Investigation Report (Summary Version)

International economic research project related to domestic and foreign integrated economic growth strategy in 2020.

(Survey on individual activity history in 100 years of life and the post-corona era)

March 2021

JIPDEC

(Japan Institute for Promotion of Digital Economy and Community)

Table of Contents

PROJECT OVERVIEW

Project Overview

■ Awareness of issues

- Individuals' ways of working, learning, and living would be independent of place or time. In the near future, the "era of individual empowerment" is expected to arrive. In the “individual empowerment era”, the activity history of individuals are consider to be important.
- However, DX (digital transformation) centered on “individuals” has not been clarified yet, although it is discussed from the view point for information banks and personal data.

■ Purpose

- In order to achieve the following three objectives, as a internationally accepted self-certification platform, we will aim to proceed DX for “individual activity history" managed by breaking away from paper certification, improving reliability, organizing information required for self-realization, and establishing data management methods, etc.
  1. Further improvement of transparency (ensuring safety) and realization of revitalization in terms of the labor market
  2. Expanding opportunities for re-learning and improving various skills of "individuals" in response to the progress of digitalization
  3. Creating new businesses related to sophisticated and individual-centered human resources and enhancing social security, etc.

■ Desired results

- Functional aspects
  - (1) Identification and Certification of Individuals
  - (2) How to link with Personal Data
  - (3) Methods for Certificating Personal Data
- Non-functional aspects
  - (4) How to handle Personal Data
  - (5) UX Improvements

Organize records handling

Considerations

- While considering the state of government-wide deliberations, including “Social Security and Tax Number System”, we examined the functional and non-functional governance required for proceeding DX in personal data.

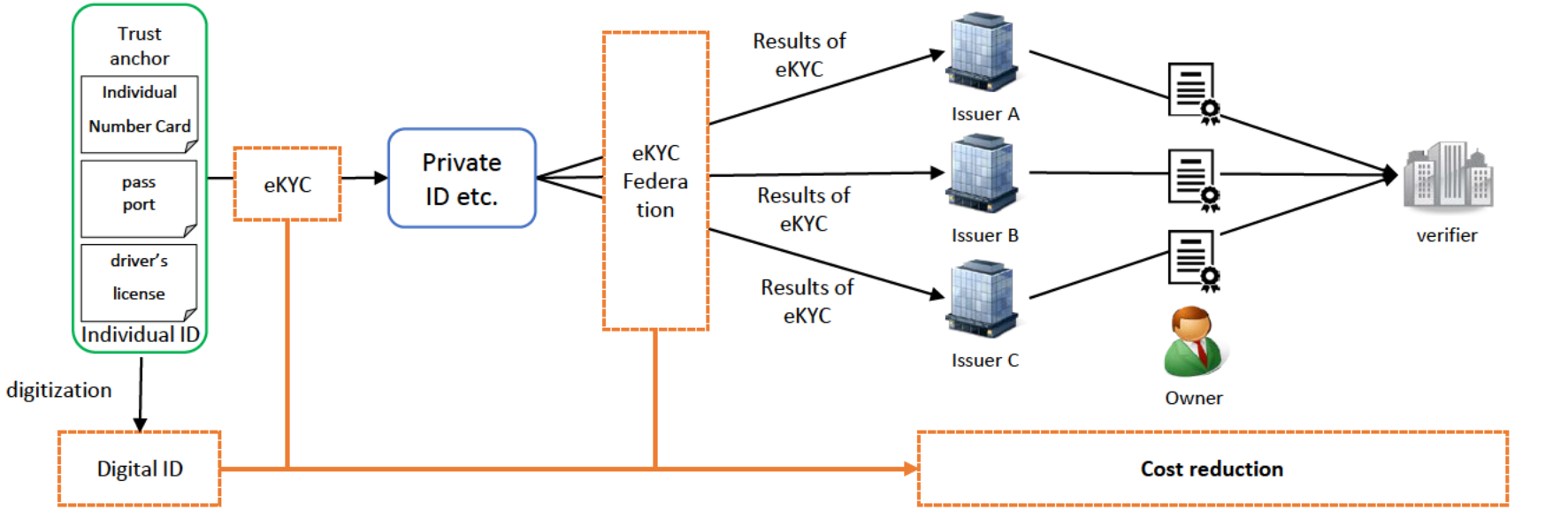
Considerations		Review overview
Functional aspects	(1) Identification and Certification of Individuals	• Personal ID and eKYCs in linking personal data • Ideal Digital Identity
	(2) How to link with Personal Data	• Digital Identity • Types of identity management • Types of federative methods that could prove personal data
	(3) Methods for Certificating Personal Data	• Components of an individual's activity history • Life cycle of activity history • Credential life cycle
Non-functional aspects	(4) How to handle Personal Data	• Approaches to Privacy • Data format • Ideal Ontology
	(5) UX Improvements	• Needs that lead to the improvement of UX • Requirements for UX Improvement

Functional aspects

(1) Identification and Certification of Individuals

Ideal Digital Identity

- One of the reasons why eKYC is not progressing in Japan is the lack of progress in the digitization of ID cards.
- In Japan, deliberations are underway at the “Study Group on Smartphones Installation of the functions of Individual Number Card" established by the Ministry of Internal Affairs and Communications. On the other hand, as an international standard, standards for digitization of passports, driver's license, and identity cards have been established.



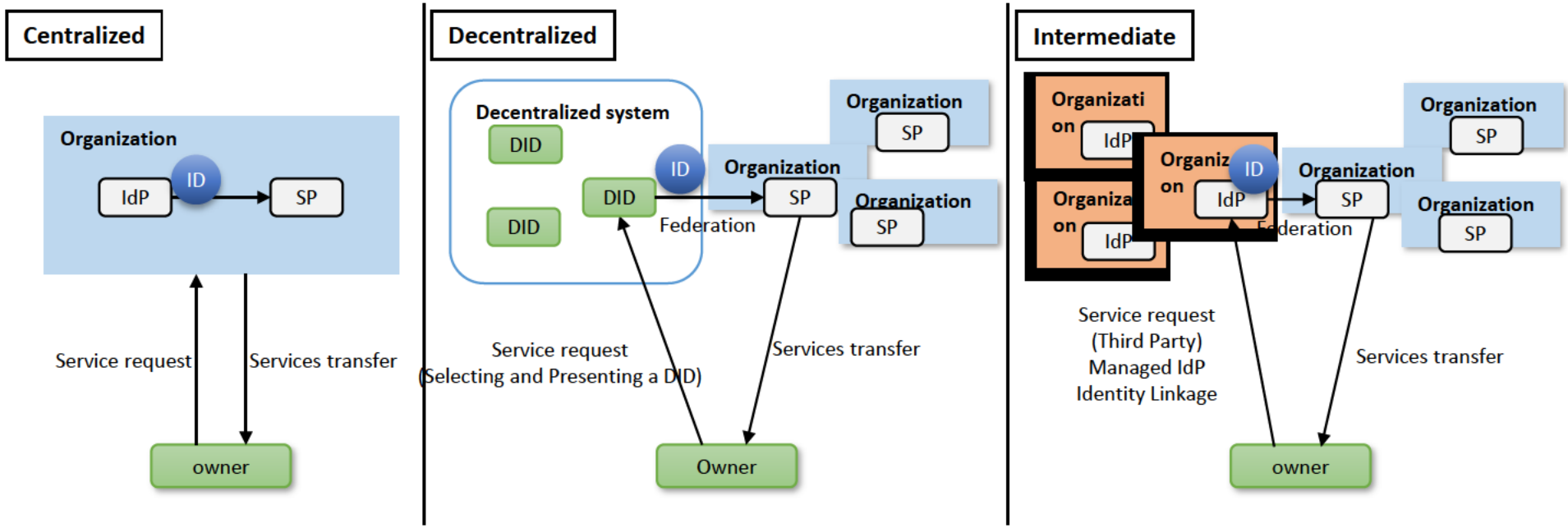
- It is necessary to develop infrastructure for digital ID in Japan.
- At the time, while the development of the infrastructure for digital ID is proceeding in accordance with international standards, the development of international standards in terms of privacy protection and security is still under way, and Japan will actively propose such measures.

Functional aspects

(2) HOW TO LINK WITH PERSONAL DATA

Types of identity management

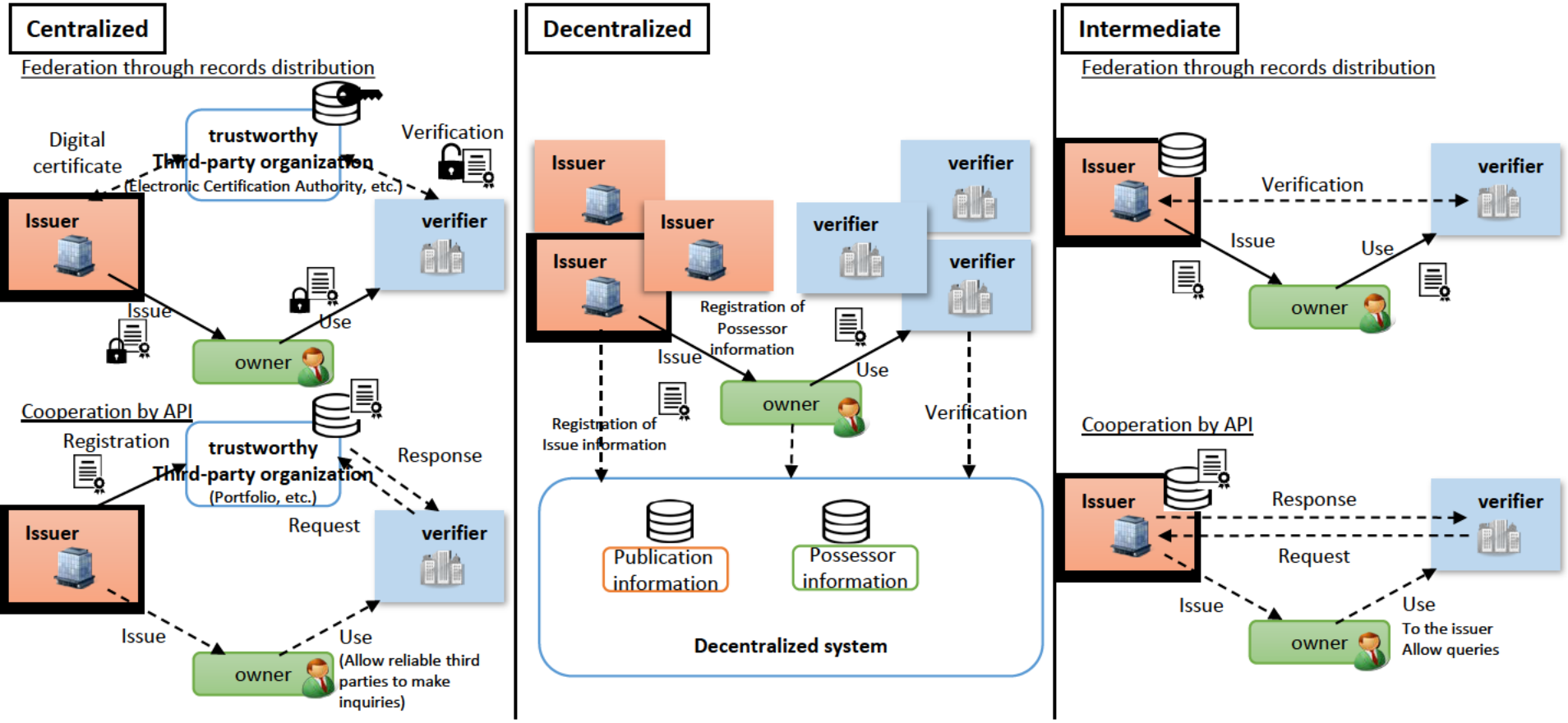
- Digital identity management could be classified into the following three categories:
  - Centralized ID management
    - The organization manages the identity of the owner.
  - Decentralized ID management
    - In a decentralized identity (DID), the owner oneself has the authority to manage the identity and cooperates to the extent permitted by the owner.
  - Intermediate ID management (Federation)
    - The identity of the owner is managed by IdP (Identity Provider) as a third party and cooperates to the extent permitted by the owner.



- Decentralized ID management is considered to be suitable for proceeding DX a personal activity history because owner could have all management authorities.
- However, it is necessary to consider the balance between responsibility and authority, because the owner is responsible for all the responsibility for using the identity.

Types of federative methods that could prove personal data

- 3 types of Federative methods that could prove personal data based on identity management.
- Centralized and intermediate types could be divided into methods of linking personal data in a verifiable format and the API provided by the issuer.



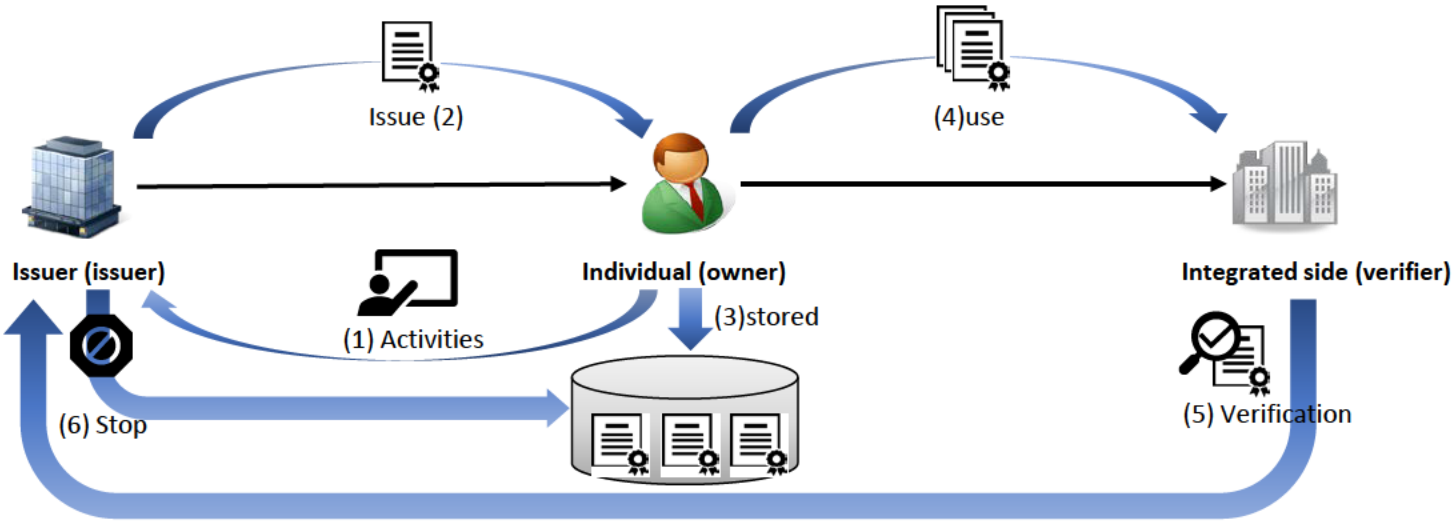
- For information to prove the status of an individual's activity history at a certain point in time, such as a certificate of qualification, coordination through records distribution is appropriate. On the other hand, in the scene where the information indicating the current state is linked, the linking by API may be better.
- Decentralized type that does not depend on the existence of the issuer is considered desirable from the perspective of the credibility of the issuer or third party (whether it will continue to exist in the future, etc.)

Functional aspects

3) METHODS FOR CERTIFICATING PERSONAL DATA

Life cycle of activity history

■ The life cycle of the digitized personal activity history data is as shown in the figure below.



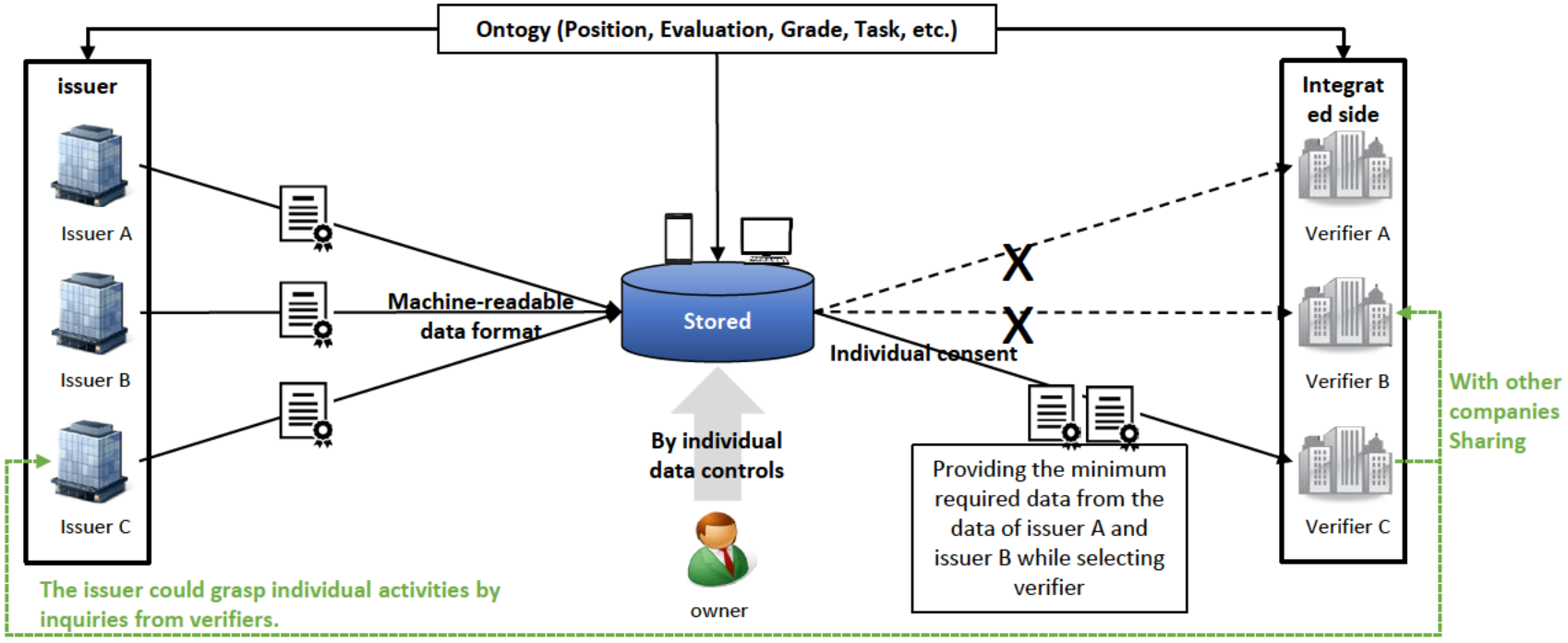
Life cycle of activity history	Contents
(1) Activities	The issuer confirms that the individual (owner) has skills and background.
(2)Issue	The issuer confirms the identity information of the individual and confirms the connection with the actual situation (Identity Proofing).
	The issuer registers in the database (Identity Register).
	The issuer issues a proof of activity history (Credential) to an individual based on the registration information.
(3)stored	Individuals stored evidence of activity history.
(4)use	Individuals present and share evidence of their activity history.
(5) Verification	The verifier confirms the proof of activity history presented by the individual.
	(AND / OR) The verifier validates the proof of activity history to the issuer according to the risk.
(6) Stop	The issuer suspends (revokes) the proof of the individual's activity history.
	(OR) The issuer reissues (revalidates) the proof of activity history to the individual.
	The (OR) issuer discontinues the business.

Non-functional aspects

4) HOW TO HANDLE PERSONAL DATA

Privacy Ontology and Data Format

- The data provided by the owner to the verifier is preferably the minimum required.
- Privacy risks due to the actions of the verifier and issuer may also be considered.
- Criteria for Ontology (Position, Evaluation, Grade, Task, etc.) have not been established.
- The format and structure of the personal activity history data and the functions to be implemented have not been determined.



- It is preferable that the data provided to the verifier could be controlled with the minimum necessary by the control by the owner.
- It is necessary to organize privacy risks and countermeasures based on the actions of verifiers and issuers.
- It is necessary to establish standard standards for owners, issuers, and verifiers to have a common understanding of positions, evaluations, grades, tasks, etc.
- In order to facilitate the distribution of personal activity history records, it is necessary to organize data formats, structures, and functions to be implemented in a structured and commonly use machine-readable format.

Non-functional aspects

(5) UX IMPROVEMENTS

Requirements for UX Improvement

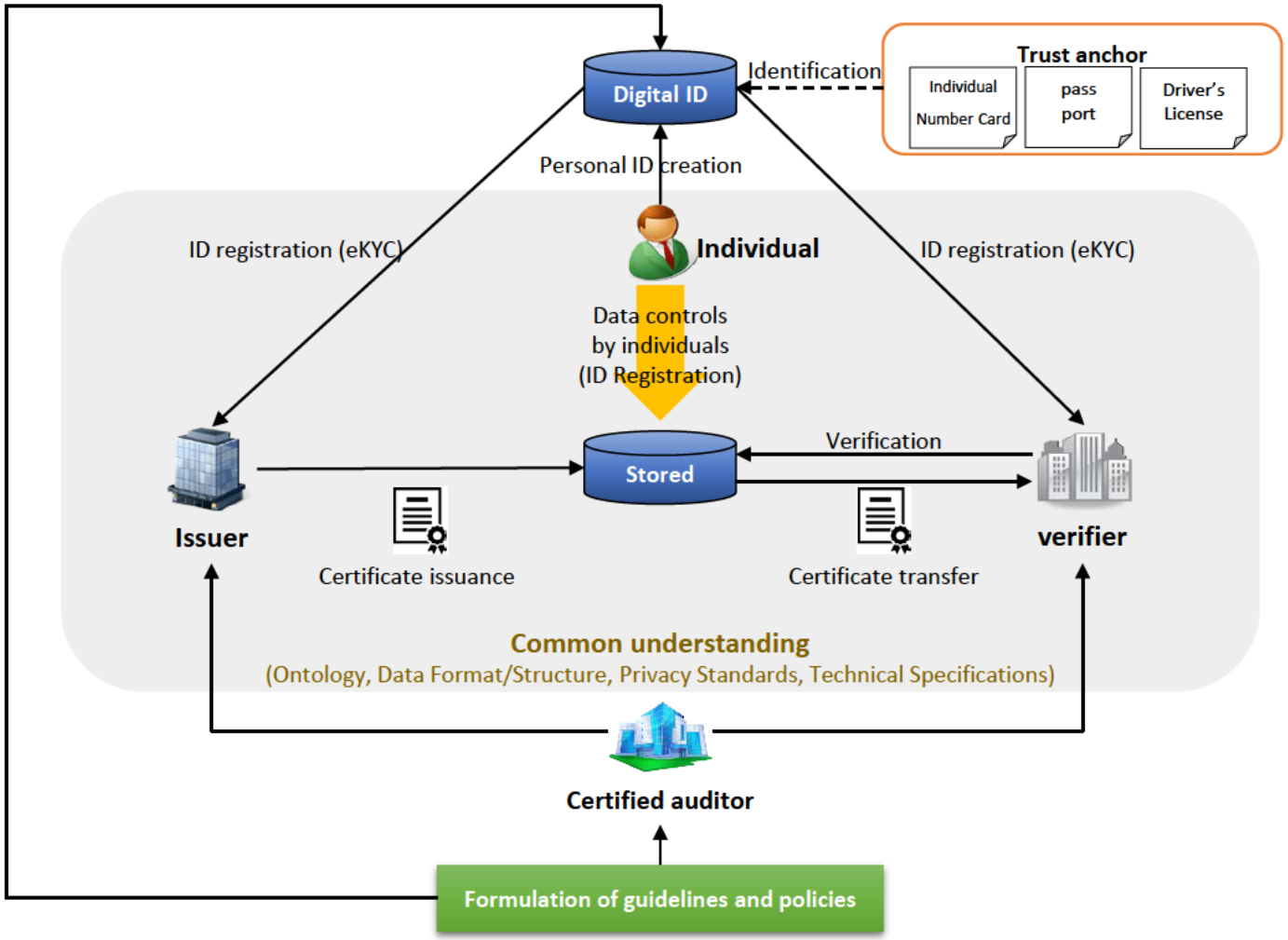
- We summarize as follows while organizing the elements required for an individual-centered social infrastructure that will continue to be used in the era of 100 years of life.

Elements	Description
Transparent	The transparency of personal activity history data is ensured by providing well-defined, comparable, shared and written information in a common language / description based on an ontology / framework.
Equitable	By allowing people with various qualifications / skills to present their qualifications / skills equally, it will be possible to obtain equal opportunities regardless of their connections.
Controllable	It has the authority to provide the necessary personal activity history data only for the parties, purposes, and periods specified by the owner. In addition, the personal activity history data provided will be used within a limited range and purpose with the consent of the individual.
Access	Owners could access their activity history records at any time. For example, if access is lost, such as when the issuer ceases to exist, reliable records of the duly issued activity history data must be directly available to restore or access credentials by other means.
Security	Compliance with relevant security standards to protect records from unauthorized editing and accessing.
Portability	Owners will be able to carry personal activity history data for their own purposes by organizing structured and commonly used machine-readable data formats and structures, functions to be implemented, etc.
Interoperability	Data could be machine readable, exchanged, and executed between systems based on a common ontology / framework. It also allows the combination of data from multiple publishers.
Shareability	Owners could share data when applying for employment, change of job, etc.
Voidability	It is possible to digitally confirm that the personal activity history data issued by the issuer would be correct.

4) BLUEPRINT OF FUTURE SOCIAL INFRASTRUCTURES (DRAFT)

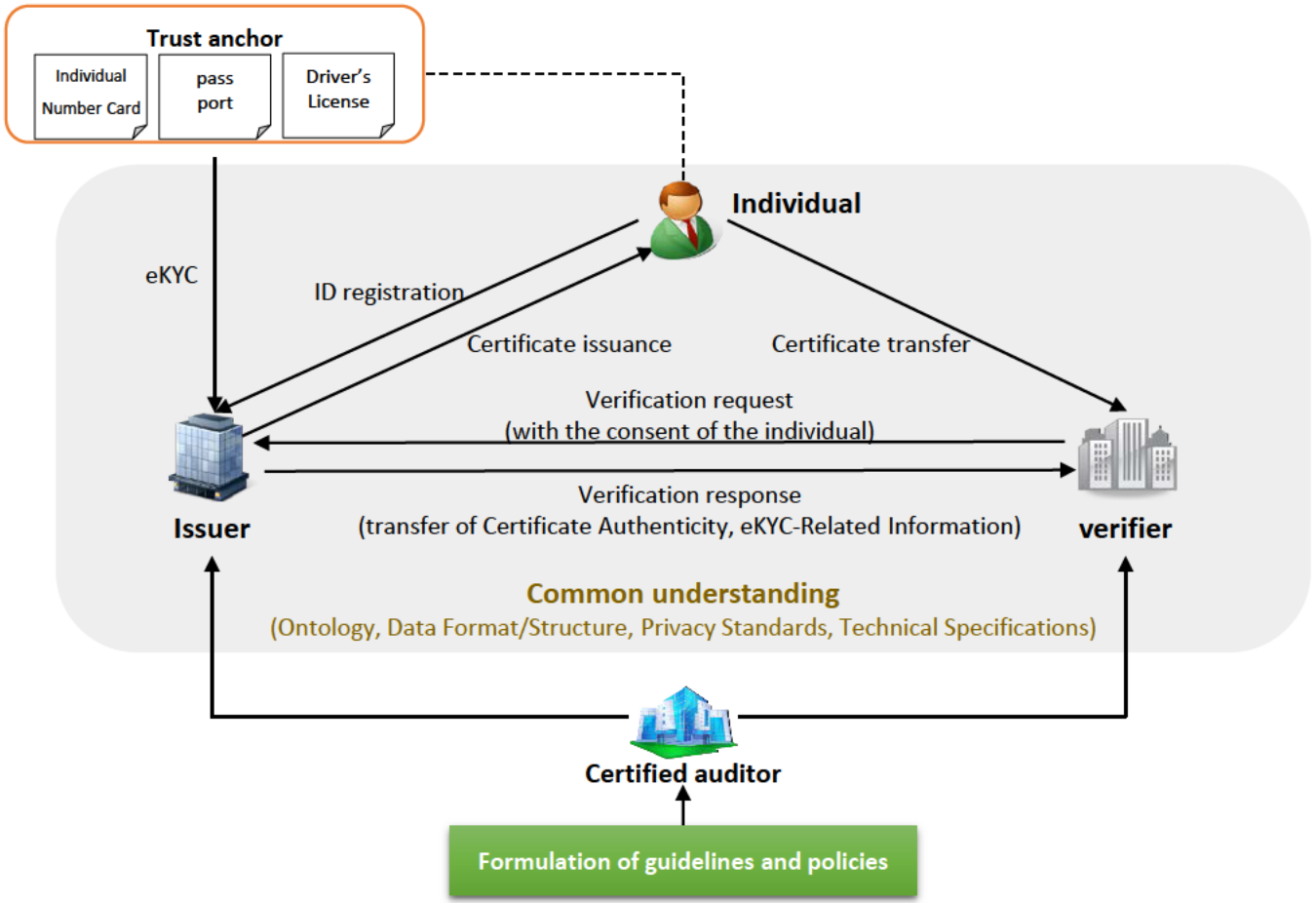
Ideal Future Social Infrastructures from a Long-Term view(Draft)

- As an individual-centered social infrastructure, individuals create their own digital IDs and control personal activity history data.
- However, at present, there are many undeveloped parts such as the mechanism of digital IDs and the response that individuals are all responsible for the use of their identities.



Ideal Future Social Infrastructures from a Medium-Term view(Draft)

- In the ideal social infrastructure from a long-term perspective, there are undeveloped issues.
- Therefore, while aiming for the ideal social infrastructure from a long-term perspective, first of all, it would be better to promote federated ID with eKYC by using already available technologies, and to develop ontology, data formats, privacy standards, etc. regarding digital certificates to be issued, stored, shared, and verified.
- Based on the above points, the following is an ideal future social infrastructure from a short- to medium-term perspective as a precedent to an ideal social infrastructure from a long-term perspective.



What to be required of the government and what to be promoted in the private sector

- Assuming the ideal future social infrastructure from a long-term perspective, the following could be considered as "what to be required of the government" and "what to be promoted in the private sector.“
- As a major premise, the lack of digitization of various certificates is also a bottleneck in building such a platform for personal activity history. It is hoped that both the public and private sectors will further promote digitalization.

Summary of the secretariat (draft)	
What to be required of the government	• Promotion of digitization of qualifications and certificates • Considering rules such as guidelines / policies and technical specifications • Examining eKYC/Digital ID mechanism and rules using Individual Number Card, etc. • Considering mechanism and rules to ensure the quality of activity history data such as qualifications • Bridging international federation of personal activity history data
What to be promoted in the private sector	• Promoting digitization of qualifications and certificates • To develop and implement socially functions to prove the authenticity of issuing qualifications • Establishing Identification Criteria with KeYC in mind • To develop and implement socially KYC/digital ID • Organizing and standardizing human resource information required by private companies and organizations • Arranging Ontology and occupational classification, and adjusting common understanding • To development and implement socially interoperable infrastructure that does not interfere with international cooperation • Handling thoroughly personal data in consideration of privacy