Trusted Web

Trusted Web White Paper Ver 2.0 Overview

Aug 2022

Secretariat of the Headquarters for Digital Market Competition,
the Cabinet Secretariat of Japan

1. Background and History of Study

○The digital transformation (DX) of society as a whole is accelerating with the outbreak of COVID-19. As **the cyber and physical spaces are merging**, the society is **transitioning to "digital society"**.

○However, various issues have surfaced. It is necessary to search for the third way that leads to neither "excessive dependence on a handful of giant companies" nor a "surveillance society."

○While **the Internet and the Web**, developed as the foundation of digital society, have data exchange protocols that are in place, **much of the data management, including identity management, depends on the services of platform operators.** As data is siloed, with little external verifiability, the situation allows no option but to believe in those platform operators.

○In light of this situation, the **"Trusted Web Promotion Council" was launched** in October 2020 in response to the June 2020 proposal presented in the "Report on the Medium-Term Vision on Competition in the Digital Market", with the scope to **realize Data Free Flow with Trust (DFFT)**. The council compiled the **white paper Ver. 1.0 in March 2021.**

○Subsequently, it conducted use case analysis and prototype development to elaborate the ideas and concepts presented in White Paper Ver. 1.0, and also identified challenges.

○ Based on the above, the council **compiled the White Paper Ver. 2.0 in July 2022** as a further road map for realizing Trusted Web**, which further fleshes out the trust framework that Trusted Web aims to achieve**, **presents the architecture** to realize it, and **discusses the governance** that should be in place.

2. Current Issues and Their Causes

○ **The Internet and the Web** were developed as **globally common infrastructure** enabling to widely access information and **creating various services**.

○ However, there is **no adequate mechanism** to **ensure trust relationships and sense of security in various social activities** in the digital society. While **users rely on platform operators for most of their trust, this distortion has created pain points.**

Examples of pain points

○**Concerns about data being exchanged,** due to such as fake news and false data controlling devices

○**Privacy risk** due to aggregation and consolidation of personal data, including biometric information

○**Balance between privacy and public interest**

○**The siloed industrial data** that is underutilized

○Concerns about the sustainability of the ecosystem **due to the winner-takes-it-all situation** etc.

○**Dysfunction of governance** using societal norms

Causes of pain points

There are concerns about :

○Whether the data being exchanged can be trusted

○Whether the party with whom the data is exchanged can be trusted

○Whether the other party's handling of the provided data can be trusted

While leveraging the benefits gained from **the Internet and the Web**, it is necessary to **add certain governance and operational mechanisms as well as functions that enable these mechanisms on the top.**

The key is "Trust"

3. Goal of Trusted Web

〇**Goal**: Build **a new trust framework for various social activities** in digital society and **enable various parties to create new values**

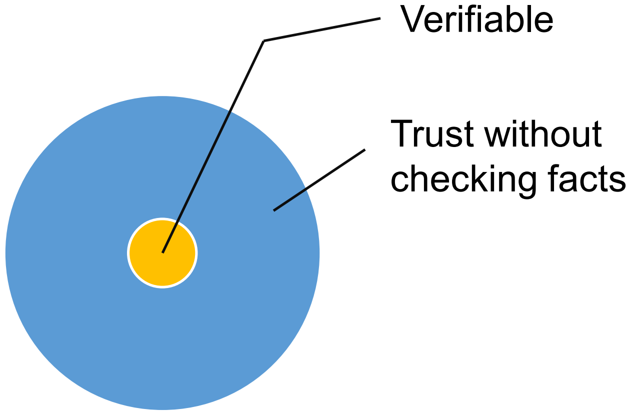
〇**New Trust framework: Without excessively relying on certain services:**

- Enables **users (individuals and organizations) to control the data related to themselves**
- **Incorporates mechanisms for** consensus building in data exchanges while also enabling to **trace the implementation of that consensus**
- **Expands the areas that can be verified, thereby increasing the level of Trust**

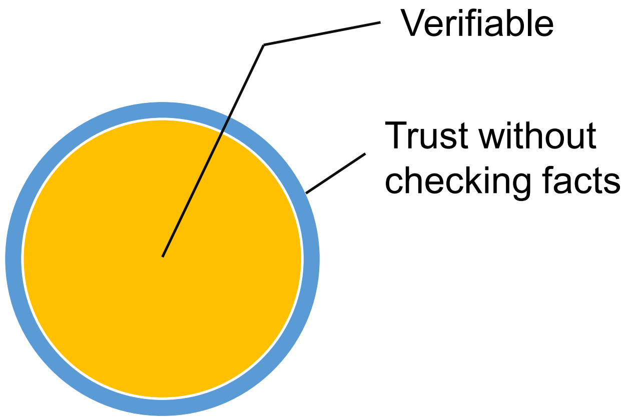
〇**Approach: Overlay approach** where benefits of the Internet and the Web are leveraged and functions are added on the top

*Trust: **The degree to which one believes that the other party behaves as expected without checking supporting facts to confirm the expectation**

Verifiable areas change depending on the mechanism applied

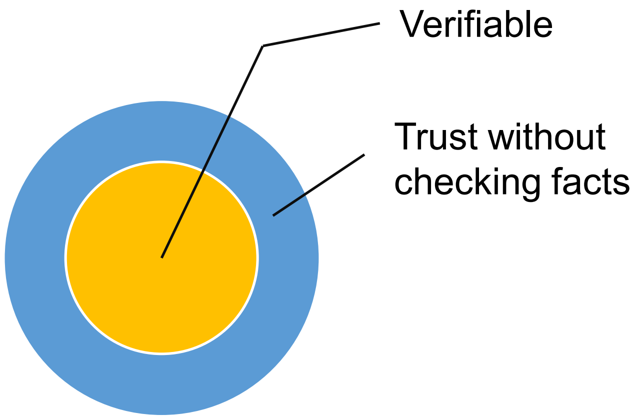


Current Internet:
As the verifiable portion is so small, decision making requires a great deal of trust in the other party.



Blockchain, etc.

*Taking into account tradeoffs related to the issues such as scalability, energy consumption, and ease of upgrading without relying on a certain technology, the circle on the right is the goal of Trusted Web



Goal of Trusted Web:
To expand the areas that can be verified, while satisfying continuity, interoperability and ease of upgrading
→ Increase the level of "Trust"

3. Trusted Web and “Web 3”

- The recently discussed “Web 3” and Trust Web **have commonalities** in that both share the **awareness over the issues** with the current Internet and Web, and that both **are oriented toward a distributed structure** and **aim to expand verifiable areas**. However, there are various views on the definition of **“Web 3,”** which we understand **have not yet reached to a consensus**.

- Trusted Web is a **technology-neutral initiative with an emphasis on identity management**. It aims to increase the level of trust not only through the use of blockchain technology but also through the use and combination of various technologies that increase verifiability.

- It is essential to incrementally build the infrastructure such as the Internet and the Web. In realizing Trusted Web, the initiative aims to create infrastructure for digital society with a higher level of trust while ensuring **Continuity** with the current Internet architecture, **Interoperability** with existing systems, and **Ease of Upgrading without excessively relying on certain technologies.**
  Also, as we move forward with the realization of Trusted Web, it is vital for us to consider **what kind of governance is needed for the digital infrastructure that Trusted Web is achieving**.

4. Benefits of Trusted Web

Benefits for businesses

- Establishment of a trust framework for data exchange through Trusted Web

  → **Essential for facilitating collaboration among businesses**, which is a prerequisite for **digital transformation (DX)** that **requires various entities' value co-creation** across organizational boundaries and sectors

Benefits for end users

- **Only the necessary data can be exchanged** through enhanced control over data
- With users' data aggregated under their control points, users can **use and share their data without involving platform operators, etc.**
- **Sense of security from enhanced verifiability of data** being exchanged

Importance for businesses to participate in realizing Trusted Web as digital infrastructure

- Businesses can **verify the values of their services** that operate on a newly built architecture → enabling quick **scale-up of their services** on new digital infrastructure
- **Working on the side of introducing new technologies and paradigms** can give them an advantage in future businesses

New Ways of Collaboration

- BUSINESSES can test services at the trial stage and, through providing the feedback from their test results, participate in the creation of digital infrastructure as a common asset
- ACADEMIA can contribute to designing of trust framework for digital infrastructure from a long-term perspective and collaborating with international communities related to web technologies
- GOVERNMENT facilitates discussions and activities of the initiative and coordinates a grand design of incentive structure

4. Examples of potential use cases leading to value creations by businesses

(1) Data exchange between parties without prior mutual trust relationships

- Supply chain management
  (e.g., Traceability for decarbonization, history of batteries equipped in a car, production forecasting and coordination in the agricultural sector, ordering and receiving processes, etc.)
- Transactions based on buyers' and sellers' mutual evaluation
  (e.g., Rebundling and sharing services of human resources and assets liquidated through DX or during COVID-19 pandemic, etc.)
- Data linkage across different industries such as mobility, tourism, disaster prevention/mitigation, etc.
  (e.g., Drone security and operation management, personal information management for overseas travelers, etc.)

(2) Sectors where verification costs are high or verification volume in paper or other form is large

- Finance and insurance (e.g., sharing of corporate financial and non-financial data, micropayments, etc.)
- Administrative procedures (e.g., SMEs' applications for subsidies, notices of death, etc.)

(3) Sectors where there is a high need of control by individuals and corporations

- Healthcare (e.g., utilization of vital data in drug prescriptions and clinical trials, sharing of health status from wearable devices, etc.)
- Digital contents (e.g., content copyright management, asset management in the metaverse, etc.)
- Digital advertising (e.g., post-cookie consent schemes, etc.)

(4) Sectors with large amounts of personal data where further use of data is expected

- Railways, airlines and other infrastructure operators, and retailers
- Local governments

5. Use case study

After the release of White Paper ver.1.0, in order to identify issues related to the four functions proposed in it, the following three use cases were studied and a prototype was developed based on one of the use cases.

(1) Case of “Individuals” exchanging their attributes ⇒ used for developing a prototype

・Studied the handling of personal attributes during job search

[Pain Points] Control over the recipients and scope of disclosure of personal attributes
Verifiability of personal attributes provided

[Issues to Consider] **Need to reorganize the four functions** proposed in ver. 1.0 white paper from **the perspective of implementation**
Need to consider how to implement the **trace function**

(2) Case of “Businesses” exchanging data with administrative agencies (application for subsidies)

・Studied the exchange of data provided to apply for the Business Restructuring Subsidies, which support businesses suffering from COVID-19 circumstances.

[Pain Points] Burden on the businesses associated with the application
Burden on the agencies to verify provided data by applicants

[Issues to Consider] Need to reorganize the required functions for verification, given that there are **various types of verification for actual submission of documents and verification for their contents.**
Need to expand **verifiability in a way that does not rely on the existing trust between entities**

(3) Case of “Supply Chain” exchanging data on chemical substance

・ Studied the exchange of data in supply chains to comply with Chemical Substances Control Law

[Pain Points] Controls over the recipients and scope of disclosure of data related to know-how including trade secrets
Verifiability of data provided

[Issues to Consider] Need for a framework that **ensures data reliability but limits the scope of disclosure** in consideration of trade secrets, etc., when **data is processed and transmitted** among multiple parties

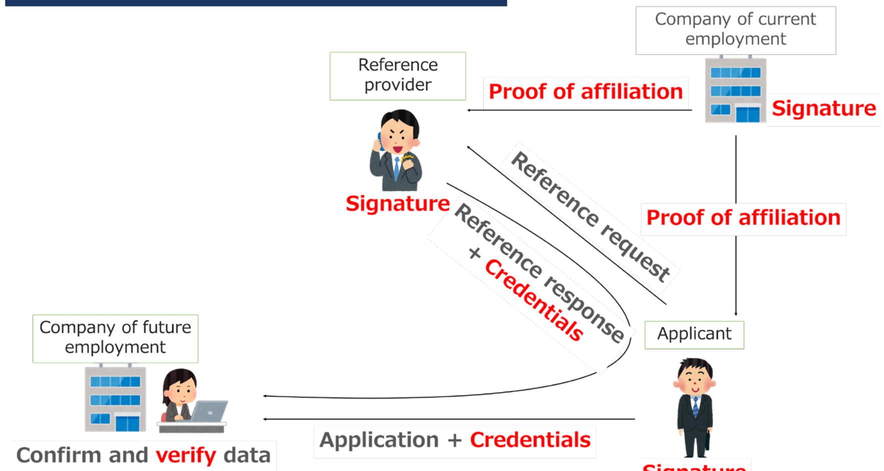
5. Prototype Implementation

Four functions proposed in White Paper ver.1.0 were implemented on a browser base to exchange personal attributes on such as skills and achievements when users search jobs. Users' control over sending and receiving verified data was realized using decentralized identifiers (DIDs) and verifiable credentials (VC).

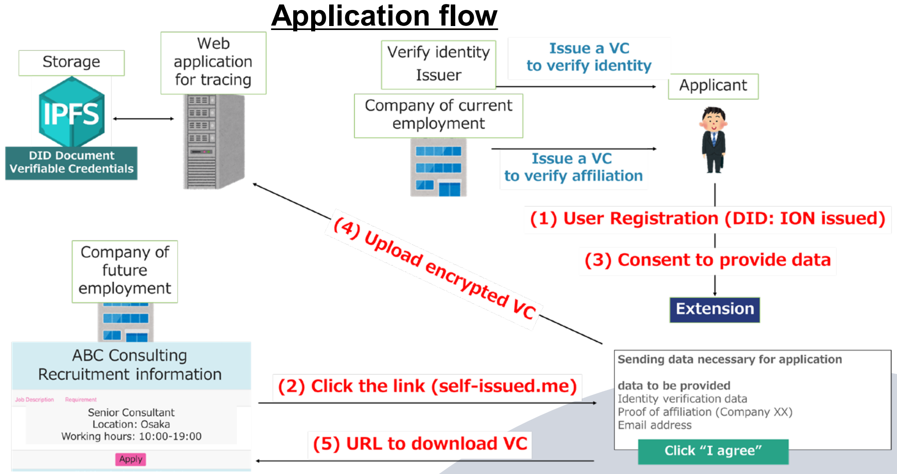
■ Four "Trusted Web" functions implemented in the prototype

Repository of the prototype developed: https://github.com/TrustedWebPromotionCouncil/

Identifier management	The prototype was designed to allow users to freely issue DIDs and link necessary data to the DIDs
Trustable communication	The prototype created VCs in a format that allowed decryption only upon receipt of data and it could be verified whether the signature was provided by the issuer
Dynamic consent	It allows data providers to select necessary data by themselves and to provide it at their own discretion
Trace	It enables users to check who has accessed the data users provided and when



Signature



Application flow
Storage
IPFS
DID Document
Verifiable Credentials
Web application for tracing
Verify identity Issuer
Issue a VC to verify identity
Applicant
Company of current employment
Issue a VC to verify affiliation
(1) User Registration (DID: ION issued)
(3) Consent to provide data
Extension
(4) Upload encrypted VC
Company of future employment
(2) Click the link (self-issued.me)
(5) URL to download VC
Job Description
Requirement
Apply
Click "I agree"

ABC Consulting
Recruitment information

Senior Consultant
Location: Osaka
Working hours: 10:00-19:00

Sending data necessary for application

data to be provided
Identity verification data
Proof of affiliation (Company XX)
Email address

Source: [5. Peer Review] "Status of Prototype Development Study" by Yuichi Ota and Shigeya Suzuki https://www.youtube.com/watch?v=BABYKkcSjg0

■ Major issues identified

- ✓ How to create a user interface that conveys the value that DIDs and VCs bring, even to those who have no idea how they work
- ✓ As the data was stored in the Inter Planetary File System (IPFS), download history was not kept, making tracing impossible (in order to enable to trace the access, we set up the centralized server for authentication, authorization and access recording, but there was still a possibility to be bypassed)
- ✓ The public key of the issuer of a VC to verify the identity and a VC to verify the affiliation must be published
- ✓ The secret key was lost when the browser extension was removed (we adopted HDWallet, but it was hard to remember 12 different words)

DID: Decentralized identifier. Individuals and organizations generate their own identifiers. It helps users to identify themselves or the data they manage while controlling the scope of disclosure of their personal attributes, etc., and decoupled from centralized registries.
VC: Verifiable attributes. In this framework, attributes can be certified by the issuer.

5. Summary of Issues identified from use cases and prototype implementation

○Functions need to be reorganized, e.g. whether it should be “trustable communication function” or “trace function”

→ Need to reorganize the interrelationship of the four functions proposed in Ver.1.0, taking into account their implementation

○The analysis of the three use cases identified the following issues to design the architecture of Trusted Web

✓ **Trust & Verifiability**

“Expanding verifiable areas”, an element of the new trust framework, is designed to be achieved with a focus on digital signatures

✓ **Data**

Data needs to be organized from the viewpoint of verifiability

✓ **Entity**

While many existing models of trust rely on trust between entities, it needs to ensure verifiability without relying on trust relationships between entities
(e.g., Data from financial institutions is provided via SMEs, etc., in the case of “Businesses” exchanging data with administrative agencies)

✓ **Identity & Visibility**

An identity may belong to multiple groups, but the visibility of such belonging varies depending on cases, such as a case where the group has no means of knowing the other group’s members or its existence. In addition, there may be constraints on the verifiable data that can be shared among the groups. These issues must be addressed.
(e.g., Relationship between downstream and upstream companies in the supply chain use case)

✓ **Transport**

In increasing the verifiability of communication, from the viewpoints of delimiting communications to the unit where its sender and receiver are verifiable and of achieving consensus among communicating parties, it is effective to use message-oriented services as the foundation and to record the individual contents of all multiple messages and identities

✓ **Data Storage location**

If the transport is composed of message-oriented services, each participant can individually record and manage its data exchanges on a message-by-message basis; there is no need to delegate this to a third party.
In terms of data storage location, Wallet can be one of the prospective means of implementation.

6. Trust framework that Trusted Web aims to achieve

Based on the use case studies and the prototype implementation, we have organized **the picture of Trust framework that Trusted Web aims to achieve**. With this picture in mind, we propose the basic design of **verifiable data model and verifiable communication model with high interoperability** as the "**architecture**" of Trusted Web.

a. Identity management

・Entities manage their own identities by using an externally linked identity management system*

b. Trust and data verification

・The fundamental value of Trusted Web is “to increase the level of trust through the expansion of verifiable areas of data”

c. Data covered by Trusted Web

・Created data and the process of data exchange are in scope

- Created data: Verifiability is ensured by digital signature technology
- Process of data exchange: Verifiability is ensured by modeling data exchanges and combining it with digital signature

d. Expansion of verifiable areas

・ The entire data set, including the signature, can be verified by i) verifying “the signature itself”, ii) verifying “the signer”, and iii) clarifying “the intent of the signature”

- Clarifying “the intent of the signature” refers to the state in which the function satisfied by the signature to achieve the purpose has been specified with data exchange framework agreed beforehand

Examples of the framework in which “the intent of the signature” is clarified:

Signatures are signed in accordance with the intent designed in the protocol (e.g., X.509 certificate, DNSSEC, etc.)

Signatures on data for digitized certification (e.g., Verifiable Credentials)

e. Modeling of data exchanges

・Data exchange is modelled in the form of messages and transactions

・The data exchange processes (orders, content, actually received or not, etc.) are mutually recorded

→ Ensures data transfer and enables to verify afterwards that the data exchange actually took place

f. Need to combine protocols

・ An architecture with a high degree of flexibility to combine standards and protocols is essential

* Implementations can adopt OpenID and other standard-based systems, and technologies such as DID/VC.

6. Four Functions in Ver.1.0 Reorganized into Six Components

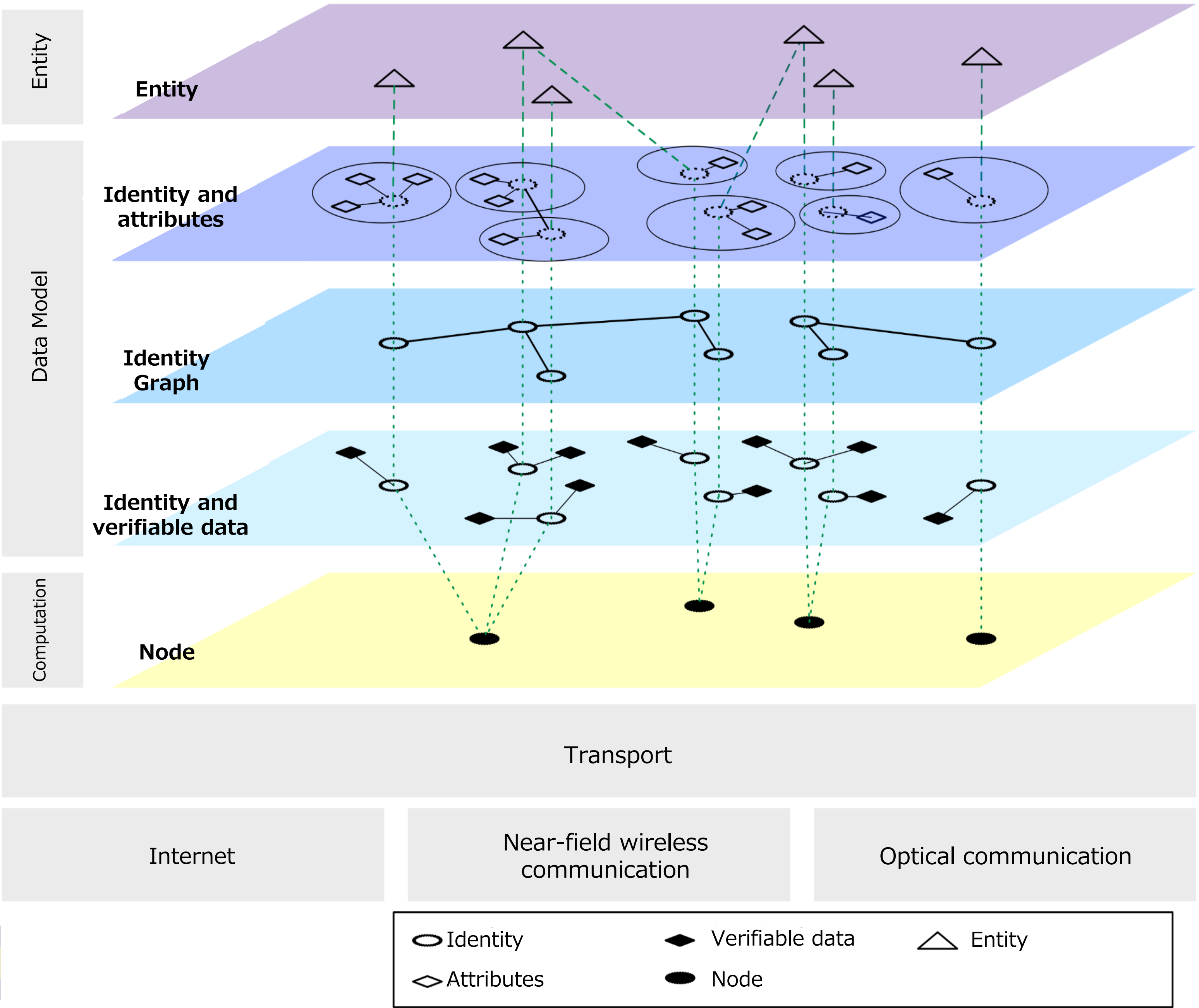
The four functions presented in Ver.1.0 were reorganized into **six components**;
- four components from a data-centric perspective: **Verifiable data**, **Identity**, **Message**, and **Transaction**
- two components from the perspective of computational resources and communication: **Node** and **Transport**

Function

- **Identifier Management**
- **Trustable Communication**
- **Dynamic Consent**
- **Trace**

Component	Description
Verifiable Data	Trusted Web **designs the operation** of verifiable data. The whole data set, including the signature, can be verified by **i) verifying "the signature itself", ii) verifying "the signer", and iii) clarifying "the intent of the signature".**
Identity	A type of **verifiable data**. It is composed of **attributes** (e.g., name of the affiliated organization). To make data verifiable, it must be linked to the signature information associated with its identity. Verifiability of data is enhanced by enabling references to the **identity graph that indicates the relationship between identities**
Node	Manages the **transmission/reception of messages**. It **performs computational processes (e.g., consensus building) upon receipt.** Nodes **record transactions** and **store the records** linked to identities.
Message	Transmitted as a **one-way message** with certainty of delivery from source to destination. **Messages are the data exchanged between nodes, and message exchanges** are implemented in the nodes.
Transaction	The data and framework that allow **the sequence of message transmission** to be confirmed between nodes. It aims to ensure that the same records are kept at all nodes **in a distributed manner.** This enables to confidentially share only among the concerned parties **without relying on external records.**
Transport	Provides **an appropriate means of sending messages** to other nodes. It is required to design ~~**a**~~ **comprehensive-communication model** to make it possible to use the various technologies (e.g., Internet, proximity wireless communication, etc.).

6. Architecture for Trusted Web



Entities indicate subjects such as individuals and organizations
(e.g. job seeker, reference provider, company of future employment, etc.)

An entity has multiple identities
(e.g. job seeker's identity as an employee, etc.)
Identity is composed of attributes
(e.g. employment date, date of birth, etc., of the job seeker)

Identity graph shows relationships among identities
NOTE: In reality, the visible range in the graphs differs depending on the identity
(e.g. there is a direct relationship between the job seeker and the reference provider as both are employees of the same company)

Verifiable data is considered to be linked to identity because data becomes verifiable after being signed by the identity
(Examples of verifiable data: job seeker's work experience, etc.)

Nodes manage transmission/reception of messages on behalf of identities.
Nodes perform various computational processes as messages are sent and received

It is effective to use message-oriented services as the foundation of transport
Design a comprehensive communication model to make it possible to use various technologies

Note:
It should be noted that the above examples could be expressed in various ways depending on the case.

6. Components of the architecture for Trusted Web

Data models and operations for the six components are defined.

Verifiable Data

- Data model
  - Components of verifiable data
  - Data components involved in advanced data processing
- Operations for verifiable data
  - Creation of verifiable data
  - Verification of signature itself
  - Verification of signers
- Advanced data processing

Identity

- Data model
  - Single identity
  - Identity Graph
- Operations for identity
  - Signature (when identity is under control)
  - Discovery
  - Data acquisition to verify the signature itself
  - Data acquisition to verify the signer
  - Advanced data processing
- Operations for Identity Graph
  - Adding relationships among identities
  - Deleting relationships among identities
  - Updating relationships among identities
  - Finding paths
  - Evaluating verifiability of the path

Node

- Data model
- Node operations
  - Message transmission/reception operations
  - Transaction operations
  - Actions (consensus building, etc.)

Message

- Data model
- Message operations
  - Creating messages
  - Verifying messages

Transaction

- Data model
- Transaction operations
  - Starting transactions
  - Ending transactions
  - Verifying transactions

Transport

- (Details to be discussed in the future)

6. Component: Verifiable Data

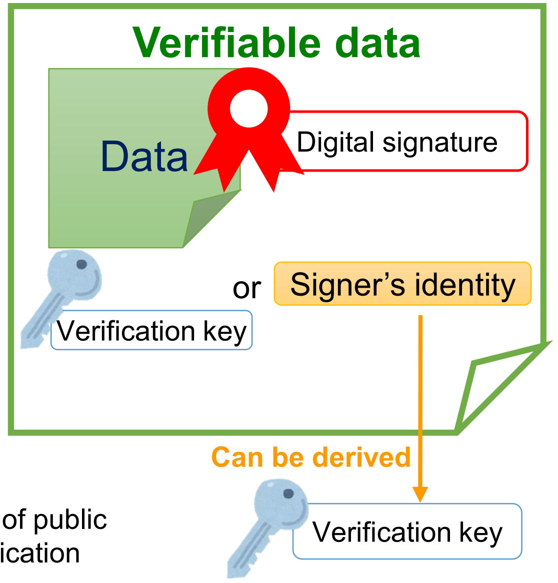
Model of Verifiable Data

- Data
- Digital signature on data
- Verification key*

  or

  Identity from which the verification key can be derived
- Intent of the signature (in the case that the intent can be indicated as data)

*The White Paper Ver.2.0 describes the key pair of public key cryptography with the public key as the "verification key" and the private key as the "signing key."



Verifiable data

Data

Digital signature

Verification key

or

Signer's identity

Can be derived

Verification key

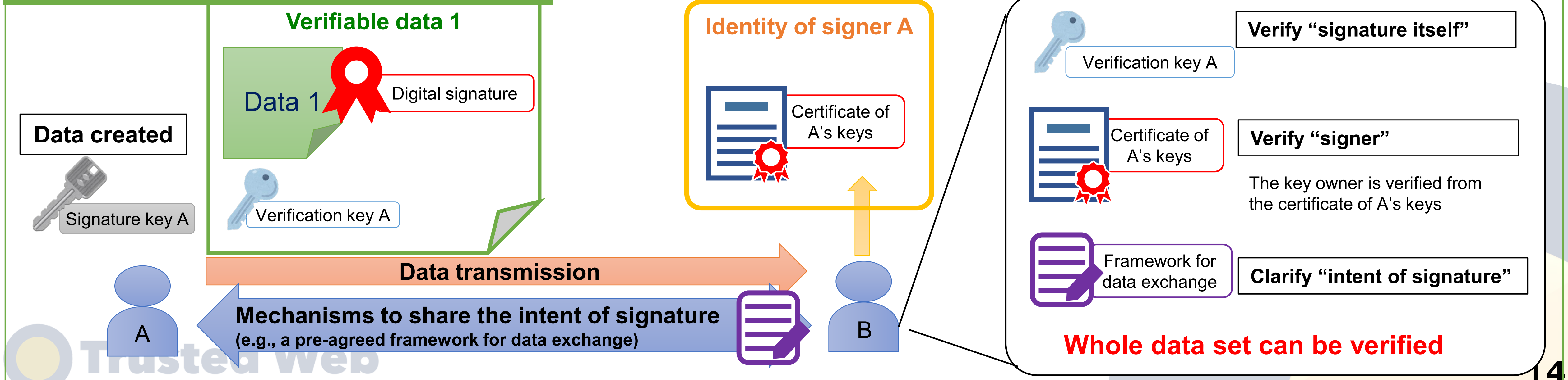
Advanced Data Processing

- Advanced cryptographic processing methods such as zero-knowledge proof*1 and secure computation*2 have been proposed.
- These processing methods can be introduced for verifiable data, but from an architectural perspective they are recognized to be combined with the identity operations as well.

*1 e.g. Without revealing her password, a certain person can prove that she knows the password

*2 Technology that enables various types of analysis while keeping data encrypted

Example of Operations on Verifiable Data



Data created

Signature key A

Verifiable data 1

Data 1

Digital signature

Verification key A

Data transmission

Mechanisms to share the intent of signature (e.g., a pre-agreed framework for data exchange)

A

B

Identity of signer A

Certificate of A's keys

Verification key A

Verify "signature itself"

Certificate of A's keys

Verify "signer"

The key owner is verified from the certificate of A's keys

Framework for data exchange

Clarify "intent of signature"

Whole data set can be verified

6. Component: Identity

Data Model of Identity

- Attributes of digital signatures
- Other attributes

Data Model of Identity Graph

A graph with identities as nodal points and one-to-one relationships as lines. Each identity manages its identity graph.

- Identity
- Data to identify the two identities (e.g. identifier)
- Data showing relationships among identities

Operations on Identity

i. Signature:

It is possible to sign with a signature key that is linked to the identity, meaning that it is possible to sign with that identity. Certain operations are required to the identity to enable this signing

ii. Discovery:

Identities need to be discoverable by some means

iii. Data acquisition to verify the signature itself:

Verifying a digital signature signed with the identity requires a key that is linked to that identity (verification key)

iv. Data acquisition to verify the signer:

To verify the signer, it is necessary to identify and verify the owner of the signature key from the verification key

v. Advanced data processing:

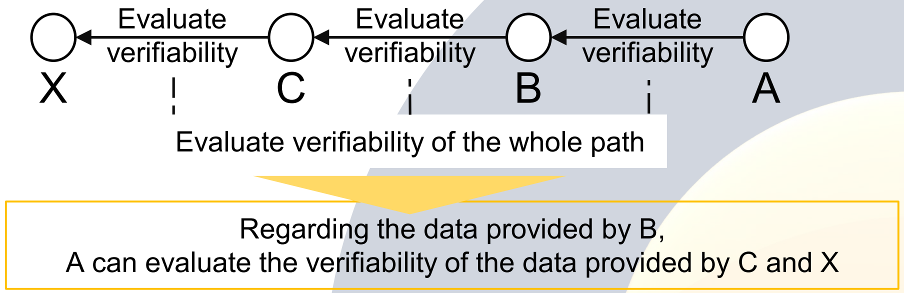
If advanced encryption technologies are implemented, operations related to these are expected to be implemented

Operations on Identity Graphs

i. Adding relationships among identities
ii. Deleting relationships among identities
iii. Updating relationships among identities
iv. Finding paths
v. Evaluating verifiability of the paths

- The graph allows tracing to the identity that signed the signature to the data to be verified. The combination of the nodal points and lines that enables tracing is called a "path."

- By evaluating the verifiability of the lines constituting a path, the verifiability of the whole path can be evaluated, eventually enabling the evaluation of verifiability of data provided by the identity that is the endpoint of tracing.



Regarding the data provided by B,
A can evaluate the verifiability of the data provided by C and X

6. Components: Node, Message, Transaction, Transport

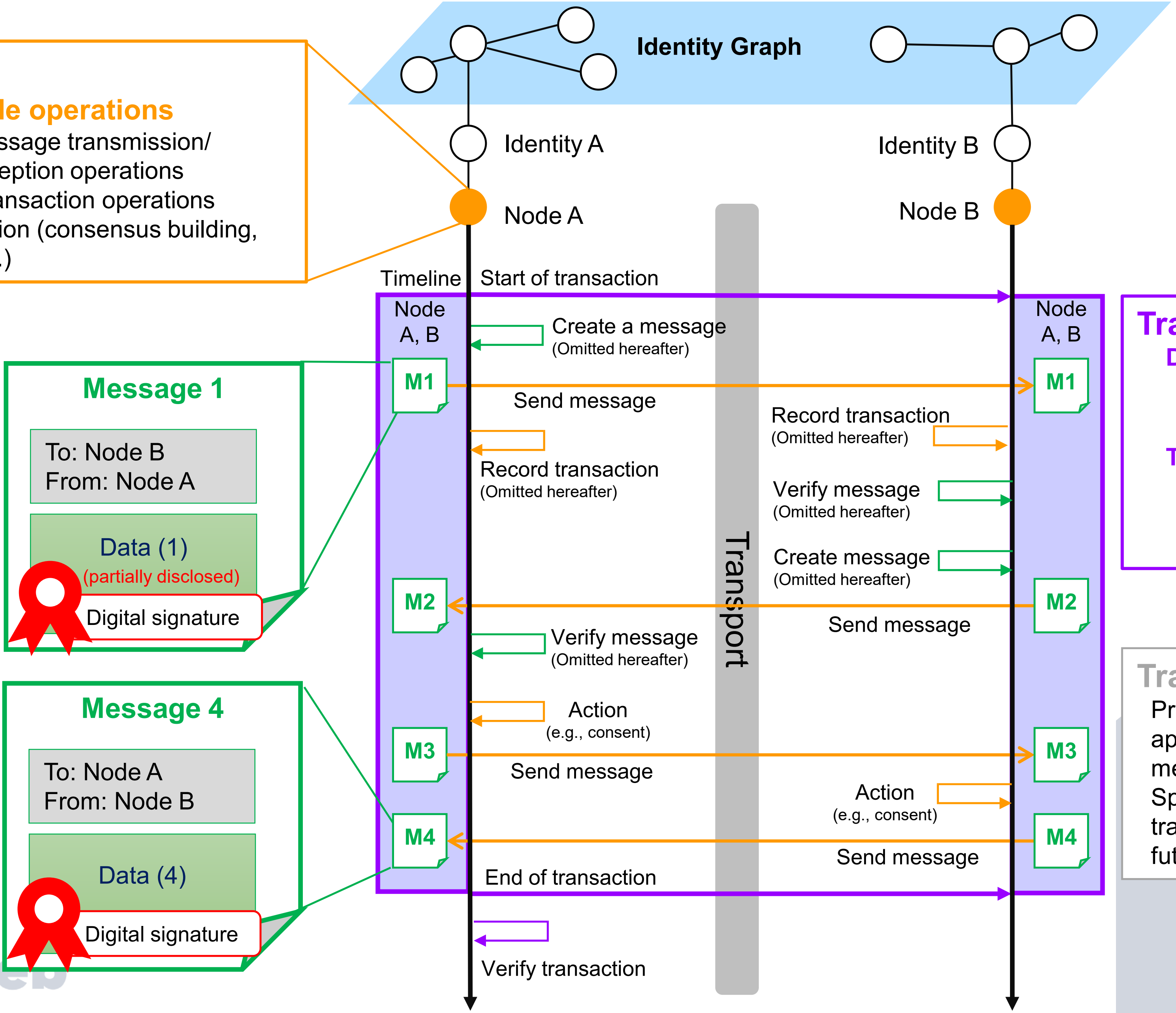
Node

Data model

- Node identifier
- Identity
- Identity Graph
- Transaction record
- Action

Node operations

- Message transmission/ reception operations
- Transaction operations
- Action (consensus building, etc.)



Message

Data model

- Header
  - Destination node identifier
  - Source node identifier
- Payload
  - Data to be sent
- Signature by sender

Message operations

- Creating messages
- Verifying messages

Transaction

Data model

- Participating nodes
- Message exchanged

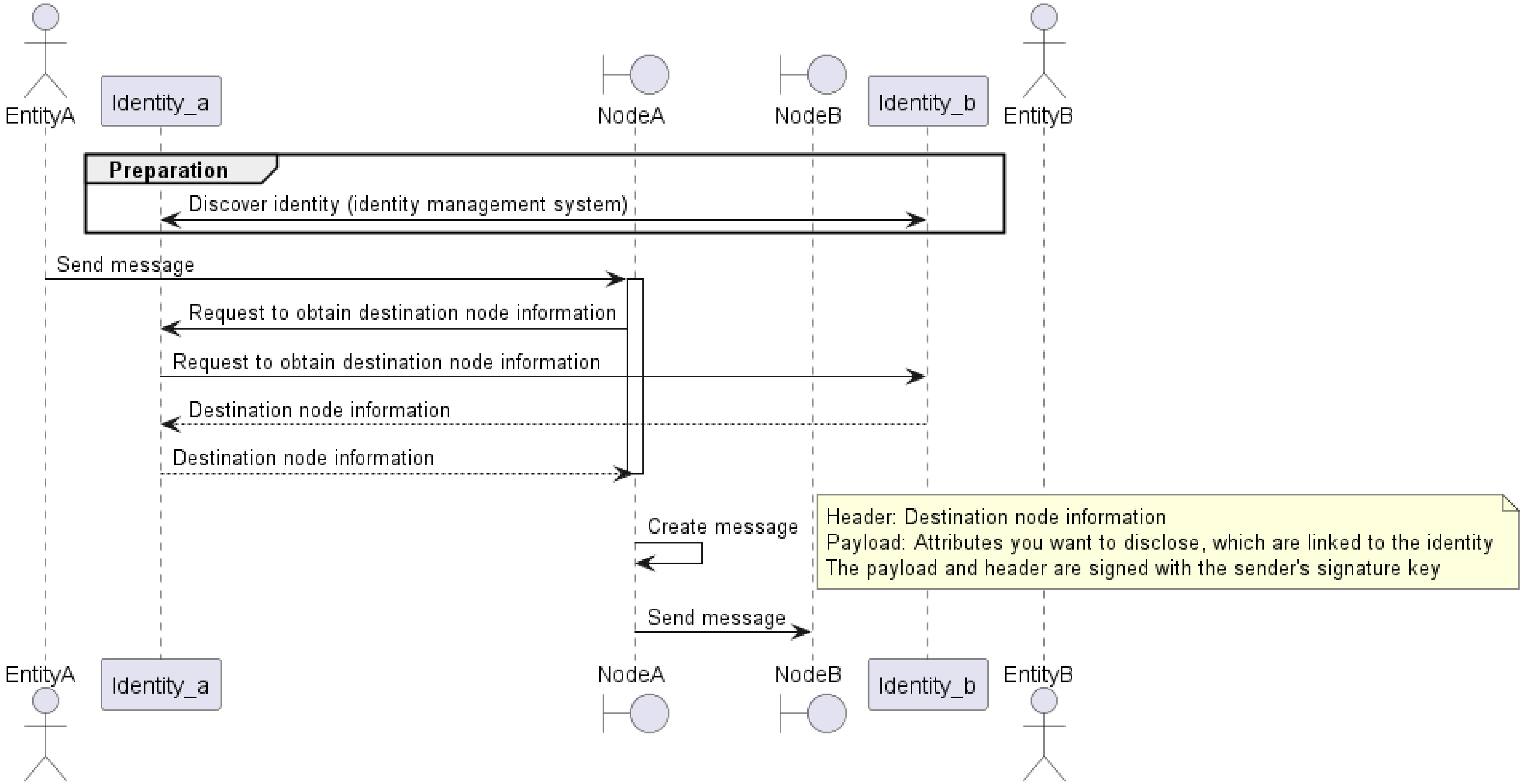
Transaction operations

- Start of transaction
- End of transaction
- Verification of transaction

Transport

Provides nodes with an appropriate means to send messages to other nodes. Specific implementation of transport will be discussed in the future

6. Workflow diagram to enable users (individuals and organizations) to control their data related to themselves



Discover identity (identity management system)

Send message

Request to obtain destination node information

Request to obtain destination node information

Destination node information

Destination node information

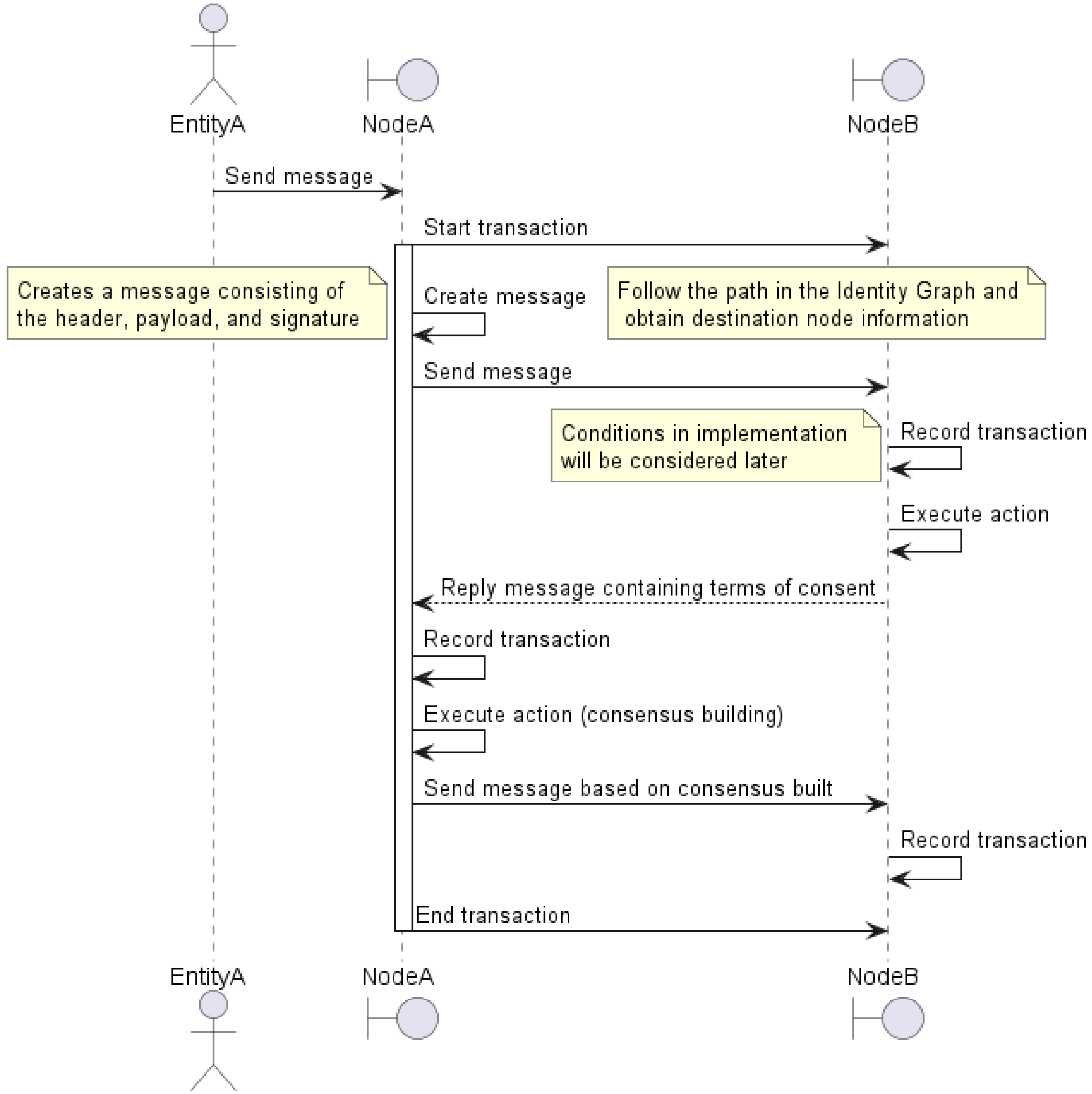
Create message

Header: Destination node information
Payload: Attributes you want to disclose, which are linked to the identity
The payload and header are signed with the sender's signature key

Send message

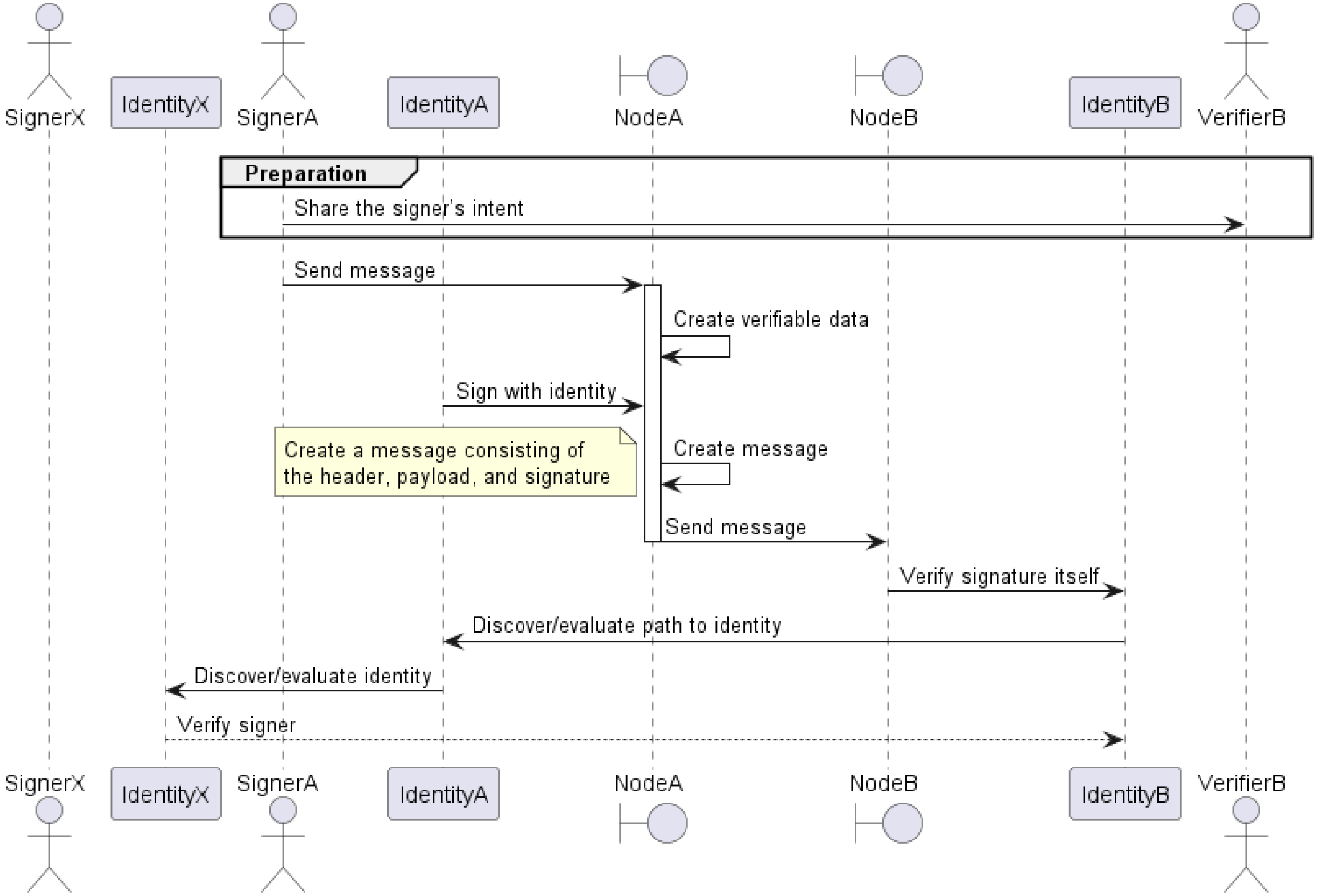
- [Identity]: Through an identity management system, etc., both parties discover the other party’s identity already created in advance
- [Message]: Create a message consisting of a header, payload, and signature
  - Header is the destination node information obtained by following the path in the Identity Graph
  - Payload is the attributes you want to disclose and is linked to the identity
  - Signature is verifiable data
- Messages are sent and received by operations at the [Node]

6. Workflow Diagram to incorporate mechanisms for consensus building in data exchanges while also enabling to trace the implementation of that consensus


EntityA
NodeA
NodeB
Send message
Start transaction
Creates a message consisting of the header, payload, and signature
Create message
Follow the path in the Identity Graph and obtain destination node information
Send message
Conditions in implementation will be considered later
Record transaction
Execute action
Reply message containing terms of consent
Record transaction
Execute action (consensus building)
Send message based on consensus built
Record transaction
End transaction
EntityA
NodeA
NodeB

- [Message]: Create a message consisting of the header, payload, and signature
  - The header is destination node information obtained by following the path in Identity Graph
  - Payload is the terms of consent (scope and period of disclosure, etc.)
  - Payload and the entire header are signed with the sender's signature key, making it a signature to the message
- Start [Transaction]
- Send and receive messages by operating at the [Node]
- Execute an action to build consensus for the message received at the [Node]
- [Node]: Record the messages sent and received sequentially. The records compose a transaction.
- [Node]: Each sending or receiving node records transactions sequentially as messages are sent or received
- End [Transaction]
- Verify [Transaction]

6. Workflow Diagram to expand the areas that can be verified, thereby increasing the level of Trust



- [Verifiable data]: Create verifiable data
- [Verifiable data]: Utilize a mechanism whereby the intent of the signature is shared between the signer and the verifier
- [Identity]: Sign with identity
- [Message]: Create a message consisting of the header, payload, and signature
- [Node]: Send verifiable data as a message
- [Node]: Receive verifiable data as a message
- [Identity]: Discover the path in the Identity Graph
- [Identity]: Evaluate verifiability from the path in the Identity Graph
- [Identity]: Discover the identity
- [Identity]: Obtain data for verification of the signature itself
- [Identity]: Obtain data for verification of the signer
- [Verifiable data/message]: Verify the message

6. Overlay approach and roadmap to realization

Through the overlay approach the initiative aims to implement Trusted Web as an architecture of the session layer and above*.

*To improve communication efficiency the transport layer may also be considered.

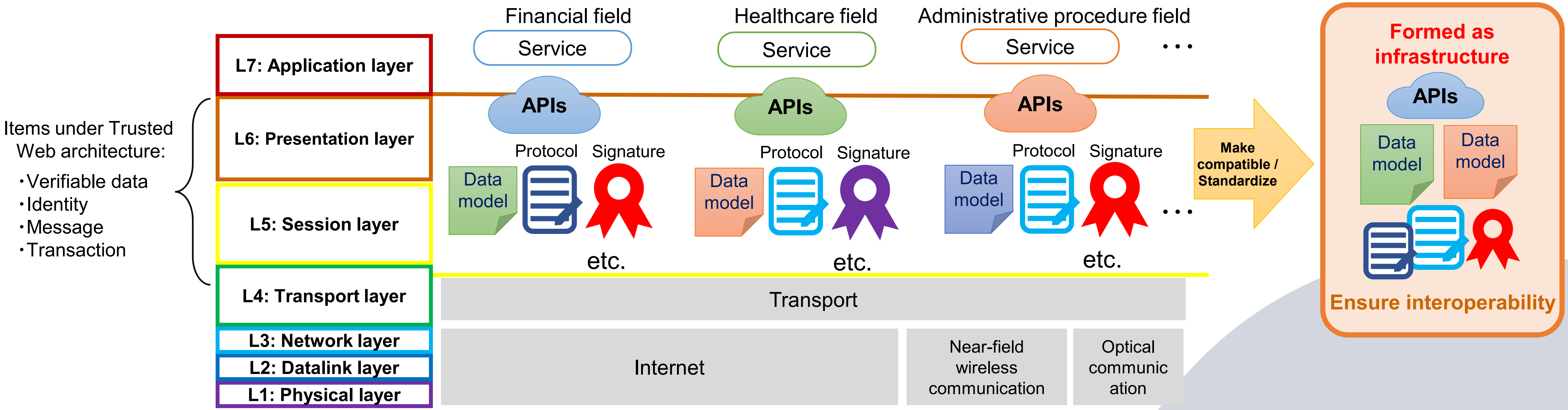
A potential scenario of the roadmap for the realization of Trusted Web

Various services that embody the functions Trusted Web aims at are provided, and their areas of use (fields) would expand

→ **A kind of middleware would be formed** between the transport and the layer of individual services

→ In the middleware, **APIs, data models, and protocols that should be compatible would be identified**, such compatibility ensures **interoperability**, leading to **standardization**

→ **Trusted Web as infrastructure would be formed.** Trusted Web would be realized though obtaining feedbacks across various services.



With the release of ver. 2.0, we **started collecting use cases** from the private sector in various fields.
Through the use case studies and implementation, we will present the benefits of Trusted Web to stakeholders in various fields and **obtain feedback on challenges and improvements to the architecture, etc.**

7. Governance

Challenge: What structure should be in place for the governance of the newly added trust framework as infrastructure?

<Basic ideas>

- Explore the governance structure suitable for Trusted Web as a common asset

・Factors such as network effects, increasing return, and decreasing costs in digital business can easily lead to monopolies and oligopolies, and lock-in effects are likely to occur.

→ In building a new trust framework in digital infrastructure, it is essential to consider a governance structure suitable for a common asset to avoid excessive reliance on certain corporate activities in order to prevent the reoccurrence of pain points seen today.

- ✓ Therefore, global and technology-neutral Internet governance should be applied mutatis mutandis.
- ✓ It is important to involve various stakeholders in standardization, implementation, operation, community formation, and other activities.

- Importance of governance in its use

・Trusted Web aims to provide functions globally and in a technology-neutral manner as a technological foundation (infrastructure).
On the other hand, applications provided on Trusted Web will also be in harmony, as necessary, with trust mechanisms composed of existing legal systems and business practices of each country.

<Key concepts guiding the governance>

a. Multi-stakeholder oriented

The various pathways and their chains underpinning the trust are supported cooperatively by various stakeholders in a distributed manner, forming the Trust as a whole system.

Through the consensus building of various stakeholders, a sustainable governance is put in place to ensure the whole system is functioning.

b. Redefine the role of government Play role of a trust anchor; develop the rules to support digital social activities, etc.

c. Transparency, traceability, and auditability

Aim to prevent malicious players from undermining the Trust of the entire system by recording the process, results, and consequences of consensus building, and making them verifiable to allow verification and check by various stakeholders

d. Incentive design to make the ecosystem sustainable

Need to consider some kind of incentive for those who play a role in building and operating the common asset

8. Next steps (FY2022)

Creation of use cases

- Collect about 10 use cases in various fields through the “Trusted Web Joint Development Project”
- Identify further challenges through feedback and reviews as the use case development progresses
- Encourage engineers to come up with ideas actively based on the use cases developed or being developed

Community formation

- Form and activate a community through the launch and operation of a website and further use of GitHub
- Utilizing GitHub, encourage independent modification and implementation of the prototype developed last year, obtain feedback, and update
- Utilizing the issue function of GitHub, constantly update technical revisions (assuming active involvement of engineers and other stakeholders related to each of the above use cases)

Overseas cooperation

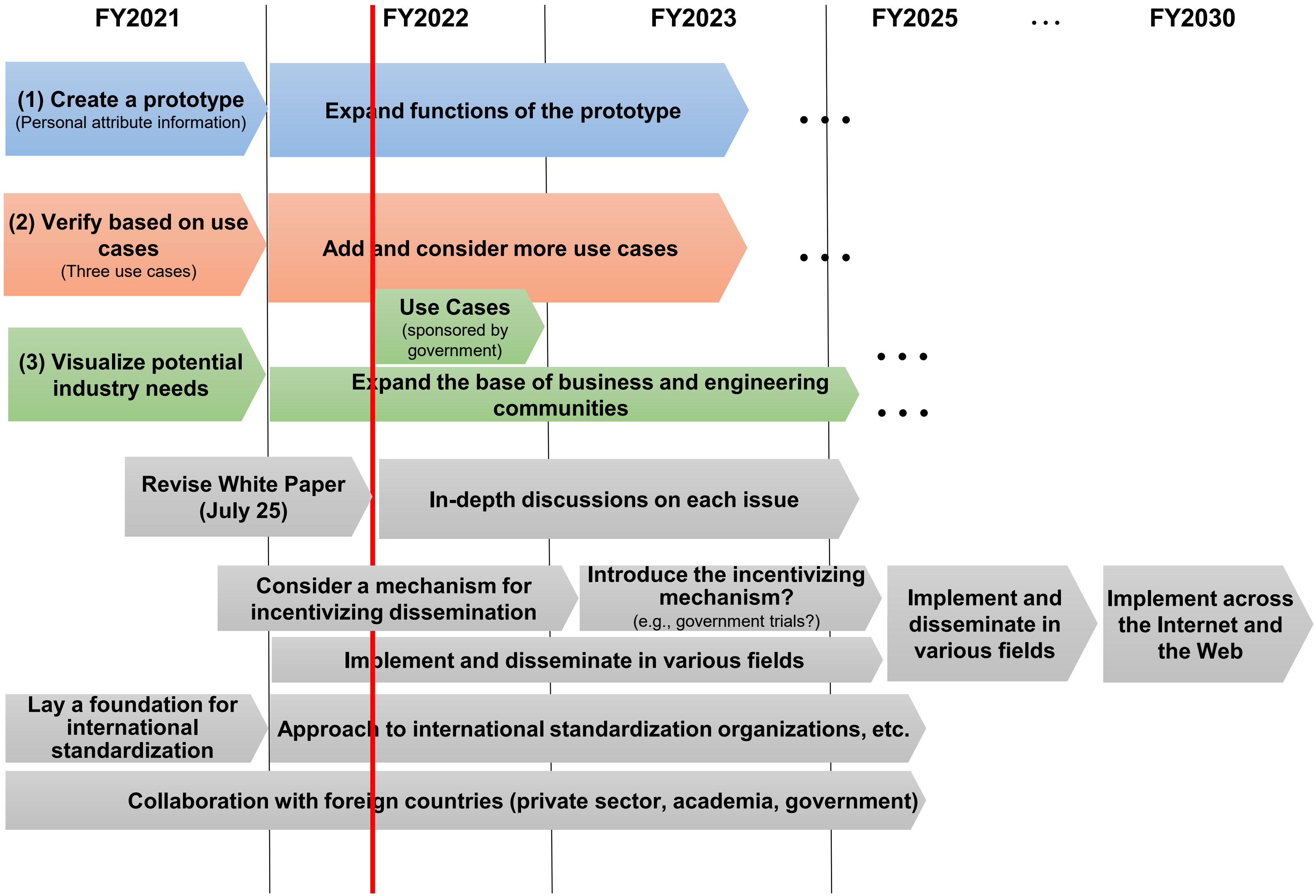
- Discuss the direction of international standardization (e.g., which organizations to approach and for what purpose, etc.) in light of the progress in the use cases, and make an approach to international standardization organizations and those that build consensus for international standards
- Exchange information and continue to build a network with overseas government agencies such as the EU that work on similar initiatives

Overall

- Disseminate information on the status of this year’s initiatives (including presentation of the above use cases) by holding events, etc., as in the previous fiscal year
- Update to “White Paper Ver.3.0”

The trust framework and architecture presented here that Trusted Web aims to achieve are only proposals at this point. We will continue to work toward realizing Trusted Web **by obtaining feedback from and having dialogues with a wide range of interested parties in Japan and abroad.**

8. Mid-term Strategy Toward 2030 (conceptual diagram)



FY2021 | FY2022 | FY2023 | FY2025 | … | FY2030

(1) Create a prototype (Personal attribute information) → **Expand functions of the prototype** → • • •

(2) Verify based on use cases (Three use cases) → **Add and consider more use cases** → • • •

Use Cases (sponsored by government) → • • •

(3) Visualize potential industry needs → **Expand the base of business and engineering communities** → • • •

Revise White Paper (July 25) → **In-depth discussions on each issue**

Consider a mechanism for incentivizing dissemination → **Introduce the incentivizing mechanism?** (e.g., government trials?) → **Implement and disseminate in various fields** → **Implement across the Internet and the Web**

Implement and disseminate in various fields

Lay a foundation for international standardization → **Approach to international standardization organizations, etc.**

Collaboration with foreign countries (private sector, academia, government)

<Result of FY2021 activities>

- Create something simple that works

→ Implement the prototype

- Further consider function, governance, etc.

→ Revise the White Paper

- Lay foundation for international standardization

→ Conduct a survey for the international standardization of Trusted Web

Trusted Web Promotion Council – List of Members

（As of August 15, 2022）

Koki Uchiyama	CEO of hottolink Inc. and CEO of Socialgist
Shinichi Urakawa	Chair, Sub-committee on Digital Economy, Keidanren/ Director, Senior Managing Executive Officer and CIO, Sompo Japan Insurance Inc.
Yuichi Ota	Founder and CEO of DataSign Inc.
Tatsuya Kurosaka	President and CEO, Kuwadate Incorporated
Nat Sakimura	Executive Fellow, Tokyo Digital Ideas, Co., Ltd.
Seiko Shirasaka	Professor, Graduate School of System Design and Management, Keio University
Haruo Takeda,	Corporate Chief Engineer, Hitachi, Ltd.
Hiroshi Tsuda,	Fellow, SVP, Head of Data & Security Research Laboratory , Fujitsu Limited
Yusuke Tomimoto	Deputy Chief Officer, Innovation Division, TOYOTA FINANCIAL SERVICES CORPORATION
HASIDA Koiti	Professor, Graduate School of Information Science and Technology, The University of Tokyo
Takanori Fujita	Project Lead for Healthcare Data Policy World Economic Forum, Centre for the Fourth Industrial Revolution Japan
Masakazu Masujima	Partner, Mori Hamada & Matsumoto
Shin'ichiro Matsuo	Research Professor, Computer Science Department, Georgetown University / Head of blockchain research, NTT Research Inc.
Kazuyoshi Mishima	Co-Founder & COO, Keychain
○Jun Murai	Distinguished Professor,Keio University
Kristina Yasuda	Microsoft Corp. Identity Standards Architect

（○: Chairperson）

Observers: Digital Agency, Ministry of Internal Affairs and Communication, Ministry of Economy, Trade, and Industry, National Institute of Information and Communications Technology (NICT), Information-technology Promotion Agency (IPA)

Trusted Web Promotion Council Task Force – List of Members

（As of August 15, 2022）

Tomoya Asai	Chief Technology Officer, WebDINO Japan
Hirochika Asai	Senior Researcher, VP of Infrastructure Strategy, Preferred Networks, Inc.
Daichi Iwata	Executive Business Producer, Enterprise Business Unit, NEC Corporation
Koki Uchiyama	CEO of hottolink Inc. and CEO of Socialgist
Masakazu Kikuchi	Secured Finance Co-founder & CEO
○Tatsuya Kurosaka	President and CEO, Kuwadate Incorporated
Kazue Sako	Professor, Department of Computer Science and Engineering, Waseda University
Shigeya Suzuki	Project Professor, Graduate School of Media and Governance, Keio University
Naohiro Fujie	Chairman, OpenID Foundation Japan
Shin'ichiro Matsuo	Research Professor, Computer Science Department, Georgetown University / Head of blockchain research, NTT Research Inc.
Sota Watanabe	Stake Technologies Pte Ltd

（○: Chairperson）