reports can be found **here**.

https://aws.amazon.com/compliance/amazon-information-requests/

Suggestions on how to proceed with financial regulation of Wallet

- Since it is necessary to properly regulate Wallet connected to financial institutions, it is considered realistic to first focus on the "outsourced/cloud type", which is the least difficult to regulate, to enable financial use.
  - For self-managed and personal devices, it is more difficult to ensure the quality of Wallet applications and operations, and to secure backdoors for criminal investigations.

- In the case of "outsourced and cloud-based," the Wallet provider and the cloud vendor used by the Wallet provider would need to be subject to financial regulation.
  - It is considered necessary to establish rules so that only Wallet providers that meet certain criteria can connect to financial institutions.
    - For example, Wallet providers should be registered, and there should be technical restrictions to ensure that only digital identities entrusted to registered Wallet providers can be used for account opening and financial transactions.
  - It is considered necessary to establish rules so that cloud vendors that store Wallet data can respond to data disclosure requests during financial crime investigations.
    - For example, as well as the Wallet provider, the cloud service that stores the Wallet data should also be required to register.
  - In order to avoid dependency on a specific Wallet provider, it is also necessary to ensure that the Wallet provider can be changed (portability).

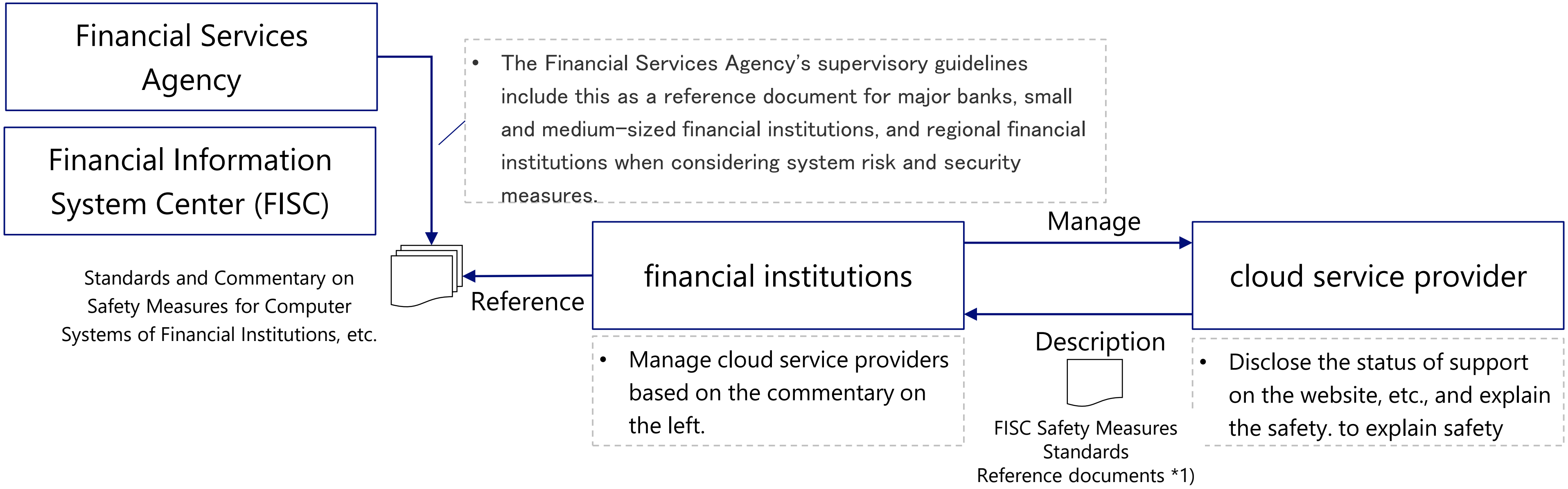
- In addition, it will be necessary to stipulate in advance the division of responsibility in the event of a problem and the request for data disclosure in the event of a financial crime investigation.

- As for the method of applying the rules, the example of applying the guidelines to the use of public cloud in financial services is considered to be helpful. (outlined in the next page).
  - Unlike the case of using public clouds, in the case of Wallet, there is no contractual relationship between financial institutions and Wallet providers. However, since Wallet providers need to be connected to financial institutions for business purposes, they will have an incentive to comply with the guidelines.

(Reference) Allowance of guidelines for the use of public clouds in financial services

- The Financial Services Agency's (FSA) supervision of financial institutions and the evaluation of public cloud services by financial institutions are based on the guidelines of the "Standards and Commentary on Safety Measures for Computer Systems of Financial Institutions" (hereinafter referred to as the "Safety Measures Standards") established by the Financial Information Systems Center (hereinafter referred to as FISC) as voluntary standards for financial institutions.

Safety Assessment of Public Cloud Services for Financial Services in Light of FISC Safety Management Standards


Financial Services Agency
Financial Information System Center (FISC)
Standards and Commentary on Safety Measures for Computer Systems of Financial Institutions, etc.
Reference
financial institutions
Manage
cloud service provider
Description
FISC Safety Measures Standards
Reference documents *1)

- The Financial Services Agency's supervisory guidelines include this as a reference document for major banks, small and medium-sized financial institutions, and regional financial institutions when considering system risk and security measures.

- Manage cloud service providers based on the commentary on the left.

- Disclose the status of support on the website, etc., and explain the safety. to explain safety

*1) Amazon Web Services Japan, Inc. AWS FISC Security Standards Compliance Reference for Financial Institutions
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_FISC_ Guidelines_9thEdition.pdf

(Discussion Point 2) Legal treatment of new identification information

- Since the identification information presented to financial institutions will be in the form of a digital identity in which the individual will be the IdP, the issue is how to legally recognize the digital identity issued by the individual.
  - The issuer of the Claim bound to the digital identity is assumed to be the same as the current issuer/ID federation source.

Comparison of the form and items of data linked to financial institutions in traditional digital identity and SSI/DID

(A) For use cases (1-1) account opening and use case (2) ongoing CDD in Chapter 2

	Data form	Data Items
Traditional digital identity	digital identity evidence (Data in IC chip, etc.)	All items with identity evidence
SSI/DID	**Digital identity issued by an individual (Claims from public institutions, etc.)**	**Only necessary items**

(B) Use case (1-2) in Chapter 2: Account opening (ID federation)

	Data form	Data Items
Traditional digital identity	Financial institutions (identity federators) Digital Identity	Identity verification items for each financial institution (Not disclosed to customers)
SSI/DID	**Digital identity issued by an individual (Claims of public institutions and financial institutions (ID linkage source))**	**Items for identification of each financial institution (Open to customers)**

Appendix:
Satisfiability of SSI/DID Characteristics Using Federation Model

Appendix

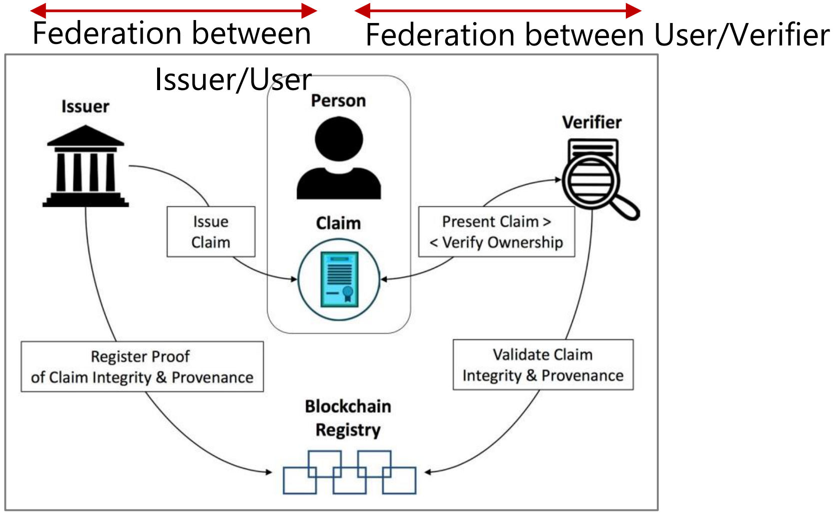
Satisfiability of SSI/DID Characteristics Using Federation Model

- In SSI model, individuals need to be able to control their own identities without the intervention of a third party as the identity management entity. To realize this, a form in which the user himself becomes the IdP is considered to secure the right of control over attribute information.
- When a user acts as an ID provider and asserts claims, there are multiple possible implementations of the topology depending on where the ID provider features are deployed. If it is deployed on a local machine such as a "Wallet", an approach to realize it by combining two Federation models* can be considered. In fact, a service with the same topology has been deployed in the past, and the feasibility was expected. On the other hand, it is difficult for these services to be widely used in actual business.

*) Introduction of Distributed / Agregated Claims Model

- In this section, based on this background, before sorting out the issues in the SSI model, we will first organize whether or not SSI/DID is satisfied in the federation model, and then sort out the issues that will hinder the deployment in actual business.

SSI model realization for locally deployed ID provider features

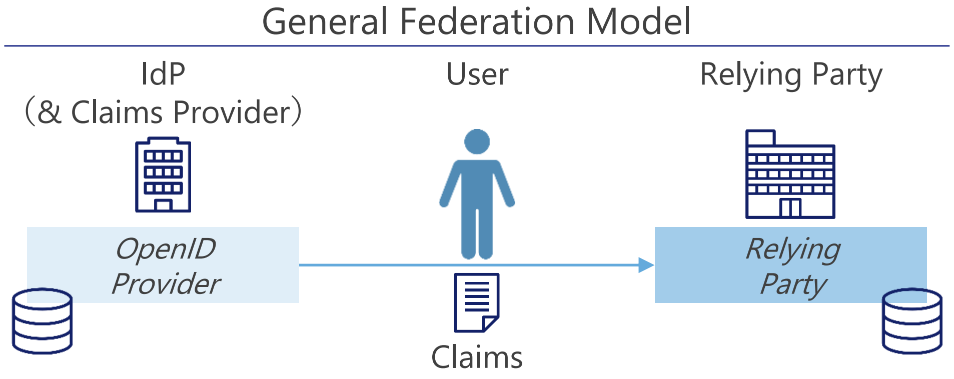

Federation between Issuer/User
Federation between User/Verifier
Issuer
Person
Verifier
Issue Claim
Claim
Present Claim >
< Verify Ownership
Register Proof of Claim Integrity & Provenance
Validate Claim Integrity & Provenance
Blockchain Registry

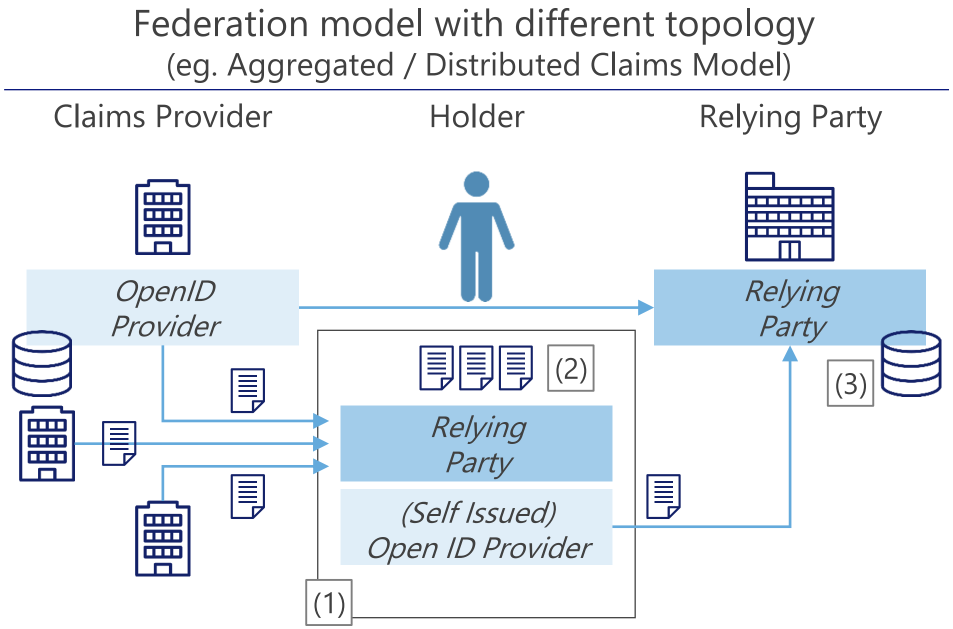
Source) decentralized-id.com with NRI additions

Appendix

Satisfiability of SSI/DID Characteristics Using Federation Model

- By changing the topology using the OpenID Connect specification, it is possible to implement 1. Separation of Authentication and Attributes, 2. Utilizing and Selectively Presentation of Distributed Attribute Information, and 3. Confidentiality of presentation destination (Unlinkability).




Federation model with different topology
(eg. Aggregated / Distributed Claims Model)
Claims Provider
Holder
Relying Party
OpenID Provider
Relying Party
(2)
(3)
Relying Party
(Self Issued) Open ID Provider
(1)

SSI/DID Characteristics	Supported specs for OpenID Connect	Implementation Overview
1. Separation of Authentication and Attributes	Self-Issuerd Open Provider （SIOP）	User becomes an IdP, so that claims can be asserted by federation between CP and Holder, and between Holder and SP.
2. Utilizing and Selectively Presentation of Distributed Attribute Information	Aggrigated Claims	Aggregate Claims on multiple CPs
	Distributed Claims	Claims collected in the Holder are selectively presented to SPs.
3. Confidentiality of presentation destination (Unlinkability)	Self-Issuerd Open Provider （SIOP）	Users themselves can become IdPs and assert claims via Holder instead of federation between CP/SP.

Satisfiability of SSI/DID Characteristics Using Federation Model

- 4. Long-term Storage and Usage of Digital Identities is outside the scope of the OpenID Conncet specification, and if it is to be implemented, it will be necessary to consider implementation in combination with other specifications related to long-term signatures.
  - As standards for long-term signatures, there are "CAdES" that supports PKCS#7 and CMS signature formats, "XAdES" that supports XML signature formats, "PAdES" that supports PDF signature formats, etc. In recent years, "JAdES" that supports JSON Web Token signature formats has also been specified by ETSI.

Scope of developing claim specs in OpenID Connect

> **5.7. Claim Stability and Uniqueness**
>
> The sub (subject) and iss (issuer) Claims, used together, are the only Claims that an RP can rely upon as a stable identifier for the End-User, since the sub Claim MUST be locally unique and never reassigned within the Issuer for a particular End-User, as described in Section 2.
> （omitted）
> **All other Claims carry no such guarantees across different issuers in terms of stability over time or uniqueness across users, and Issuers are permitted to apply local restrictions and policies.**

Source) ETSI, ISO

Standard examples of a long-term signature

Standard for long-term signatures	Target format	Main Standards (Technical Specification)
CAdES （CMS Advanced Electronic Signatures）	CMS, PKCS#7	ETSI TS 101 733 v2.2.1 (2013-04) ISO 14533-1:2014
XAdES （CMS Advanced Electronic Signatures）	XML	ETSI TS 101 903 v1.4.1 (2009-06) ISO 14533-2:2012
PAdES （PDF Advanced Electronic Signature）	PDF	ETSI TS 102 778-1/2/3/4/5 (2009-07) ETSI TS 102 778-3 V1.2.1 (2010-07) ISO 14533-3:2017 ISO32000-2: 2020
JAdES **（JSON Advanced Electronic Signature）**	**JSON**	**ETSI TS 119 182-1 V1.1.1 (2021-03)**

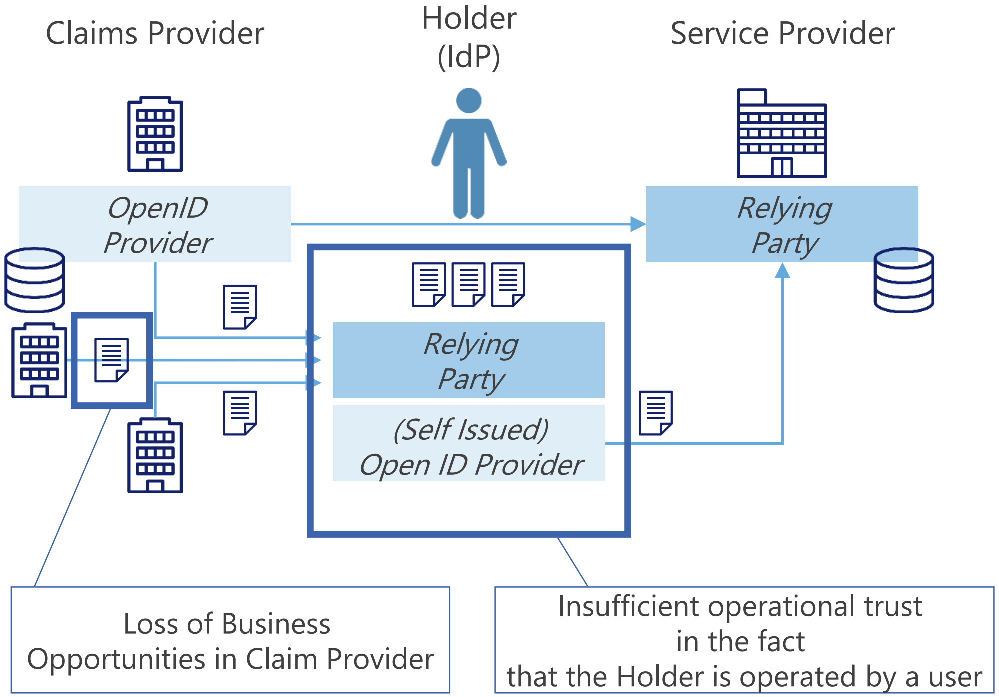
Appendix

Overview of Issues in SSI/DID Realization Using Federation Model

- As mentioned earlier, we examined the possibility of deploying an IMS with the four characteristics based on OpenID Connect, and we derived the hypothesis that it may be possible to implement the technology.
- In order to confirm our hypothesis, we surveyed and checked the cases where the service has been deployed*. Although we were able to confirm a certain level of functional sufficiency, it became clear that the use of the service was not widespread due to concerns about both business and operational perspectives. This is an issue that can occur not only with OpenID Connect but also with other SSI models (see 3-4-3 for details

(*) Distributed identifier obtaining by Linksafe, directory service by neustar, etc.

Problem areas in realizing SSI/DID in the federation model



Claims Provider
Holder (IdP)
Service Provider
OpenID Provider
Relying Party
Relying Party
(Self Issued) Open ID Provider
Loss of Business Opportunities in Claim Provider
Insufficient operational trust in the fact that the Holder is operated by a user

Examples of issues in actual services of the federation model

- The main issue on the business side is the opposition of claim providers, represented by data brokers, to the reduction of opportunities to provide data and to the secrecy of their partners.
- The main operational issue is that if the Holder is left completely to the user, there may be cases where the Holder cannot be trusted by the Claims Provider/Relying Party due to concerns about its operational and management capabilities.

Chapter 4: Future Issues in the Use of Digital Identity

4-1. Structure of this chapter

4-1. Structure of this chapter

Structure of this chapter

■ Purpose of this chapter

- In this chapter, future issues based on the overall analysis conducted in chapters from 1 to 3 are analyzed.
- More concretely, we will identify areas need to be further elaborated for the utilization of digital identities including SSI/DID, in other words, issues that should be discussed with participation of various stakeholders, including regulators, engineers, businesses, etc.

■ Analytical Methodology of this chapter

- Identification of issues will be conducted through, first, identifying problems raised in the Chapters from 1 to3 but with no accurate solutions within among them and, second, identifying and organizing specific concerns for each issue those stakeholders have.

4-2. Challenges and directions for solutions

4-2. stakeholders and their interests in each issue

Structure of this section

- In this and subsequent pages, we will examine the direction of problem solving and for each of the issues raised in Chapters 2 and 3, as well as the stakeholders and their concerns regarding each issue.
- The direction of problem solving was organized with reference to the advanced cases discussed in section 2-4 and the discussion in chapter 3.
- For stakeholders/interests, we identified stakeholders and objectives that would influence the direction of problem solving and organized potential interests.
- As a result, regardless of whether the issue is related to SSI/DID or not, there are several issues that seem to require coordination of interests among stakeholders, suggesting the need for a multi-stakeholder approach to resolution.
- The issues in Chapter 2 and Chapter 3 are divided and dealt with in 4-2-1 and 4-2-2, respectively, and the following information is provided for each. Some of the issues in both chapters overlap (e.g., division of responsibilities), but since the stakeholders are different, they are described separately.

4-2-1. Challenges and stakeholder concerns for the use of digital identities

- We extracted and organized the stakeholders and their interests in solving the issues raised in Chapter 2.
  In addition, we extracted and organized the stakeholders and their interests in solving the issues raised in Chapter 2 with SSI/DID.

4-2-2. Challenges and stakeholder concerns for the use of SSI/DID

- Extraction and organization of stakeholders and interests in utilizing SSI/DID was conducted.

1) Direction for solving “IAL” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
1) IAL	• **Develop a regulatory framework to promote appropriate use of digital IMS.**	• Establish an appropriate IAL and develop AML regulations linked to the IAL. As an approach to the development of the IAL, it is assumed that highly reliable national IDs will be widely used, and the development of AML regulations to enable this may be considered. (Case(2)(3)) • In addition, the scope of IAL maintenance may not be limited to identity verification, but may be extended to the level of assurance of customer attributes necessary for AML compliance (case(1)).	• financial authorities	• Promotion of principle-based measures that incorporate technological innovation • Sophistication of AML through the use of highly reliable IDs
			• financial institutions	• Sophistication of AML through the use of highly reliable IDs • Clarification of rules to clarify the scope of the company's responsibility
			• Customer	• Variety of identity choices available

4-2-1. Challenges and stakeholder concerns for the use of digital identities

2) Direction for solving “ID linking” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
2) ID linkage	• **Inadequate business model and division of responsibilities among ID linking parties**	• Clarification of the division of responsibilities through consultations among the parties concerned (case(5)) –Clarify the ultimate responsibility for performing various checks, etc. when KYC sharing using digital IDs is realized. –Clarify who is responsible for ensuring that data is up-to-date when new accounts are opened and when ongoing customer management is implemented. –Clarification of the boundary of responsibility in the event that a customer or a financial institution using an ID suffers some kind of damage due to a data error.	• financial authorities	• Clarify responsibilities in terms of regulatory oversight
			• Financial Institutions (digital ID sender/recipient)	• Limit the scope of the company's responsibility from a business perspective
			• Customer	• Clarification of responsibility in terms of compensation in case of disadvantage
			• Solutions Vendors	• Limit the scope of the company's responsibility from a business perspective
	• **Increased dependence on specific financial institutions (IdPs)**	• In order to reduce the dependency on a specific IdP, SSI/DID is considered to be one of the solutions to the problem, as discussed in Chapter 3. • On the other hand, as discussed in Chapter 3, one aspect of the implementation of financial regulations is the desirability of establishing a more reliable management system, such as outsourcing the operation and management of SSI/DID data to Wallet vendors and the Wallet management environment being in the cloud.	• financial authorities	• Building a more reliable management system
			• Major Financial Institutions	• Expand revenue from ID linking business as an IdP
			• financial institutions	• Reduce compliance costs by relying on IdP as RP
			• Customer	• Management that does not depend on a specific IdP
			• Wallet Vendor	• revenue increase • Flexibility of operation
			• Cloud Vendors	• revenue increase • Flexibility of operation

3) Direction for solving “Privacy” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
3) Privacy	• **As a data provider, the burden of handling customer consent for the provision of information to third parties is high.** • **As a data recipient, I have a heavy burden of explanation and confirmation for the data provider regarding the provision of information to third parties.**	• By using the SSI/DID system, the customer agrees to use the data with the companies based on their own sovereignty, thereby avoiding the form of third-party provision and reducing the burden.	• Personal Information Protection Authorities	• Protect customer privacy
			• Financial institutions and businesses (information linkage partners)	• Reduce the burden of providing information to third parties through SSI/DID. • The burden of transitioning to a new system • Compliance with Laws and Regulations
			• Customer	• Privacy protection • The burden of transitioning to a new system • Clarification of Consent Items
	• **Increased risk of variance between customers and financial institutions regarding the purpose and scope of data utilization**	• It is necessary to cover the veracity of the explanations provided by businesses regarding data utilization by means of audits, etc. by a third party.	• Personal Information Protection Authorities	• Protect customer privacy • Implementation of measures in compliance with laws and regulations
			• financial institutions	• Less burdensome response • Promotion of Data Utilization
			• Third-party organizations that audit financial institutions	• Confirmation of regulatory compliance • Implementation of measures in compliance with laws and regulations
			• Customer	• Ensuring privacy • Implementation of measures in compliance with laws and regulations

4) Direction for solving "Financial Inclusion” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
4) Financial inclusion	• **Financial exclusion of people who are not digitally compatible**	• Respond according to the current status of business development of financial institutions in each country and the political system of each country. – Actions based on the policy of bringing all citizens into the digital world by developing the infrastructure (identity management infrastructure and payment infrastructure) necessary for finance using digital identities on a national level (case(2) Singapore and case(3) India). – Policy of accepting both analog and digital forms by utilizing existing operations (Japan and other developed countries) • Financial authorities and financial institutions are trying to make AML more advanced through digitization in some aspects, so it is necessary to strike a balance between AML advancement and financial inclusion.	• financial authorities	• Achieve financial inclusion (especially in emerging countries) • Advancement of AML/CFT
			• Government authorities	• Promotion of digitization
			• financial institutions	• Advancement of AML/CFT • economy (saving money)
			• Customer	• Smooth access to financial services

4-2-1. Challenges and stakeholder concerns for the use of digital identities

5) Direction for solving “Interoperability” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
5) Interoperability	• **Burden of dealing with complicated ID linkage specifications**	• Technical specifications and related legal systems will be developed through collaboration between the public and private sectors, aiming for broad dissemination throughout society (case(9) Australia).	• financial authorities	• Establishment of an ID coordination environment through the development of a trust framework through collaboration between government agencies and the private sector, such as issuing government IDs.
			• standards body	• Technical Specification • Global standard, technical specifications with no significant cost burden
			• financial institutions	• Using Solutions • Global standard, technical specifications with no significant cost burden
			• Solution Vendors	• Providing Solutions • Global standard, technical specifications with no significant cost burden

6) Direction for solving “Investment decisions for transition to new operations” issues and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
6) Investment decisions for transitioning to new operations	• **Difficult to make investment decisions to change existing optimized operations to use digital IMS**	• In order to make the investment amount reasonable from the standpoint of cost-effectiveness, consider the following –Cost reduction through joint use of infrastructure –Engage the government to promote the development of the country. –Monetization through ID linkage (case(5))	• financial authorities	• Promote the use of digital IDs from the perspective of AML advancement, etc.
			• financial institutions	• Investment commensurate with effectiveness
			• ID distribution platform provider	• Collection of reasonable compensation for infrastructure development

4-2-1. Challenges and stakeholder concerns for the use of digital identities

7) Direction for solving “Various issues of cross-border transactions” and conflicts

Category	Issue	Direction of problem solving	Stakeholders	matters of interest
7) Issues in Cross-border Transactions	• **Differences in AML/CFT regulations in each country and legal barriers to cross-border data sharing in implementing FATF standards and other regulatory and supervisory requirements**	• One possible approach would be to unify confirmation at the time of transaction using eID, which can be applied to a wide area, and to develop an AML Directive that is consistent with the unification of confirmation at the time of transaction for a wide area (case(1) in the EU and case(7) in Scandinavia).	• financial authorities	• Development of regulatory framework/trust framework
			• financial institutions	• Decrease regulatory gap between jurisdictions to reduce costs
			• Customer	• Ensuring Convenience

4-2-2. Challenges and stakeholder concern in utilizing SSI/DID

1) Legal and public system issues

Category	Issue	Direction of problem solving	Stakeholder	Concern
1) Legal and public system	Engaging government and policy makers	• Public system issues need to be responded to in order to make the technical and legal framework for providing national ID documents that are supported for SSI. • For example, regulation of electronic signatures and electronic transactions that are supported for SSI/DID, and positioning them as certifications to be verifiable for electronic documents, etc.	• Financial Authorities	• Promotion of digitalization of financial services
			• Finance organization	• Promote the use of SSI/DID services
			• User	• Improved convenience and enhanced privacy
	Privacy Protection	• There is a need to review and, if necessary, revise the existing system for data protection regulations to protect the data, rights, and privacy of those who promote and direct SSI. • For example, consider the right to protect private keys for wallet operations. • When distributed ledgers or blockchain networks are used for SSI/DID, there is a risk that personal/confidential data may be registered in the distributed ledger. A review of regulations and the establishment of operational guidelines, etc. for their use will be required as necessary.	• Financial Authorities	• Disclosure of information (e.g., private keys) in the event of a financial crime
			• User/Consumer group	• Rights protection (e.g., freedom of expression, human rights)
			• Financial Authorities	• Identify issues and challenges that have not yet been addressed in existing regulations and guidelines
			• Finance organization/ business operators	• Provision of services and solutions that comply with various laws and regulations
			• User	• Determine which services have adequate privacy measures

2) Operational issues

Category	Issue	Direction of problem solving	Stakeholder	Concern
2) Operational	Trust Framework	• It is necessary to develop national and regional public and private frameworks to establish certification of qualified identity providers, such as the European Union's eIDAS.	• Finance organization/ business operators	• Regulatory compliance and service expansion
			• Regulatory authorities	• Regulatory development of trust frameworks
			• User	• Ensuring Convenience
	Liability	• In the SSI model, the user who controls the wallet acts as the IDP, and the user himself/herself is required to fulfill the responsibilities that should be fulfilled by the government, company, or organization in the past. Therefore, it is important to provide support to the user, but it is unclear who will be responsible, how they will be responsible, the boundaries of responsibility, and how they will be handled in case of emergency. • In lack of appropriate stakeholder participation, there is a risk that the responsibilities that should be taken into account will be missing and that the demarcation point will be unclear.	• Financial Authorities	• Clarify responsibilities in terms of regulatory oversight
			• User	• Clarification of responsibility in terms of compensation in case of disadvantage
			• Digital ID sender/receiver financial institutions/ID distribution platform providers/wallet providers	• Avoidance of liability in terms of risk aversion

4-2-2. Challenges and stakeholder concern in utilizing SSI/DID

2) Operational issues

Category	Issue	Direction of problem solving	Stakeholder	Concern
2) Operational	Standardization	• It is necessary for DID, VC, etc. to be accepted and recommended as standards by standardization bodies (SDOs) such as IEEE, ISO, ITU, and NIST. • The confusion of specifications makes it necessary for implementation vendors to consider interoperable implementations for each specification. This results in increased solution development and operating costs. • Individual implementations and fragmentation are growing, and reliance on specific vendors is increasing as a result, moving away from the SSI/DID model which aims to move away from reliance on identity providers (lack of agility and portability).	• Standards body	• Formulation and maintenance of technical specifications
			• Financial Authorities	• Regulatory development and evaluating the application of technology to regulations
			• Finance organization	• Using SSI/DID Solutions
			• Identity platform providers and wallet providers	• Provision and commercialization of identity solutions and functions

4-2-2. Challenges and stakeholder concern in utilizing SSI/DID

3) Business issues

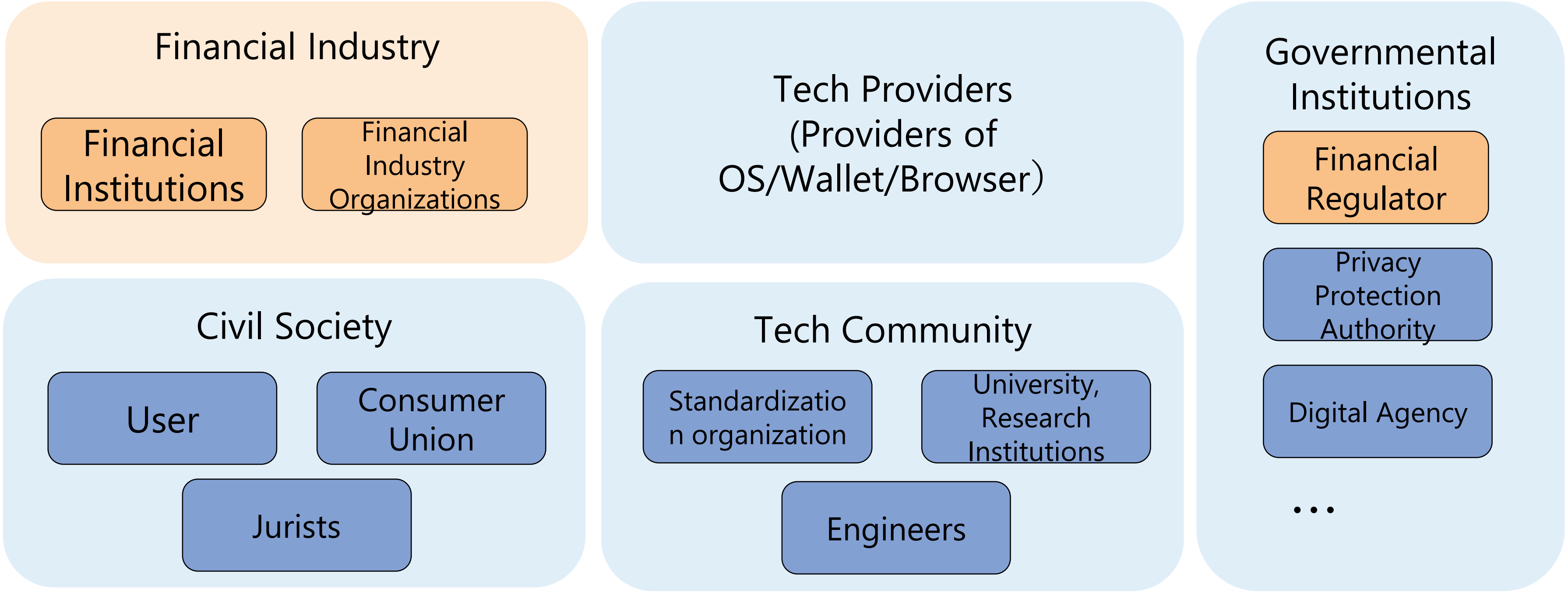
Category	Issue	Direction of problem solving	Stakeholder	Concern
3) Business	Adaptation to current IT/digital systems	• To make SSI/DID available, credential issuance and validation, current IT systems may need to be migrated or new systems may need to be built, but in many cases the investment is not yet worth it. • It is unlikely that all systems to which the system is asserted will migrate to the new scheme (SSI/DID scheme), and for the time being it will be necessary to be aware of the co-existence of the existing scheme (Federation scheme) and to deal with both schemes.	• Finance organization/ business operators	• Investment within the scope of explainable return on investment
			• Financial Authorities	• Promote the use of DID from the perspective of curbing onboarding costs across the industry.
			• Identity platform providers and wallet providers	• Collection of reasonable compensation for infrastructure development
	Lack of consideration of individual adoption/use cases	• Currently, SSI/DID is not widely used, and it is necessary for companies and governments to continue to propose easy-to-use solutions to individual users.	• User	• Smooth use of services
			• Consumer group	• Consumer protection, avoiding digital divide
			• Regulatory authorities	• Promotion of digitization
			• Finance organization	• Promote financial inclusion and responding to AML regulations
			• Identity platform providers and wallet providers	• Eliminating barriers to entry

4-2-1/2. Challenges and stakeholder concerns for the use of digital identities

(Reference) FIs need to collaborate with Tech Providers, Tech Community, Civil Society and Governmental Institutions outside of financial sector for resolving issues identified.

- We referenced discussion on "Trusted Web" white paper published by Headquarters for Digital Market Competition as a reference for identifying stakeholders.
  - "Stakeholders include not only engineers and platformers, but also various organization, such as service providers, infrastructure providers, university and research institutions, users, consumer unions, civil society, legal professionals, governments and so on." Source) "Trusted Web White Paper Ver1.0", p. 20 (Unofficial translation from Japanese version by NRI)
- Based on this notion, we categorized stakeholders in the financial sector as follows. As shown below, Financial Industry has to have cooperation and discussion for resolving issues identifies in 4.2. with various stakeholders which may include totally new organizations for FIs.

Stakeholders related to digital identity in the financial sector (Orange: Existing SH for FIs, Blue: new SH for FIs)



Financial Industry
Financial Institutions
Financial Industry Organizations
Tech Providers (Providers of OS/Wallet/Browser)
Governmental Institutions
Financial Regulator
Privacy Protection Authority
Digital Agency
…
Civil Society
User
Consumer Union
Jurists
Tech Community
Standardization organization
University, Research Institutions
Engineers

4-2-1/2. Challenges and stakeholder concerns for the use of digital identities

(Reference) Overview of the multi-stakeholder approach

- The Japan Financial Services Agency's report "A Study on Governance for Decentralized Finance Systems Using Blockchain Technologies" investigates the effectiveness of "multi-stakeholder governance" in examining the governance of decentralized financial systems, and we believe that multi-stakeholder governance is equally effective in addressing the challenges of digital identity.
- The research report summarizes the advantages of multi-stakeholder governance as follows.

Multi-stakeholder governance is a governance mechanism with continuity that consists of three or more stakeholders (interested parties) of the decentralized financial system with an emphasis on diversity and balance, and through meetings where each party can participate and discuss on an equal footing, to communicate through consensus-building and other means to resolve issues that are difficult to resolve by a single party or two.

The advantages of multi-stakeholder governance

To achieve multi-stakeholder governance, it is first necessary to form a multi-stakeholder conference body. In addition, the conference body needs to be structured with an emphasis on diversity and balance.

On the other hand, in order for the diversity and balance of the stakeholders that make up the conference body to be ensured, at least (1) the direct interests of the stakeholders, (2) the social attributes of the person in charge, (3) the competence (capability) of the person in charge, etc. must be clearly categorized. In particular, for the items (1) and (2), a balance (state of balance in distribution) is expected to be achieved across the entire conference body, and for the item (3), a certain level or higher must be achieved.

In other words, an orientation towards multi-stakeholder governance means that the parties' roles need to be clarified. Therefore, it is necessary to agree in advance that the definition of the parties mentioned in "Identification of issues" in the previous section ("Challenges posed by a decentralized financial system"), will be clarified. In other words, agreeing to the introduction of multi-stakeholder governance in a decentralized financial system implies that the parties of the decentralized financial system agree to relativize their roles and clarify their positions in the envisioned overall system in advance.

On the other hand, the relative clarity of definitions and roles would allow the followings:

- Decomposing the responsibilities to be taken (or avoided)
- Setting the parties' culpability for liability and limiting domain (distinguishing between infinite and finite)
- Setting the dividing line between the parties based on decomposed liability

If these roles and responsibilities are identified, we expect to see (1) a division of labor based on mutual respect, (2) improved ability to solve problems based on the division of labor, and (3) greater incentives to contribute to multi-stakeholder governance.

Source) JFSA, "A Study on Governance for Decentralized Finance Systems Using Blockchain Technologies" (May 2020)