2021

Digital Trust Forum

RULEMAKING COMMITTEE'S WHITE PAPER VERSION 1

DECEMBER 7, 2021

DIGITAL TRUST FORUM RULEMAKING COMMITTEE

Contents

Digital Trust Forum Rulemaking Committee White Paper (Ver. 1)

Digital Trust Forum Rulemaking Committee

I Introduction

While the global society has several challenges for the Sustainable Development Goals (SDGs), the Japanese Government is proposing Society 5.0[1], a society which incorporate digital technologies such as AI, 5G, IoT in all industries and social activities and balances economic advancement with the resolution of social problem.

To achieve Society 5.0, it is expected to establish a system for ensuring trustworthiness on the premise of harmonization with foreign regulations such as EU's eIDAS[2] which is based on coordination of various stakeholders and anticipation of international data flow. The Government presents two points, one is free and open data distribution as Data Free Flow with Trust (DFFT)[3] and the other is safety and security of data.

Achievement of this policy requires the connected society. However, malicious acts, i.e. cyberattacks or cybercrimes have not been completely eliminated in spite of various countermeasures and actions taken until now. To build the digital society in the future, it is extremely important to transit to the social structure on the premise of zero trust[4] and securing trustworthiness on data used in such society.

While promoting advanced security operation to protect the data used in the digital society, improvement of environment for mutual authentication in the whole society and secure data exchange are essential to transform into the above-mentioned social structure.

The Digital Government Ministers' Meeting[5] led by the Japanese Cabinet Secretariat and the Data Strategy Taskforce[6] for establishing a public-private framework mentioned "Trustworthiness of Data" (Trust)[7] requirement for securing trustworthiness on Society 5.0 as follows: "To achieve Society 5.0, that highly integrates cyberspace and physical space, it must be ensured and demonstrated that the data in cyberspace be correctly generated as claimed (authenticity) and not tampered (integrity)." They also pointed out it was extremely important to secure the data integrity and reliability of data collaboration infrastructure. In addition, since remote work must be promoted because of COVID-19 pandemic, it is required to promote abolition of administrative procedure requiring paper documents, seal-stamping and

---

1 https://www8.cao.go.jp/cstp/society5_0/

2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

3 "Outline on the New IT Policy in the Digital Era", IT Strategic Headquarters, decided on June 7, 2019, https://cio.go.jp/node/2534

4 A concept to carry out security countermeasures on the assumption of “never trust”. For example, in order to carry out those countermeasures, it does not based on distinction of network location that the trust is granted to internal network, not to external one, but it bases on that no trust is granted regardless of network location.

5 https://www.kantei.go.jp/jp/singi/it2/egov/

6 https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai4/gijisidai.html
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/gijisidai.html

7 Hereinafter referred to as "trustworthiness".

in-person meeting and consider how to secure the reliability in the above-mentioned digitization.

This white paper addresses securing trustworthiness in digitization as a social challenge, analyzes technical issues to solve it and suggests a system and actions for the solution.

In the present physical space, the trustworthiness is secured by conventionally using paper documents and seal-stamping for various transactions and contracts. To transit these conventional ways for safe and secure processing in cyberspace essential to Society 5.0 and DFFT, the trust must be secured for connection between physical space and cyberspace and also between cyberspaces. This white paper analyzes technical issues from the following two viewpoints and also suggests Trust as a Service (TaaS) to solve them:

・Viewpoint 1: Connection between physical space and cyberspace (securing vertical trust); and
・Viewpoint 2: Trust between cyberspaces (securing horizontal trust)

We consider it is increasingly important to establish a system to secure the trustworthiness in digitization and accelerate its implementation in society in conjunction with rulemaking, and they must be accomplished by cooperation of various stakeholders throughout the solution of social challenges and technical issues. In doing so, it is essential to harmonize the relevant regulation with foreign ones such as European eIDAS Regulation in consideration of international data distribution.

The Digital Trust Forum will promote the concept of "Digital Trust", a basic concept for realization of Society 5.0, establish Trust as a Service (TaaS) as a system to utilize Digital Trust in the real world, propose rulemaking to prepare the legal system and accelerate social implementation and spread.

II Scope: Digital Trust toward realization of Society 5.0

1 Background

In recent years, while the Internet is widespread in the economy and human life, the data-led digital society with cloud services, artificial intelligence (AI) and Internet of Things (IoT) is coming. In addition, the COVID-19 pandemic brought us the opportunity to reconsider the administrative procedure requiring paper documents, seal-stamping and in-person meeting principles as well as teleworks and remote meetings in "New Normal".

With ever-increasing needs of putting online various procedures in business and administration, important things are to remove concerns of people who are familiar with papers, give them a feeling of security, improve users' convenience by optimizing the procedures in digital society and thereby establish a system to provide a real feeling of entirely streamlined society in order to enjoy the benefits of digital. To this end, such a system to secure the trustworthiness on data in digital society and safe and secure data distribution is indispensable. As a basic concept to aim at this society, we propose "Digital Trust" as defined below. Though digitization and putting online is being proceeded for separate services to prevent further spread of COVID-19 infection, important things for achieving Society 5.0 are to secure the trustworthiness to achieve collaboration of these services and systems and to make use of them safely and securely, as mentioned by the Data Strategy Task Force.

2 Definition of Digital Trust

The Data Strategy Task Force describes the "overall picture of trustworthiness" as follows: "To realize Society 5.0, that highly integrates cyberspace and physical space, it must be ensured and demonstrated that the data in cyberspace be correctly generated as claimed (authenticity) and not tampered (integrity)." Based on this, we define "Digital Trust" to achieve Society 5.0 as follows.

[Definition of Digital Trust]
Digital Trust is defined as a system to provide effects such as bringing firmness[8] in digitization of services, procedures and data distribution in industries and administrations between physical space and cyberspace by securing the trust for human, organization, things, data, etc. by use of digital technology. An example of securing trustworthiness (trust) is to ensure authenticity of sender and addressee and data integrity through the network allowing verification by the connected parties and third parties as well as their verifiability of appropriateness of procedure[9]/system.

[8] To bring procedures, etc. into firm and reliable condition.
[9] A series of activities and procedures having interrelation or interaction to accomplish the purpose of industrial activities, services, procedures, etc.

Achievement of Digital Trust requires both social system and digital system. We call the latter for realization of Digital Trust as Trust as a Service (TaaS) and detail it in Chapter V.

This concept corresponds to "Trust Framework Arrangement"[10] presented by the Data Strategy Task Force[11] in May 2021. As a basic concept for securing trustworthiness in Society 5.0, Digital Trust must be immediately established by public-private collaboration.

Digital Trust defined here is to realize secured trustworthiness of data from a point of view different from cyber security. A zero-trust based method to achieve this goal is to collect the data to be protected into the cloud. In addition, realization of Digital Trust allows us to assure transition to society creating new innovation by data distribution and safe and secure data linkage on the assumption that much data is transferred and stored in dispersed system based on DFFT's idea.

3 Structure of this White Paper

This White Paper describes the background of demand on trust, status of trust in several countries and regions and reason of necessity of Digital Trust in the midst of digitization toward Society 5.0 (Chapter III).

It also describes the targets and challenges of Digital Trust (Chapter IV), and then advocates Trust as a Service (TaaS), a solution as digital system to realize Digital Trust, and challenges for realization (Chapter V). Lastly, it raises challenges to be considered for next White Paper and recommends the actions to be taken for social implementation of Digital Trust (Chapter VI).

III Status of environment and its change

1 Reason of demand on trust in the midst of digitization

On the background of increasing amount of data by progress of digitization and drive of innovation, improvement of AI technology and so on, various countries around the world regard data as infrastructure of their wealth and international competitiveness in this digital society, establish and strongly drive their strategy toward new society.

The Japanese Government introduces digital technology such as AI, 5G, IoT, etc. into various industries and social life and proposes Society 5.0, that highly integrates cyberspace and physical space.

The achievement of Society 5.0, which highly integrates cyberspace and physical space and highly utilize data, will significantly impact the conventional industrial structure and business. For example, it

[10] It describes that, the elements of trustworthiness, i.e. who (entity/intention), what (fact/information) and when (time) about data generation, are as declared (authenticity), and non-tampering (integrity), must be secured and proved as such, and that each of arguing points will be adjusted, and when adjusted, consideration of the direction of solution will start in relevant agencies.

[11] https://www.kantei.go.jp/jp/singi/it2/dgov/dai10/siryou_b.pdf

is assumed that the realization will change or influence each of the layers: (1) physical space; (2) connection of physical space and cyberspace; and (3) cyberspace as described below.

(1) Physical space

① Change of business configuration

- According to purpose of industrial activity, service, procedure, etc., fixed/static connection of person, organization and thing has changed to dynamic connection (unbundling/rebundling[12]).
- Transition to remote/online services
- With the above transition, extension of opportunities of cooperation/collaboration between companies or organizations

② Structural change of supply chain

- Complication of supply chain associated with softwarization, networking and modulization
- Diversification of suppliers, etc. and globalization of supply chain
- Evolution to dynamically modifiable supply chain

③ Change of industrial structure

- Reduced barriers to entry between business sectors by digitization and specialization, and progress of restructuring of industries and of merge of different business sectors

(2) Connection between physical space and cyberspace

The key to strengthen industrial competitiveness is utilization of large amounts of data daily accumulated in the field such as factory, medical service, automobiles, construction. It is expected that cyber and physical fusion will accelerate toward the utilization and that dependence on cyberspace will increase in future.

① Extension of non-site-specific working style and services

- Extension of private online services
- Transition to digitalized procedures in administration such as Digital Government action plan, etc.

② Strengthen of industrial competitiveness by utilization of data

- Rapid increase of IoT devices for industry, automobiles, medical services, etc.
- Various efforts to strengthen industrial competitiveness by cyber/physical system such as Industrial Internet Consortium (IIC) of the United States, and Industry 4.0 of Germany, etc.
- Creation of a new industry through new entry of different sector and/or collaboration of data in different fields.

③ Servitization of manufacturers

- Since Open-Source Software (OSS) and 3D printers have increasingly commoditized various

[12] "Discussion Paper on Digital Markets", the Ministry of Economy, Trade and Industry, January 8, 2020, https://www.meti.go.jp/press/2020/01/20210108002/20200108002-1.pdf

kinds of product, manufacturers are embarking servicing business including maintenance after shipment, making use of digital technology and real data.

(3) Cyberspace

① Increasing amount of distributed data
Generalization of data distribution in dispersed environment to connect various organizations, business sectors, industries or their created values through data beyond borders

② Increasing risks in cyberspace
- Increasing risks due to advancement and complication of cyber attacks
- Increasing attack surfaces due to increase of data distribution
- Increasing attacks which cannot be prevented only by system protection, e.g. business e-mail compromise (BEC).

Based on these anticipated changes and influences, it is expected that the realization of safe and secure Society 5.0 that highly integrates cyber and physical spaces has risks described in the following (1) to (3).

(1) The problems in cyberspace will increase the potential for serious impacts on physical space and business activities of companies.
(2) As the cyberspace expands, the risks to protection of privacy, security and data increase.
(3) Transfer of vast amounts of distributed data between organizations and between machines will increase necessity of check of source or authenticity of data and demand on automation of such check.

To address the above risks while coping with both economic development and social challenges by effective data utilization, it is essential to make international rules necessary for free data distribution while securing trust concerning distributed data.
Especially, data adds value to itself by combination with other data or actually being used. Therefore, it is very important for creation of innovation to not only hoard data but also establish an ecosystem which can be shared beyond business sectors and industries. What supports the creation of innovation is a system to check trust between entities including those not physical but present such as organizations or parties, as well as physical entities such as person, thing.

To this end, we consider Japan should aim at realization of securing trust on ① authenticity of person who produced data and data provider, ② securing data integrity and ③ validity of procedure/system, etc. and disseminate newly created values to society and at making international rules to use data with secureness by safely and freely distributing data between related entities, in consideration of:

(1) connection between industries and between organizations;
(2) actual society reproduced and built on cyberspace (digital twin);
(3) data connection on cyberspace and data handling.

2 Overseas situations

(1) The United States

Standardization of technology and scheme concerning trust service are established from the viewpoint of national security mainly led by the Federal Government.

Personal Identity Verification (PIV) card, complying with Federal Information Processing Standards Publication 201 (FIPS-201), is a card known for widely covering electronic authentication. It has a very wide range of functions such as face-to-face authentication process, electronic authentication, electronic signature, encryption, biometric authentication and is issued to government officials. For private sectors, PIV-Interoperable (PIV-I) card is issued.

NIST SP 800-63[13], published by the National Institute of Standards and Technology (NIST), is known as a guideline for electronic authentication. It covers online authentication in online services of the governmental agencies, which is remotely performed via network to grant IT systems access to important data, etc. The guideline provides requirements for identity authentication for registration to system, assurance levels for authentication and flowcharts for selection of assurance level suitable for purpose.

Federal PKI (FPKI) is known as an infrastructure for electronic authentication which gives safe connection (authentication) between governmental agencies and between governmental agency and related company by use of electronic certificate and consists of hundreds of Certification Authorities (CA). It allows connection with other governmental agencies and private organizations via bridge CA and interconnection by policy mapping at an assurance level specified in NIST SP800-63.

Regarding the legislation concerning electronic signature as expression of personal intention, the Uniform Electronic Transactions Act (UETA) was enacted in 1999 as a uniform act at a state level, followed by the Electronic Signatures in Global and National Commerce Act (ESIGN Act)[14] in 2000. Under the ESIGN Act, various electronic signatures including remote signature and data of scanned hand-written signature were recognized to be legally equivalent to hand-written ones in every state.

Information confidentiality classification called Classified Information (CI) or Controlled Unclassified Information (CUI) is known as classification of information concerning national security. Under the Executive Order 13526 in December 2009, the provisions for classification system such as classification or protection of CI were set forth for Classified National Security Information). The concept

[13] NIST, Digital Identity Guidelines (guideline for electronic authentication), https://pages.nist.gov/800-63-3/

[14] The Electronic Signatures in Global and National Commerce Act (E-Sign Act), https://www.fdic.gov/regulations/compliance/manual/10/X-3.1.pdf

of CUI aims at protection of confidentiality of supply chain for production of products related to national security such as military weapons, which is an information category defined under the Executive Order 13556 in November 2010. The National Archives & Records Administration (NARA) is responsible to the overall Federal Government for system of CUI protection. According to the instruction from NARA, NIST provided the standard for CUI protection as NIST SP 800-171[15] on the basis of NIST SP 800-53[16]. The SP800-53 provides the catalog for security control measures. The SP 800-171 is a guideline prescribing recommended security requirements for Controlled Unclassified Information (CUI) targeting private sector as supplier for the government.

Meanwhile, the Zero Trust Architecture (NIST SP 800-207)[17] is a report providing a guideline for transition from physical space to cyberspace. This report is based on assumption of Zero Trust that attackers can exist on every network inside and outside of an organization and suggests Zero Trust Architecture to realize security on cyberspace on this assumption. This architecture stands on the viewpoint of cyberspace, but is considered to include useful way of thinking to secure the trust in cyberspace.

The trend in private sector is establishment of system having social acceptability by standards or regulations on data distribution on a private basis, as well as deployment[18] to private services starting from government-related trust scheme and infrastructures (NIST SP 800-63 and so on).

[15] NIST, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
[16] NIST, Security and Privacy Controls for Information Systems and Organizations, https://www.nist.gov/privacy-framework/nist-sp-800-53
[17] NIST, Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final
[18] EXOSTAR, Inc., etc.
https://www.evaaviation.com/cui-dfars-nist-sp800-171/usaexostar/

(2) EU

Trust service and scheme are established from the viewpoint of economic development. In 2010, the European Commission announced the Digital Single Market (DSM) Strategy. Along with this strategy, the member states of the European Union (EU) adjusted different laws, schemes, communication environment among them. Then the EU repealed the Electronic Signature Directive published in 1999 and established a comprehensive and uniform regulation of trust services including electronic identification (eID) and electronic signature as eIDAS Regulation in 2014 and it was taken into effect on July 2016.

The eIDAS Regulation legally prescribes identity verification and authentication, standards and system for assuring trustworthiness of various kinds of trust services and operation of the trusted list which makes the trust services mechanically verifiable. The trust services under the eIDAS Regulation are the following:

- generation, verification, and validation of electronic signatures, electronic seals or electronic timestamps;
- e-delivery service and generation, verification, and validation of certificates concerning that service;
- generation, verification and validation of certificates for website authentication; and
- preservation of electronic signatures, electronic seals and certificates for those services.

When the eIDAS Regulation was taken into effect, the number of qualified trust service providers (QTSP) was 151, but as of January 2021, it increased to 200.

The most recent status is that ENISA published an eIDAS Promotion Report on February 2021 to facilitate the introduction of eID and trust service. Its report of actual state of remote identity proofing[19] is especially important and gives a direction of survey on remote ID Proofing, which is based on the understanding that face-to-face ID Proofing is troublesome and danger in COVID-19 situation. This is backgrounded by the recognition that it is unclear how the condition "equivalent to face-to-face", required for remote ID Proofing, should be interpreted, though remote ID Proofing is allowed by the eIDAS Regulation. Answers to questionnaire were collected from the present stakeholders involved in remote ID Proofing, and analysis of threats to remote ID Proofing service and examples of countermeasures were compiled in Recommendations for future (Chapter 5, Paragraph 3).

[19] Remote ID Proofing, https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

(3) United Nations

In the Working Group IV (Electronic Commerce)[20] of United Nations Commission on International Trade Law (UNCITRAL), it is under discussion to establish international provisions for recognition of eID and trust services in cross-border electronic transaction[21].

This topic had been discussed since 2018 and for trust services, the agreement was reached in the most recent 60th Meeting in 2020. At present, it is not clear whether the provisions will be established as a model law or published as a guideline, but it would be a beacon for UN member nations to implement international electronic transaction. Definitions of related terms are shown below.

(d) “Electronic identification”, in the context of IdM services, means a process used to achieve sufficient assurance in the binding between a [subject][person] and an identity.
(g) “Identity management (IdM) services” means services consisting of managing identity proofing or electronic identification of [subjects][persons] in electronic form.
(j) “Identity proofing” means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a [subject][person] within a particular context.
(m) “Trust service” means an electronic service that provides assurance of certain qualities of a data message and includes electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services.
(n) “Trust service provider” means a person that provides one or more trust services.

3 Domestic situations

In 2019, the Act on Use of Information and Communications Technology in Administrative Procedure (Digital Procedure Act) was enacted, which determined the basic three digitization principles (① Digital First, ② Once Only, ③ Connected One-stop) and required, in principle, administrative procedures of Japan to be put online.

The Act emphasizes the importance of viewpoint of "Digitalization" that means building a new social infrastructure for next age presupposing digital, not "Digitization" that just means putting online the present procedures in writing or face-to-face like conventional digitization.

On October 9, 2020, the Digital Government Ministers' Meeting was organized for digitization of administration, where "Working Group to Fundamentally Improve the Individual Number System and the Digital Transformation of National and Local Governments", "Data Strategy Task Force" and "Working Group for Digital Transformation Related Bills" were established. Now they embody and

[20] https://uncitral.un.org/en/working_groups/4/electronic_commerce
[21] Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services, https://undocs.org/en/A/CN.9/WG.IV/WP.162

accelerate their respective policies.

The Working Group to Fundamentally Improve the Individual Number System and the Digital Transformation of National and Local Governments prepared a process chart for digitization of various cards using Individual Number Card. This process chart presents the importance of establishment of comprehensive framework to secure the trust including three factors for which the trustworthiness is required in cyberspace to transform the data in physical space into that of cyberspace: a) expression of intent, b) origin of data, c) existence and trust anchor functions.

The Data Strategy Task Force[22] describes the "overall picture of trustworthiness" as follows: "To realize Society 5.0, that highly integrates cyberspace and physical space, it must be ensured and demonstrated that the data in cyberspace be correctly generated as claimed (authenticity) and not tampered (integrity)." The Task Force presents three factors in cyberspace consisting of: "entity/intention" as a proof of expression of intention; "fact/information" as a proof of origin of data; and "existence/time" as a proof of existence.

In the Digital Government Action Plan[23], the Working Group for Digital Transformation Related Bills clarified the three digitization principles consisting of ① Digital First, ② Once Only and ③ Connected One-stop and determined that putting the administrative procedures of Japan online must be implemented according to these principles. For preparation of infrastructure to realize the Digital Government, the Action Plan advocates promotion of Individual Number Card for identity check and preparation of base registry environment for data strategic promotion.

Data Free Flow with Trust, the concept based on the pillars of assurance, security and quality of data and sent out into the world, aims at promotion of international free data distribution, meaning that the data useful for business and solution of social challenges freely pass beyond borders, while protecting privacy, security and trustworthiness on intellectual property rights.

For the streams of both promotions of digitization and data distribution, realizing Digital Trust is an urgent task.

[22] https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai4/siryou1-1.pdf
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-2.pdf
[23] https://www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou4.pdf

4 Summary of Trends in Trust

Table 1 summarizes the trends in the United States, Japan and EU. These countries understand the necessity of trust in cyberspace and have started preparation of environment beginning at online identity authentication. However, comprehensive preparation of environment, suggestion of architecture, social implementation and rulemaking are future challenges.

Based on consideration of trend comparison, the future direction to secure trust in Japan would be as follows:

- suggestion on solution of identity authentication and attribute information in terms of Individual Number Card and base registry;
- realization of high value-added trustworthiness linked with base registry;
    - Example 1 - Linking attribute information of an organization with base registry to check its qualification for participation in public bidding when the application for participation is received.
    - Example 2 - Automation of check of existence and attribute information of legal person using gBizINFO
        - The gBizINFO is an information website for domestic corporates and managed by the Ministry of Economy, Trade and Industry.[24] It covers about four million corporates with respective designated corporate number and has functions of collective search and display of information on corporate number, corporate name, address of head office as well as corporate activity information possessed and published by the government, including contract with ministries, commendations, etc.
        - When a private Trust Service provider issues electronic certificate to a corporate representative, a corporate itself or corporate-owned website, the API of gBizINFO open to the public gives online access to the existence of corporate and attribute information including address, name and title of its representative.
        - While corporate names (in the Japanese syllabaries, alternative characters, alphabetical notation) and office information are organized, it is expected to automate issue of electronic certificates in future by use of gBizINFO as the base registry for corporates.
- Disclosure of information serving as an internationally sharable base point of trustworthiness capable of automatically checking trustworthiness of vast amounts of distributed data (Trust Anchor).

[24] https://info.gbiz.go.jp/index.html

Table 1 - Summary of trends on Trust in the U.S., Japan and EU

Item	**The United States**	**Japan**	EU
Related acts	- National Commerce Act: E-SIGN - Uniform Electronic Transactions Act: UETA - USA: Government Paperwork Elimination Act: GPEA - Executive Order 13526, 13556	- Act on Electronic Signatures and Certification Service - Public Individual Certification Act - Commercial Registration Act - The Act on Dissemination and Promotion of Electronic Power of Attorney	eIDAS
National ID, ID Management	SP800-63, FIPS-201, PIV(-I) card, SSN	Individual Number Card (electronic certificate for public personal authentication)	eID (eID card issued per country)
Trust Anchor, Trust Presentation	Federal Bridge CA (FBCA)	- Government Bridge CA (machine-readable) - Official Gazette (human-readable)	Trusted List
Audit, accreditation	- According to FPKI policy - Extension of NIST SP 800-53: Cybersecurity Maturity Model Certification (stricter than ISMS and existing up to Level 3. Data Countermeasure by CUI + cyber countermeasure: CA audit, described as an extension of NIST SP 800-53, but the truth is unknown)	- Accreditation of specified certification business (The Act on Electronic Signatures and Certification Service) - Accreditation of handling electronic power of attorney (the Act on Dissemination and Promotion of Electronic Power of Attorney) - Accreditation of timestamping service - Accreditation under Article 17, Item No. 5 of the Public Personal Authentication Act	- eIDAS QTSP - ETSI EN 319 401 (General Policy) - ETSI EN 319 411 (Policy for CA) - ETSI EN 319 403 (Standard for conformity assessment body) - ISO/IEC 17065 (Standard for conformity assessment body)
Cybersecurity countermeasure	- NIST Cybersecurity Framework, - SP 800-171 , SP 800-53	- ISMS - METI Cyber/Physical Security Framework	- ISMS - EU Cyber Security Certification Framework
Transition to cyberspace	NIST SP 800-207 "Zero Trust Architecture"	Preparation of environment such as data distribution infrastructure, Trust Anchor, etc. is considered.	Digital Agenda for Europe Promote realization of Digital Single Market
Challenges of trust in digitization	Industrial application of services starting from the government trust scheme/infrastructure (NIST SP 800-63, etc.)	Online authentication using Individual Number Card and others are considered, but comprehensive preparation and architecture based on functional configuration to realize this environment will be addressed in future.	Identity authentication equivalent to face-to-face authentication required for eIDAS is under standardization. Commitment to institutional action on this and international mutual recognition of eIDAS with countries outside the EU.

IV Challenges towards Realization of Digital Trust

1 Purpose of Digital Trust and social challenges

As describes in Chapter II, the “overall picture of trust” is as follows: “To achieve Society 5.0, that highly integrates cyberspace and physical space, it must be ensured and demonstrated that the data in cyberspace be correctly generated as claimed (authenticity) and not tampered (integrity)”. In addition, the procedures must be completed by using the introducing means with less burden on users and interacting services of organization beyond individual systems.

Figure 1 shows the examples of procedure on paper on the assumption of opening a corporate bank account. A bank account is opened by paperwork with various documents and certificates between ministries, banks, corporates and persons who perform such procedures. The purpose of Digital Trust is to realize safe and secure digitization of such interaction of services between organizations, which is a social challenge we commit.

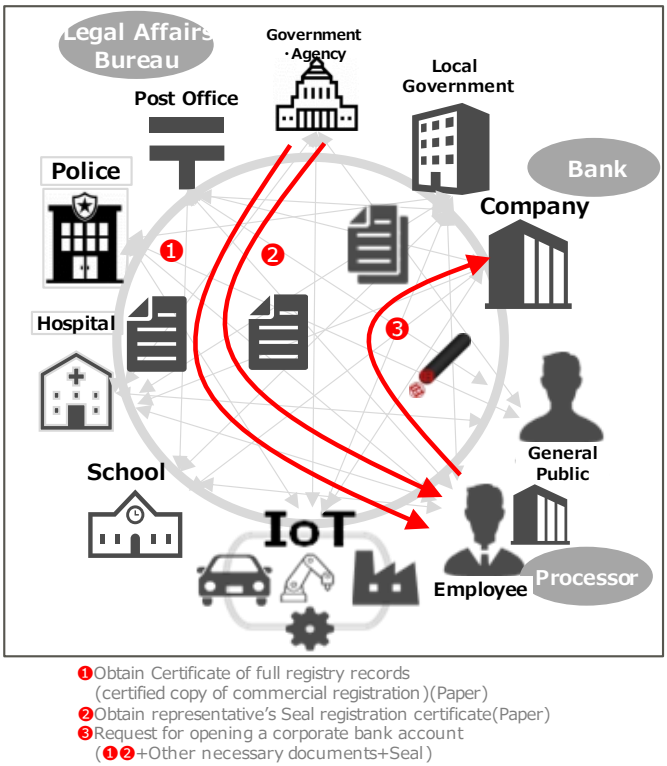


Figure 1- Procedure for opening a corporate bank account (on paper)

2 Effects introduced by Digital Trust: Realization of Providing Firmness

In order to accomplish a procedure in which organizations' services interact beyond their systems, the data used for the procedure is important. Explanation of the reason is given below, using Figure 2 showing the relationship between services/procedures between several organizations/enterprises and data used.

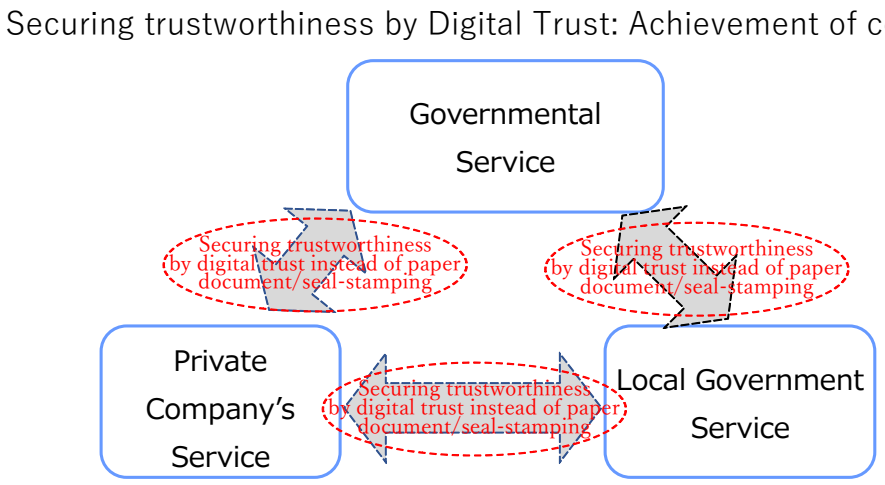


Figure 2 - Securing trustworthiness by Digital Trust and Achievement of Providing Firmness

It is considered each of transactions from ① to ③ as arrowed in Figure 1 is individually digitized. On the other side, in Figure 2, it can be seen that the transactions indicated by broken line are not digitized, and that papers connect different services or systems. Paperwork involves errors, because it requires steps with manual entry into terminal or handwork. Especially, such errors are more likely to happen with complicated entry or work step. However, promotion of digitization will cut off human work, and, in addition, digitization with enhanced usability for users will reduce human errors.

Digital Trust aims at securing trustworthiness of data converted by such digitization of papers and seal-stamping and thereby enhancement of usability in digitiation to realize a certain level of improved robustness and certainty (certainty) over the whole digitized procedures.

(1) Examples of achievement of certainity

To realize a certain level of improved robustness and certainty (certainity) over the whole digitized procedures, it is important for Digital Trust to enhance usability for steps involving handwork, as well as securing data trustworthiness by trust services supported by legel system. Here are some examples for understanding this. The following case is the digitization of procedure using business documents such as quotations and invoices by means of communication tool such as e-mail.

For example, e-mail is a major communication tool for business, but it has the following issues.

① The authenticity of sender is not secured and it is difficult to distinguish whether the e-mail is true, fraudulent or phishing.
② Transaction information such as quote, invoice cannot be automatically linked with work operation system described later.
③ Risk of erroneous transmission remains and there is a concern of leakage of personal information, and so on.
④ It is hard to throughly direct confirmation of delivery and receipt, and even if a receipt notification is received, its authenticity is not secured, and it can be hardly deemed as a firm evidence.

To solve this kind of issue, the eIDAS Regulation defines Electronic Registered Delivery Service (hereinafter referred to as ERDS or e-delivery service[25]), so to say, electronic registered mail, as one of trust services, enabling secure transimission and receipt of various business documents. The ERDS architecture is shown in the 4-corner model[26] in Figure 3.

[25] For examples of ERDS, eDelivery and Registered Electronic Mail (REM) Services are known. The following ETSI document explains REM, and for instance, it refers to S/MIME (”Authentication in the REM MSI may rely on the features provided by SASL [i.12], TLS (e.g. certificate-based authentication), S/MIME [i.7] digital signature over the submitted message, or other mechanisms.”)
https://www.etsi.org/deliver/etsi_en/319500_319599/31953201/01.00.00_20/en_31953201v010000a.pdf

[26] Connecting Europe Facility: Introducing CEF eDelivery
https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/03_eDELIVERY/S02_ERDS_REM_SOLUTIONS_SERVICES/INTRODUCING_CEF_eDELIVERY_RASMUSSEN_EC_DG_DIGIT.pdf

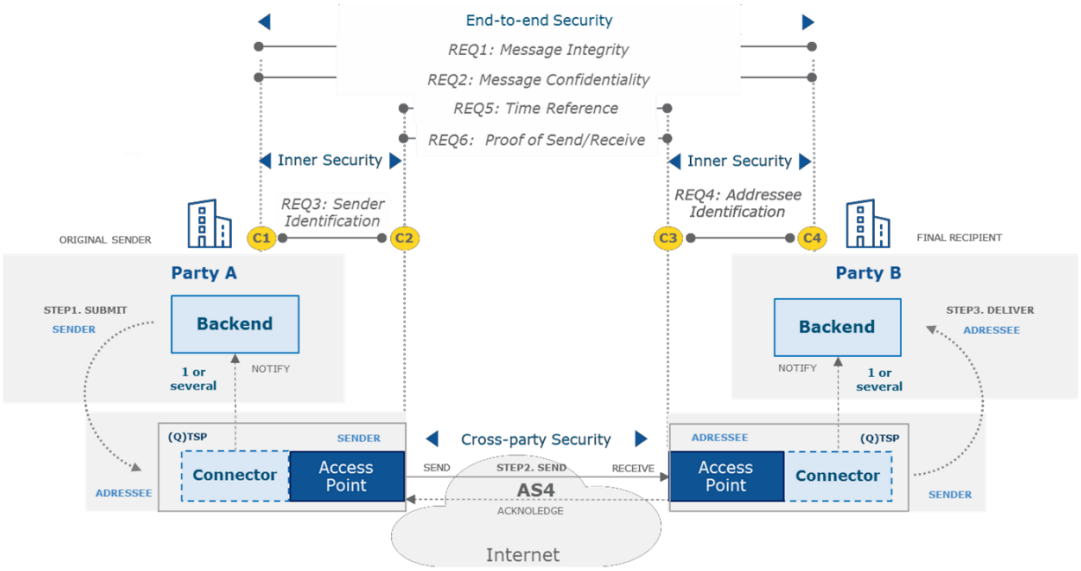


Figure 3 Architecture of Electronic Registered Delivery Service (ERDS)

In this figure, in the communication between the sender C1 and the addressee C4, the ERDS used by C1 is expressed as C3, and the other ERDS used by C4 is expressed as C3.

The ERDS has requirements for authentication process of sender and addressee, securing end-to-end authenticity of message text between C1 and C4, authenticity of message document between C2 and C3, and employs e-seal or electronic signature. Accredited Qualified Electronic Registered Delivery Service (QERDS) prescribes the requirements from REQ1 to REQ6 in Table 2.[27]

If the message texts between C1 and C4 are used in a closed way, providing e-seal on the messege document can secure the trustworthiness between C2 and C3. (REQ5) On the other hand, if the message received by C4 must be sent to outside, it is necessary to secure authenticity of end-to-end message texts between C1 and C4. For example, if the addressee of invoice or receipt is different from the payer, i.e. adjustment of an employee's advance payment, insurance claim, C1 puts e-seal to secure authenticity of the end-to-end message text between C1 and C4. (REQ1)

[27] CEF eDelivery Building Block Version 1.00 Security Controls
Linking eIDAS (Q)ERDS & CEF eDelivery
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance?preview=/82773295/82802571/(CEFeDelivery).(SecurityControls).(v1.00).pdf

Securing the end-to-end authenticity of message document between C1 and C4 in this way ensures the integrity of sent and received message text, the message text sent by identified sender and received by identified addressee, accuracy of date and time of sending and receipt by QERDS. These procedures will be firmed up, even if the addressee of invoice and receipt is different from the payer, or adjustment of advance payment or insurance claim service is digitized.

Table 2 Summary of Requirements of Qualified Electronic Delivery Service under the eIDAS Regulation

Requirements for Qualified Electronic Delivery Service	Interpretation in CEF e-delivery	Coverage of security
REQ1: Message Integrity	Messages shall be secured against any modification during transmission. This shall be secured by an advanced electronic signature/an advanced electronic seal.	End-to-end Security (C1-C4)
REQ2: Message Confidentiality	Messages shall be encrypted during transmission.	End-to-end Security (C1-C4)
REQ3: Sender Identification	The identity of the sender shall be verified with a high level of confidence via authentication process and/or an advanced electronic signature/an advanced electronic seal.	Inner Security (C1-C2)
REQ4: Addressee Identification	Identity of addressee shall be verified before the delivery of the message via authentication process and/or an advanced electronic signature/ an advanced electronic seal.	Inner Security (C3-C4)
REQ5: Time-Reference	The date and time of sending and receiving a message shall be indicated via a qualified electronic timestamp which is guaranteed by an advanced electronic signature/an advanced electronic seal.	Cross-party Security (C2-C3)
REQ6: Proof of Send/Receive	Sender and receiver of the message should be provided with evidence of message addressee and deliver. To this, timestamp, or qualified timestamp in case of qualified status, should be used and linked with the date and time of sending and receiving.	Cross-party Security (C2-C3)

3 World aim to achieve and analysis of challenges

In most of current procedures, papers and seal-stamping are generally used in physical space only to secure the trustworthiness and to connect between corporate and municipality or between services. To drive digitization of these procedures, a system to secure trust of data is required for each organization and for each service to develop the service from physical space to cyberspace by electronic signature and timestamp, as described in the preceding clause. Figure 4 helps to visualize the model for analyzing these challenges in digitization.

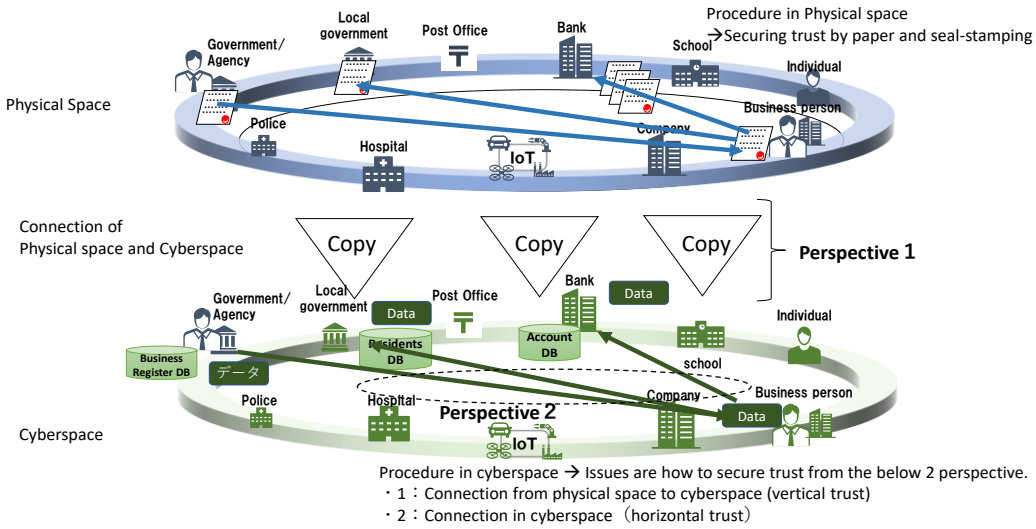


Figure 4 Model of issues in trustworthy digitization

Figure 4 illustrates the model of challenges in digitization of procedures in three layers: physical space; connection between physical space and cyberspace; and cyberspace. For procedures in physical space, papers and seal-stamping are used to secure the trustworthiness, but in order to achieve these procedures in cyberspace, the challenge is to secure the trust from the following two viewpoints.

- Viewpoint 1: Trust of connection from physical space to cyberspace (securing vertical trust)

  At the boundary of cyberspace and physical space, information must be converted with appropriate correctness according to that of required information, that is, correctness of transcription function (including the meaning of "correct translation"). For this, the following issues must be solved.

  - Issue of ID in cyberspace to person, organization and thing in physical space, and check of existence in physical space when ID is issued.

- Checking that the procedures in physical space are correctly achieved by the system of cyberspace.
- Linking ID in cyberspace with person, organisation and thing in physical space (authentication, etc.)
- Rules and scheme relating to above check and link required according to severity of procedures in physical space.

- Viewpoint 2: Trust of connection between cyberspaces (securing horizontal trustworthiness)
  Measures required for distribution/management of data and for proper editing/processing and a system to take these measures are necessary, and to this, the following issues must be solved.
  - The origin, time and confirmation of intention relating to procedures done in cyberspace and data
  - Linking IDs of same person, organisation or thing in physical space with those in cyberspace[28]
  - Rules and scheme relating to above check and link required according to severity of procedures in physical space.

Considering the example of opening corporate account shown in Figure 1, the current procedures (AsIs), challenges in digitization and shape after transition to digitization (ToBe) are explained below in order.

[28] It refers to linkage within legal system such as for protection of personal information.

(1) Current situation (example of opening a corporate account)

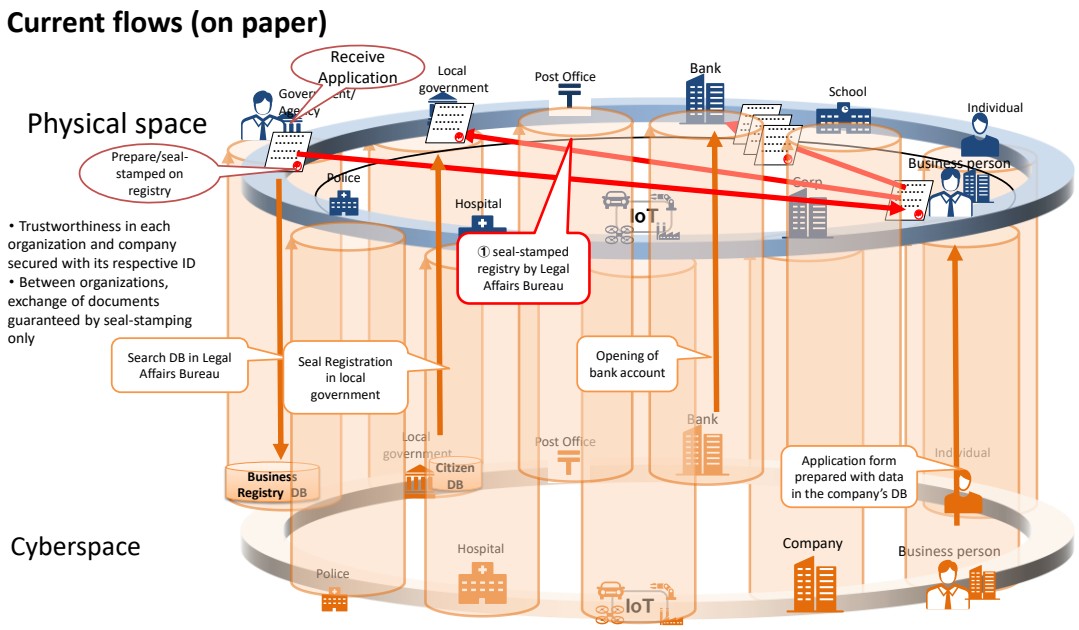


Figure 5 Flow of current processing with papers

Figure 5 shows the current flow of opening a corporate bank account as illustrated in Figure 1. First, an applying corporate logs in its system and acquires necessary information from its database (in cyberspace) and then submits application forms (on papers) for a certified copy of commercial registration (certificate of full registry records) and a seal registration certificate to the Legal Affairs Bureau (in physical space). After the Bureau receives them (processed in physical space up to this point), they are searched and checked on the registry database of the Bureau (these processes are in cyberspace). According to the result of check, the certified copy of commercial registration (certificate of full registry records), etc. seal-stamped by the Bureau, are submitted to the applying corporate (in physical space). Then the corporate submits obtained certification documents with other documents including the corporate's articles of incorporation obtained from its database (in cyberspace) to the bank (in physical space) to open its corporate bank account.

As just described, in the contemporary society, while information on database of corporates and organizations in cyberspace is used, paper documents are basically exchanged between different organizations in physical space. At present, realization of their safety and secureness are based on the authenticity of documents issued and seal-stamped by public offices, etc., and it can be said that the chain of trust begins from them.

This kind of complicated process in which paper documents (in digital space) and digitized information (in cyberspace) come and go between organizations is a bottle neck against the future streamlining of digitization and processes and high-volume processing.

(2) Problems in digitization (example of opening a corporate bank account)

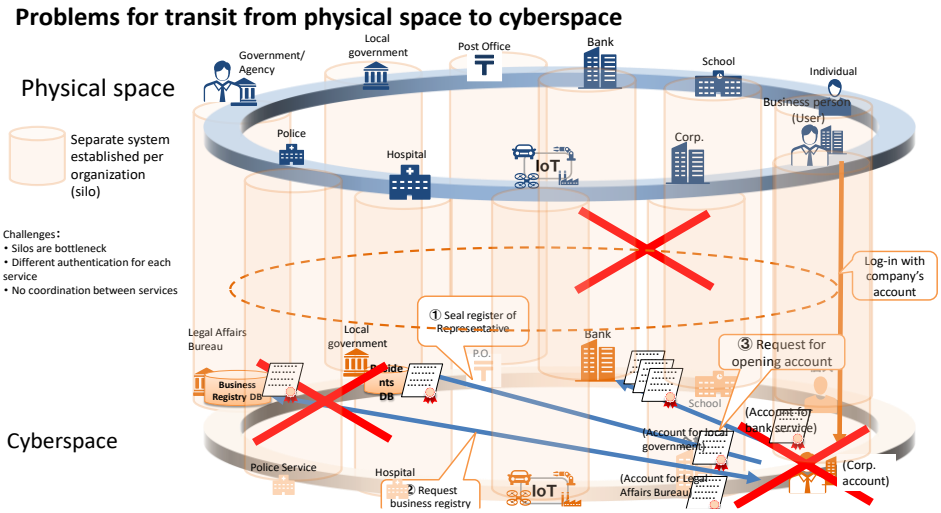


Figure 6 Challenges in transition to cyberspace

Figure 6 illustrates the problems in case of transition of the current procedures on paper to those in cyberspace. When a corporate applies for a certified copy of commercial registration (certificate of full registry records) and seal registration certificate to the legal affairs bureau through cyberspace, there is a problem for consistency between their individual silo type systems, associated with management of ID and authority per ID. Silo type system refers to a system is provided in a silo established for each organization such as corporate, bank, legal affairs bureau and closed by firewall. Another problem is that, since there is a difference of securing trust between their individual systems, the measures required for proper editing and processing between other silo type systems, and the system to do so, are not established. These problems make it difficult to mutually secure the trust of data between different organizations. At present, therefore, it is difficult to deliver and receive the data with trust between corporate and the bureau or between corporate and bank as described in the broken line in Figure 6.

Unless we solve different authentications for each silo and securing trust, it is hard to transition to procedures in cyberspace.

(3) Image after transition to digitization (example of opening a corporate bank account)

On the other hand, Figure 7 illustrated the ideal world that DFFT and Society 5.0 aim at. Once the user, in physical space, logs in and start the process from smart phone or PC according to prescribed procedure, an application is sent from the corporate to the legal affairs bureau, and the bureau sends the result in cyberspace. Then another application is sent with the result and necessary information, with the trust of documents secured, from the corporate in cyberspace to the bank in which the account is to be opened.

When the bank confirms the trust, the bank account is opened. The opening as information in cyberspace is notified to the corporate, and the applicant in physical space can confirm the completion of process. That is, in this world, only the process in physical space is required at the beginning to complete the process, while the trustworthiness of information is secured in cyberspace.

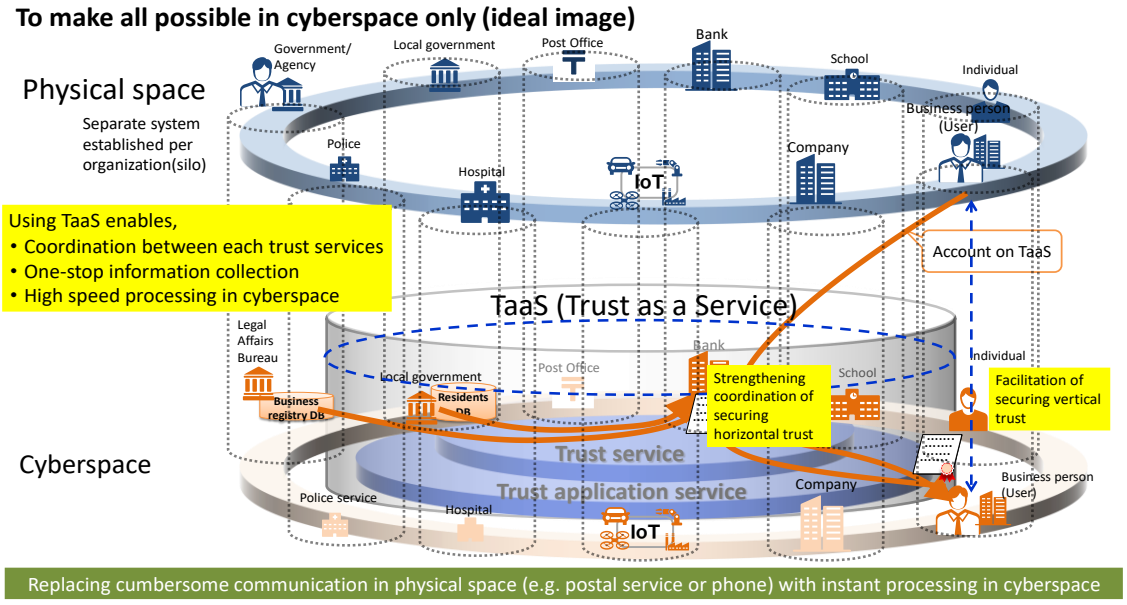


Figure 7 Ideal image aim to achieve

To further promote digitization including deployment of DFFT and Society 5.0 in future like this, realization of the following two new systems is required.

One is a system to provide easy access to trust services such as timestamp or electronic signature, even in case an exclusive system to connect physical space and cyberspace with chained authenticity has not been independently established. (Viewpoint 1: Facilitation of securing vertical trust)

The other is a system to realize an intermediate world between individual silo type trust worlds to carry out interaction in cyberspace between organizations or services currently performed in physical space. (Viewpoint 2: Strengthening interaction for securing horizontal trust)

Realization of the structure (Figure 7) like this lowers the barrier of introduction due to the scale of business and allows everyone to connect physical space and cyberspace with trust and use this. The aims are to give access safely and securely in various ways by using newly defined functions while enabling continued use of conventional type, achieve Society 5.0, trust across borders and DFFT.

4 Technical challenges for achievement of Digital Trust

In consideration of the above-mentioned technical challenges, this section describes challenges for achievement for Digital Trust.

Figure 8 illustrates that services are realized in combination of entity such as person, organization, thing, etc., procedure and system. It also represents a model of technical challenges to realize procedure across more than one organization/corporate.

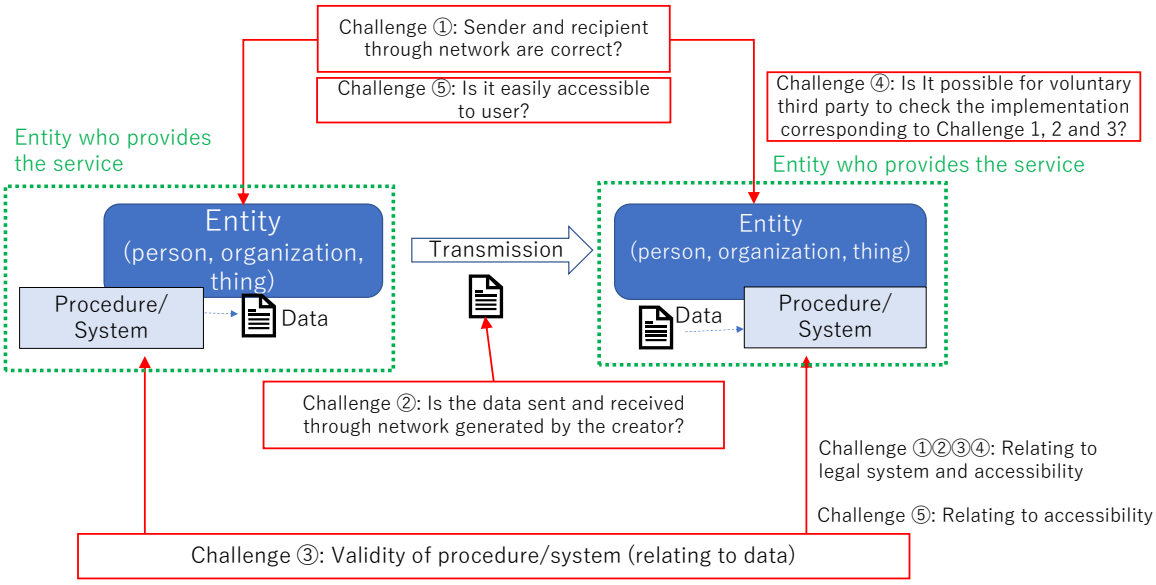


Figure 8 Model of challenges to achieve Digital Trust

Figure 8 also provides a model to achieve the definition of Digital Trust, "ensuring authenticity of transmitting and receiving parties and data integrity through the network allowing for verification by the parties or third parties as well as their validity of appropriateness of procedure/system."

To achieve Digital Trust on the basis of Zero Trust concept on the presumption of "Never Trust", it is important to allow verification by the parties or third parties (1) whether the sender and addressee are as intended each other, (2) whether the data is sent and received without fail and (3) whether the data is generated through correct process, as well as giving validity under the legal system when these are accomplished.

In addition, since the Digital Trust aims at realize a certain level of improved robustness and certainty (certainity) over the whole digitized procedures, it is also important to enhance usability for that purpose.

Figure 9 provides a viewpoint of usability. It is cited from the distributed material of the 9th Meeting of the government's Growth Strategy Council.[29] One of the "to be" items in Figure 9 is "promotion of

[29] The Cabinet Secretariat, the Committee on Growth Strategy, the 9th Meeting on Growth Strategy, Attached document 4 "Efforts to realize digital society" (April 12, 2021)

human-friendly digitization". In addition, it mentions "Realization of thorough UI and UX/services to the nation" in collaboration of citizens, nation/municipalities, quasi-public bodies and private sectors. Realization of these is one of the biggest challenges.

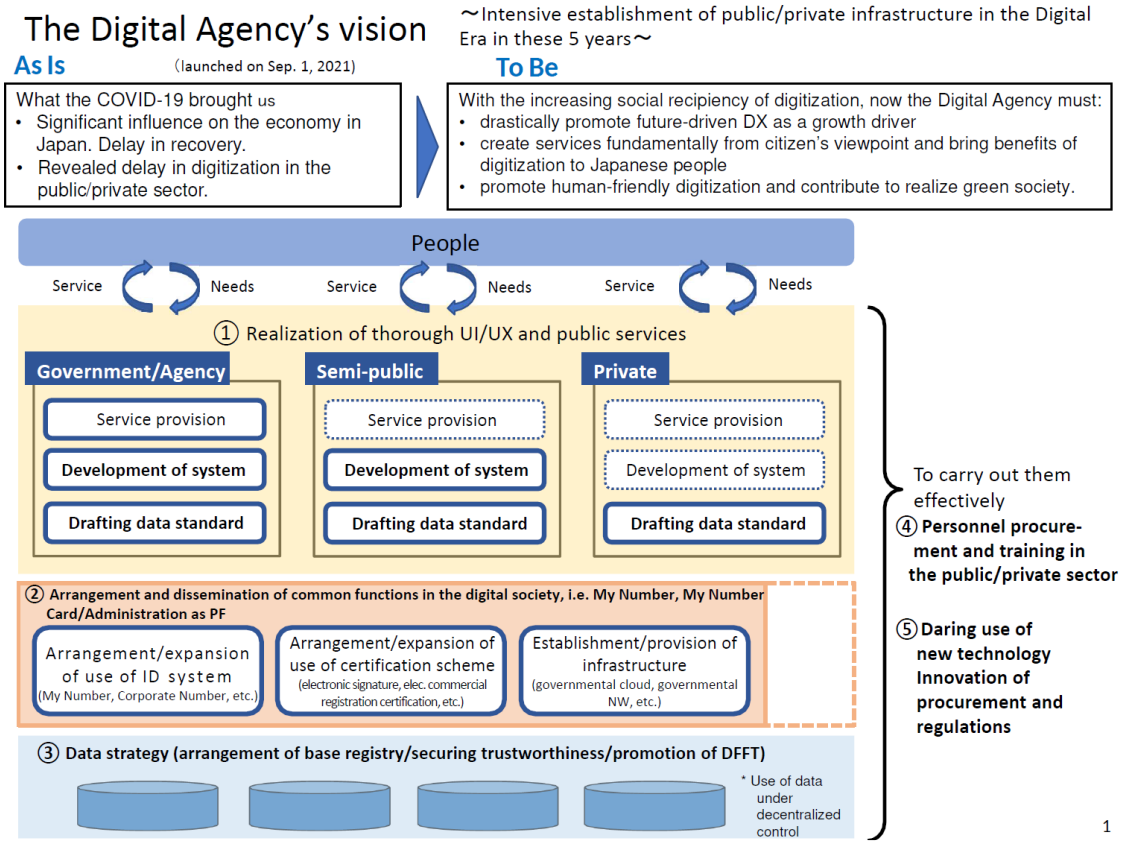


Figure 9 Image which the Digital Agency aims at (from the material for the 9th meeting of Growth Strategy Council)

In consderation of them, the technical challenges for realization of Digital Trust can be listed according to Figure 8 as the following Challenge ① to ⑤.

[Challenge ①: Are the sender and the addressee correct?]

It addresses both Viewpoint 1 and 2.

At first, it focuses on the entities sending and receiving data. The important thing is mutual confirmation of authenticity, that is, mutually confirming who is the other and whether the other is authentic. The authenticity of entity is fundamental for all things, leading to delivery and receipt of data on this presumption. Realization of this function to secure the authenticity is the first challenge.

[Challenge ②: Is the data sent and received correct?]

https://www.cas.go.jp/jp/seisaku/seicho/seichosenryakukaigi/dai9/siryou4.pdf

It addresses Viewpoint 2.

It is the second challenge to secure the integrity of data, that is, ensuring the data itself sent and received is correct and correctly sent and received, and the received data is consistent with the sent one. Unless the integrity of data is secured, it is impossible to conduct transactions between the parties and share information.

[Challenge ③: Validity of procedure/system relating to data]

It addresses Viewpoint 2.

The third one is related to procedure/system. If the validity of procedure/system related to sent and received data, the trustworthiness cannot be provided for services, procedures, industrial activities realized by them, and values created in these activities. Therefore, securing the validity is the third challenge.

[Challenge ④: Are the challenges ①, ② and ③ able to be verified?]

It addresses both Viewpoint 1 and 2.

The fourth challenge to prove the value of Digital Trust is that voluntary third party requiring to secure authenticity of entity by mutual confirmation of sender and addressee and integrity of data sent and received between entities, which is achieved by solving the above ① and ②, and to achieve verifiability of the validity of procedure/system related to received data by the parties and third party.

[Challenge ⑤: Is the system easily available for users?]

It addresses both Viewpoint 1 and 2.

The fifth challenge is to realize user-friendly system, which is essential for solving Challenge ① through ⑤ and supporting achievement of Digital Trust for various users and service providers.

V Suggestions on the Functions for Solution

Solution of the challenges described in Chapter IV requires not only direct use of trust services such as timestamp and electronic signature, but also a new system to connect physical space and cyberspace through the chained trust as shown in Figure 7. With this, we are heading for realization of the system capable of extending an area for connecting physical space and cyberspace which have not been used sufficiently, while continuing direct use of trust services for connecting physical space and cyberspace with trust.

If the newly suggested part of the layers is described more concretely, its configuration is as shown in Figure 10. In other words, TaaS can be sorted into the functions for facilitating use of trust, trust application service layer and trust service layer in addition to conventional functions produced individually, while each role of them is clarified. This leads to a new definition of the system to connect physical space and cyberspace. (Solution of Viewpoint 1)

A system to connect physical space and cyberspace through the chained trust and that to connect individual silo type trust worlds should be provided by promotion of use and interaction of trust application service layer and trust service layer by addition of the function for facilitating use of trust. (Solution of Viewpoint 2)

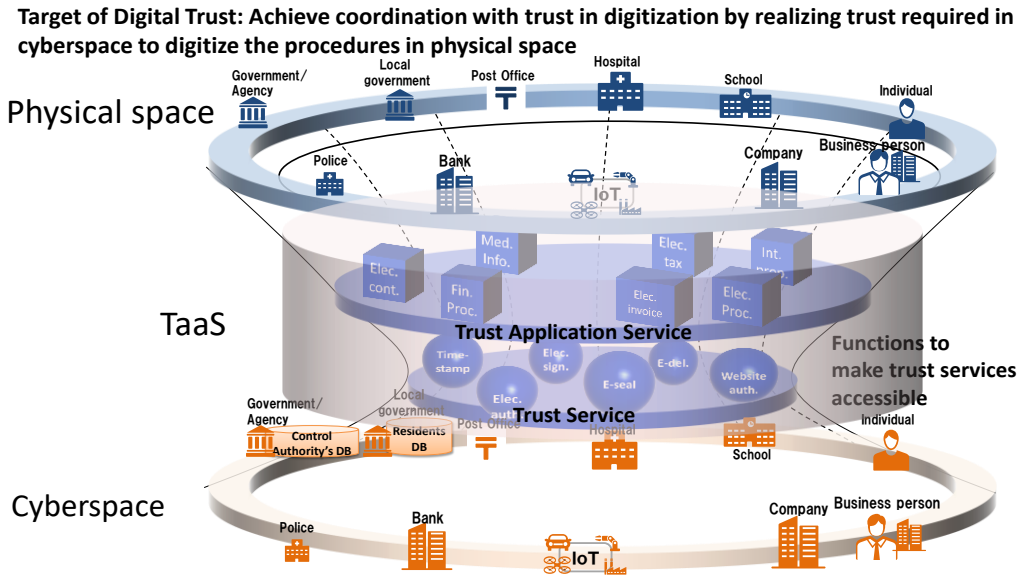


Figure 10 A new system to be realized: TaaS

Realization of the system solving these two points will enable users to process extensive procedures across corporates/organizations only in cyberspace and efficiently in a short period by only one log-in and to disseminate Society 5.0 and DFFT into the world. To achieve this, we propose "Trust as a Service (TaaS)" and explain it as follows.

1 What is "TaaS (Trust as a Service)" ?

TaaS is a means to solve Challenge ① to ⑤ for achievement of Digital Trust as shown in Chapter IV and is provided as service type. It has functions to address Solution ① to ⑤, each corresponding to Challenge ① to ⑤. The details of these solutions ① to ⑤ are described in Section V. 2, Configuration of TaaS.

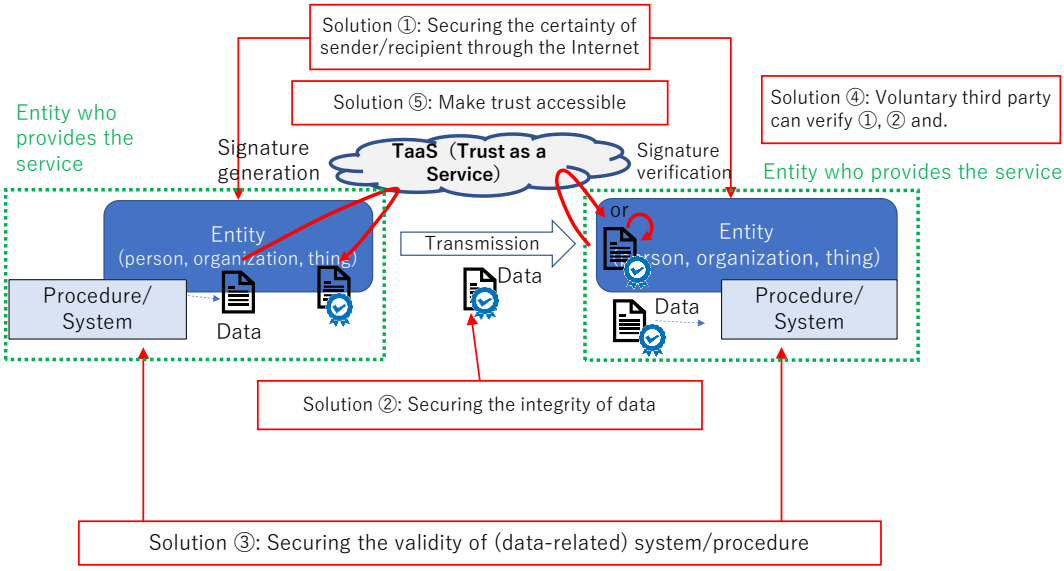


Figure 11 Realization of service type Digital Trust by TaaS

TaaS is the digital system to achieve Digital Trust. Figure 12 illustrates the effect provided by TaaS.

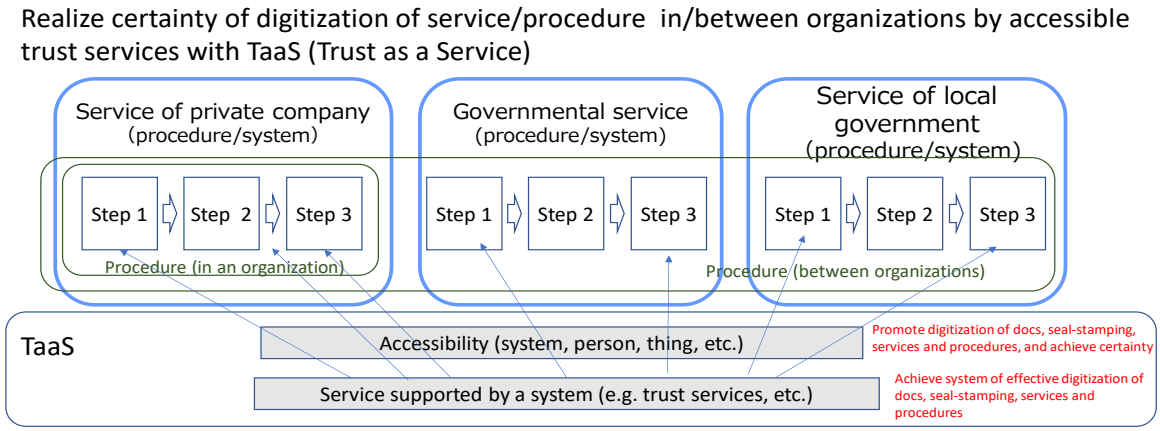


Figure 12 TaaS to achieve Digital Trust

TaaS aims to secure trustworthiness of data replaced in association with digitization of papers, seal-stamping, services and procedures and on enhancement of user-friendliness in digitization, and thereby on realization of a certain level of certainty over the whole digitized services and procedures.

Securing trustworthiness of data is realized by preparation of legal system in association with digitization of papers, seal-stamping, services and procedures. The system's effectiveness is secured by services supported by other legal system such as trust services. Firming up is realized by providing functions relating to user-friendliness such as remote type service for organizations, systems, persons and things using TaaS.

The former secures the systematic effectiveness of Digital Trust, and the latter makes Digital Trust widely available to organizations, systems, persons and things. With these, TaaS serves as a digital system to achieve Digital Trust, which provides a certain level of certainty over the whole digitized services and procedures.

2 Configuration of TaaS

Figure 13 illustrates the functional configuration of TaaS. TaaS consists of three elements, i.e. trust services, functions for facilitation of use and trust application services.

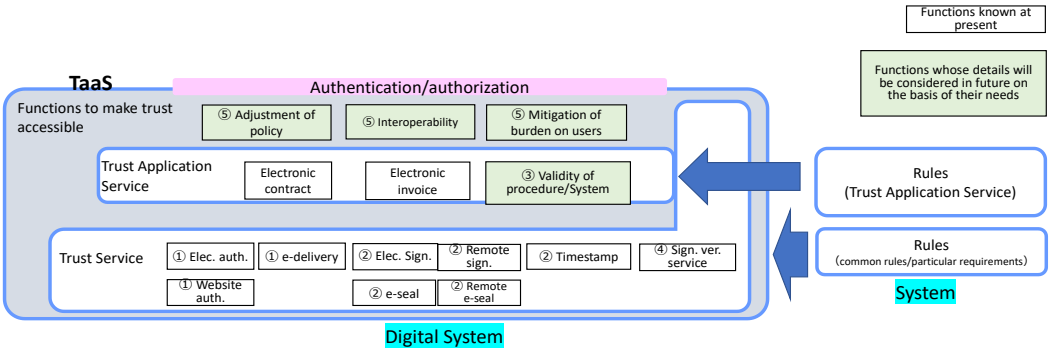
The trust services of TaaS in this White Paper refer to electronic authentication, electronic signature[30], remote signature, electronic seal[31], timestamp[32], electronic delivery, website authentication and signature verification service, etc. to achieve trust of data in cyberspace. These have been known as trust services in the eIDAS Regulation, etc. and support the effectiveness of system in association with digitization of papers and seal-stamping.

Functions for facilitation of use implement Solution ① to ⑤ in Figure 11 and establish the solidity by realizing user-friendliness of remote services, etc. for organizations, systems, persons and things using TaaS. These functions give solidity supported by effectiveness of system in association with trust services.

Trust application service relates to specific activities such as electronic contract, electronic procurement, etc. Trust application service provides solidity supported by effectiveness of system for specific activities covered by trust application, by interaction with trust service or function for facilitation of use.

All TaaS functions are accessible through authentication/authorization function required for confirmation of use for each function. In addition, they can provide a certain level of guarantee for functioning, if the trustworthiness meets specified standard.[33]

[30] It proves "entity/intention" as expression of intention.
[31] It proves "fact/information" as origin.
[32] It proves "existence/time" to indicate the existence of the signature.
[33] For this certain level of standard, it is essential to "prepare the standard for evaluation of trustworthiness" as an urgent issue.



Trust Application Service: Trust service-applied service
Trust Service: electronic authentication, electronic signature, remote signature, electronic seal, timestamp, e-delivery, website authentication, and signature verification service, etc.
Functions to make trust accessible: Auxiliary functions to make trust services accessible from trust Application Service, system service and actual space according to intended purpose

Figure 13 Functional configuration of TaaS

[Solution ①: Confirmation of sender's trustworthy level]

Generally, in order to confirm the party for exchange of data in cyberspace, the certainty of sender is secured by the receiver who verifies electronic signature given to the data. Like this, there is means just to verify the certainty of sender after the data recipient receives data and there is no system to verify the certainty of the addressee from sender's point of view. Therefore, there is a risk that the sender may deliver its data to unintended addressee. To solve the Challenge ①, a system to verify the certainty of receiver before the sender sends the data is necessary.

For example, such system may be: when the sender inquires on the basis of receiver's identified ID, the response is sent back to the sender to inform whether the receiver is trustworthy or not, as determined by the receiver's Identity Assurance Level (IAL) when the ID is issued to the receiver, and the certainty of receiver can be confirmed. Providing this kind of system as remote type service by API etc. will improve the accessibility for the system or users.

- Electronic authentication: Confirmation of existence of ID in cyberspace.
- Electronic Registered Delivery Service (ERDS): ERDS ensures integrity of sent and received data, data having been sent by identified sender, receipt by the identified receiver and accuracies of data and time of sending/receipt by QERDS.

[Solution ②: Securing the integrity of data]

It must be ensured that the sent and received data is identical and trustworthy. In this case, one point is whether the data is sent or received upon recognition designating of the access right to the data and information for authenticated ID. Another point is whether it secures that the data is not falsified between sending and receipt or not. A system to ensure these two points is essential.

For solution of the Challenge ②, we must consider a system to ensure the integrity of data issued by organization or thing by electronic signature in conjunction with establishment of the legal system, because the Electronic Signature Act, the legal basis in Japan, is intended for the subject as natural person. For cloud services granting electronic signature, introduction of system can be easier for users, if such services are provided as remote type service by granting electronic signature required for the system to ensure the data integrity and properly providing API for verification of signature.

On the other hand, when attribute data relating to issued ID is stored in, and made reference to, base registry by coordination with the system possessing the information, it is important to ensure data integrity of information and for user to use acquired information safely. This kind of case is described in Chapter V "6. Use Case of TaaS".

- Electronic signature (remote signature): To secure integrity of contents of data by individuals
- Electronic seal (remote e-seal): To secure integrity of contents of data by organizations
- Timestamp: To secure integrity relating to time when the data existed.

[Solution ③: Authenticity of procedure system]

Trust of data in cyberspace must be secured by clarifying who, for what, and when the data is produced (e.g. who provide the data and whether the data is tampered or not). This requires systems to ensure that the data was generated by proper procedure and to assure the certainty of module components composing the system. In short, clarifying "how" the data was produced ensures the authenticity of procedure to handle the data.

For example, in case more than one organization or companies involves in procedure, multiple person, organization and things involve in service or supply chain or data generation procedure, not only the certainty of them but also their order is important. A solution of this, for instance, is a function which secures the authenticity of procedure by assuring the certainty of identity by electronic signature and the time of data manipulation by timestamp (trustworthiness of time of existence), where such electronic signature and timestamp are given whenever the data is manipulated by related person/organization (entity/intention) or thing (fact/information). Providing this kind of system as remote type service by API, etc. will improve easiness of introduction of system for users.

The publication titled "Q&A for seal-stamping" dated June 19, 2020 and issued by the three ministries (the Cabinet Office, the Ministry of Justice and the Ministry of Economy, Trade and Industry) illustrates some ways to secure the means for proof the authenticity document. In this publication, the process leading to formation of contracts and billing such as "storage of records of e-mails communicated with customers" in continued transaction and "storage of process of formation of documents and contracts (e-mails and communication on SNS)" is described as a means to verify that the formation of document is authentic.

This Q&A refers to sent and received e-mails and SNS as a means of archive of records. This function makes it possible to store information with certainty including the procedure of formation of documents as a process and allow us to select the means with higher certainty and convenience to prove the authenticity of documents.

As mentioned above, there are various ways to secure authenticity of procedure or system, but we will consider more details depending on the needs.

[Solution ④: Voluntary third party verification]

Digital Trust requires that voluntary third party can remotely verify whether the system to solve the problems ① through ③ are used. For this, a system enables voluntary third party to verify the certainty of addressee, data integrity and the authenticity of procedure system is essential. Accessibility to organization, system, human and things is achieved by providing this kind of system as remote type service by API available to voluntary third party in addition to conventional local verification, while keeping above a certain level of certainty realized with Digital Trust through third party verification not depending on the system service used by user but using data only. In addition, by making it verifiable by voluntary third party, the data can be verified not only at the time of generation, transmission and use but also at some time in the future. In other words, if voluntary third party can verify the data after using it, as well as during use of it for service or procedure, the level of certainty can be enhanced.[34]

For example, in verification of certainty of the data receiver in ①, the evidence of judgment of the result, i.e. “whether the counterparty is trustworthy or not”, returned to the user is presented to the third party. In this case, information according to the standard such as Identity Assurance Level (IAL) of the data receiver or Authenticator Assurance Level (AAL) showing the certainty of authentication is presented. For organization, thing, procedure or system, the legal basis for judgment of trust is not established in Japan. Therefore, establishment of legal systems is required.

[34] One of known realization means is Long term electronic signatures, which is defined in RFC3126 (https://datatracker.ietf.org/doc/html/rfc3126), etc.

[Solution ⑤: Accessibility to Trust]

By ensuring accessibility[35] to introduce and make use of trust services or trust application services, promotion and dissemination of digitization with trustworthiness are achieved. To achieve accessibility, we aim to achieve optimization of the society-wide cost of digitization with secured trust by providing a system to solve challenges common in many users as Trust as a Service.

The present situation of considerations is as follows, and we will consider more details depending on the needs.

- Adjustment of policy: Considering in depth the functions to support introduction of trust services according to the rules and scheme depending on severity of procedures in physical space, in order to mitigate the burden on users for such introduction of trust services.
  - In realization of certain procedure by connecting more than one trust service, the functions we assume are those to unify the policies of those trust services.
- Interoperability: Achieve to promote and disseminate digitization with secured trust with ensuring compatibility of API, data, services and applications, etc.
  - Example of compatibility between services: If an electronic contract service used by a company willing to bid using electronic contract is not compatible with the service used for bidding, the company may not be able to participate in the bidding. (This means the compatibility of electronic contract affects the business.) It is considered to solve the problem with another service compatible for the electronic contract. (e.g. common service for registration of user key and ID used for electronic contract.)
  - Example of compatibility of service and application: If there is any difference of system of uniquely identifiable ID/number for person or organization between the service of CA and business application, it is not possible to determine the authenticity of verification result of electronic signature or electronic seal. It is considered to solve problem by service which achieve conversion of such systems of uniquely identifiable ID/number for person or organization.
- Mitigation of burdens on users: Though electronic signature and timestamp have been used by now, it is required for users to (i) generate data, (ii) grant trust[36] (e.g. expressing intention of sign by authentication and log-in to signature service and electronically signing the data on the service's UI and uploading the signature data to the service.) and (iii) sending the signed data to the addressee. Among them, the step (ii) is a burden on users. Therefore, it is achieved to mitigate the burden by simplifying users' steps through implementation of (ii) behind (i) in usual operations by users (e.g.

[35] It is in concert with "human-friendly digitization" in Attachment 4 for the 9th Meeting on Growth Strategy of the Cabinet Secretary", https://www.cas.go.jp/jp/seisaku/seicho/seichosenryakukaigi/dai9/siryou4.pdf

[36] It refers to securing the other party's authenticity, data integrity and validity of procedure/system.

preparation of document to be submitted to the administration agencies). Concretely, a system to limit the steps to (i) and (iii) [i.e. (ii) is implemented behind that of (i)] as shown in Figure 14 is essential. It achieves to promote and disseminate of these services by mitigating users' burden and certainty by control of human errors.

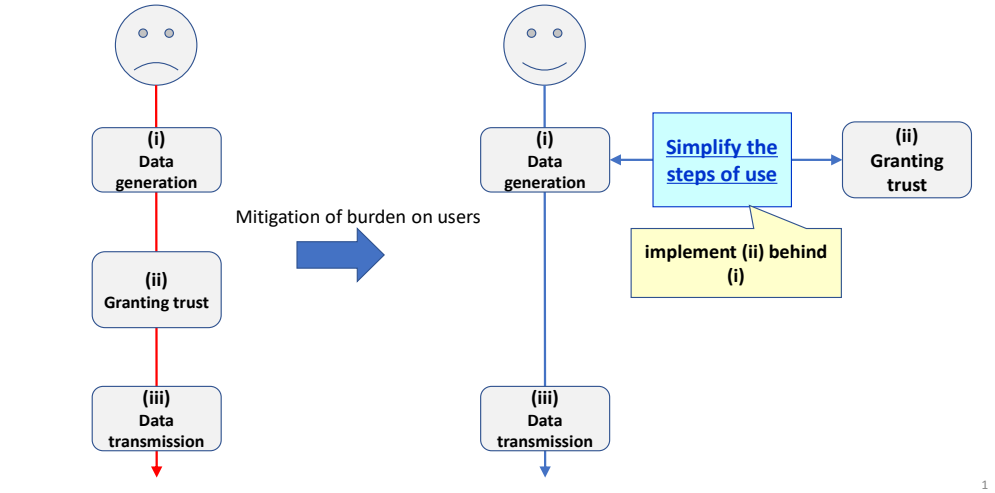
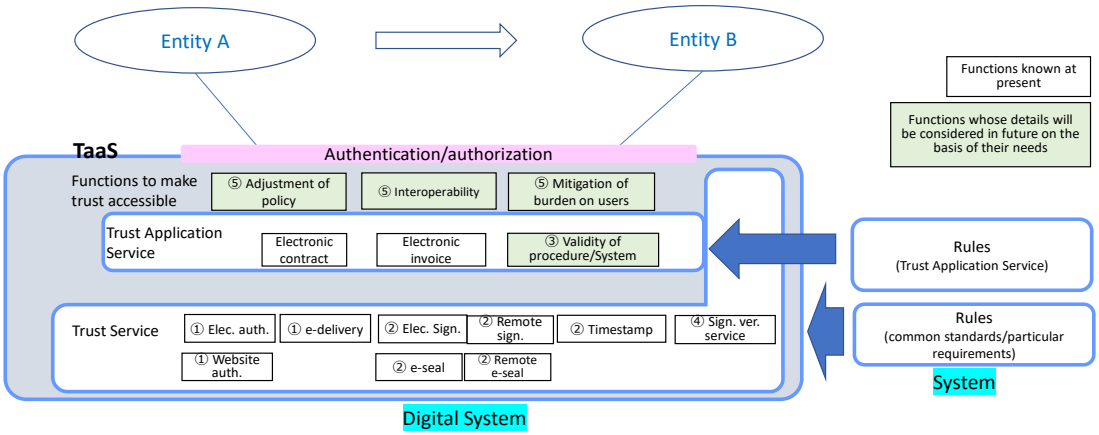


Figure 14 The system to achieve mitigation of burden of users

3 Image of use of TaaS



Trust Application Service: Trust service-applied service
Trust Service: electronic authentication, electronic signature, remote signature, electronic seal, timestamp, e-delivery, website authentication and signature verification service, etc.
Functions to make trust accessible: Auxiliary functions to make trust services accessible from Trust Application Service, system service and actual space according to intended purpose

Figure 15 Basic image of use of TaaS

Figure 15 illustrates the basic image of use of TaaS. Invoking TaaS through API, etc. can achieve to secure the trust in transmission of data as digitization in place of signature or seal-stamping from entity A to entity B. While securing trust provides legal effectiveness on digitization of papers/seal-stamping, it is achieved by a function to make trust accessible and provide a certain level of certainty to the entire digitized procedures.

Since TaaS serves as a service for achievement of Digital Trust to support Society 5.0, it is considered to often link with data linkage infrastructure or application for individual operation. This is illustrated in Figure 16.

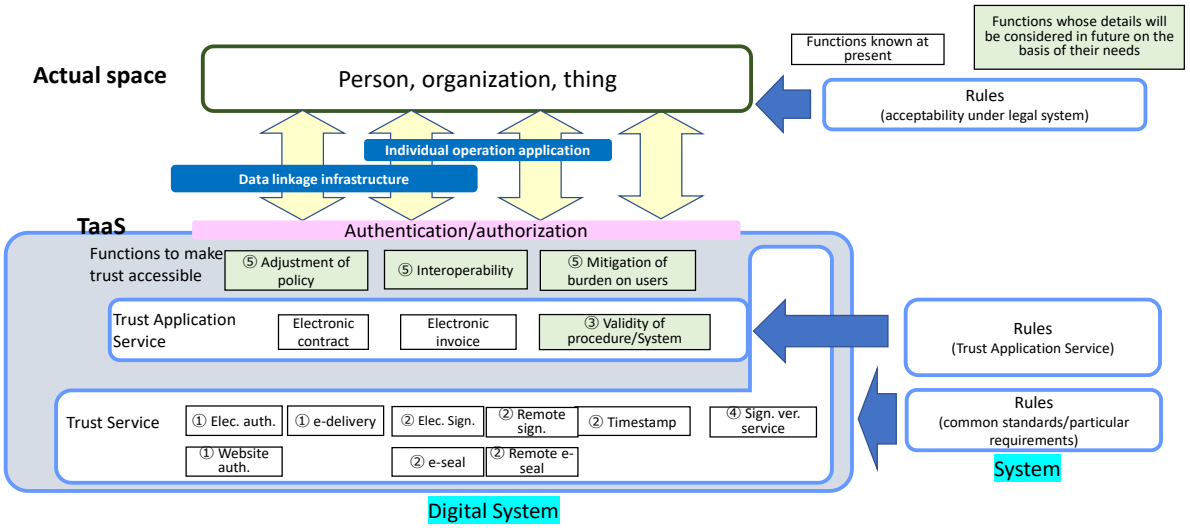
Data linkage infrastructure is intended for making use of data across sectors which is promoted by the Japanese government to achieve Society 5.0. In a broad sense, it enables data linkage owned by various stakeholders involved in the public and private sectors and allows cross-sectoral use of data.

Trust application service enables to secure trust of the operation of application itself by meeting certain level of trustworthiness. On the other hand, an application for individual operation is optional. Using TaaS secures trust of data processed by such application.

In some case as shown in Figure 16, the patterns in which an entity such as person, organization, thing uses TaaS are (i) and (ii) below. It can use TaaS through authentication/authorization required for each TaaS function. The appropriate use pattern depends on use case.

(i) Direct use

(ii) Through either of individual operation application or data linkage infrastructure, or both



Trust Application Service: Trust service-applied service
Trust Service: Electronic authentication, electronic signature, remote signature, electronic seal, timestamp, e-delivery, website authentication and signature verification service, etc.
Functions to make trust accessible: Auxiliary functions to make trust services accessible from Trust Application Service, system/service and actual space according to intended purpose

Figure 16 Image of use of TaaS (coordination with data linkage infrastructure/individual operation application)

4 Benefits of TaaS

- Benefit 1: Certainty

  With digitization of signature and seal-stamping used for procedure, if the function of TaaS with ease of use realize verification of authenticity of counterparty and integrity of data, and verifiability of validity of relevant procedure/system, the services and procedures of companies and local governments can be certain. For example, it can be easily confirmed the authenticity of electronic procedure by connected one-stop or when and what organization issued electronic invoice through online service.

- Benefit 2: Efficiency

  When conventional procedures, which have relied on papers, telephone, facsimile, etc. until now, are carried out as digitized service, the efficiency of entire procedure will be improved with making them automatically executable in a combination of machine-reading, etc.. For example, with regards to data in base registry possessed by public agencies, local governments or companies, if verification of its integrity and verifiability regarding validation of procedure/system concerning data distribution are secured by achievement of Digital Trust,

connected one-stop electronic procedure and private online service (using registration information stored in base registry) can be more efficient.

- Benefit 3: Risk management
  Declaration that services and procedures provided by any organization or person comply with correct procedures specified in given working rules, contracting procedures, etc., contributes to risk management. It is expected that this way of thinking can be used for verification whether the entity, procedure, or system satisfies with trustworthiness[37] in supply chain.
- Benefit 4: Check of doubts
  In companies, public agencies and local governments, there are many transactions such as contract with the counterparty, claims for funds under the contract, payment upon receipt of invoice, and so on. Since they must do business with various clients, in some transactions, they may have doubts or get involved in disputes. It is real that we cannot eliminate such issues. It is needless to say about the importance of taking preventive measures against the issues with Digital Trust. To prepare for such cases in parallel, another important thing is to ensure that we can prove the authentic provenance of documents we rely on (including digital documents) with taking preventive measures.

5 Convenience of TaaS: Online issuance of ID at high Identity Assurance Level and remote signature

In this White Paper, we consider that high Identity Assurance Level (IAL) and realization of accessibility are important for dissemination of TaaS, and Figure 17 gives an example. It is a combination of identity authentication of remote ID and remote signature, and the steps (1), (2) and (3) in Figure 17 are realized in one-stop and on-the-fly approach. It would significantly facilitate the use of TaaS and contribute to dissemination of trust application.

(1) An applicant applies for use to the trust application.
(2) Along with (1), Certificated Authority (CA) checks the identity online with Individual Number Card, etc. and base registry such as corporate registration information, national qualification database, etc. and issues an electronic certificate with the corporation's name and with attribute of national qualification in remote signature service.
(3) The user can use electronic signature in one-stop approach in the cloud through trust application.

[37] For example, ISO/IEC JTC 1/WG 13 defines trustworthiness as "the ability to meet stakeholders' expectations in a provable, verifiable and measurable way" and describes that "verifications is required to ensure that stakeholders' expectations are met."

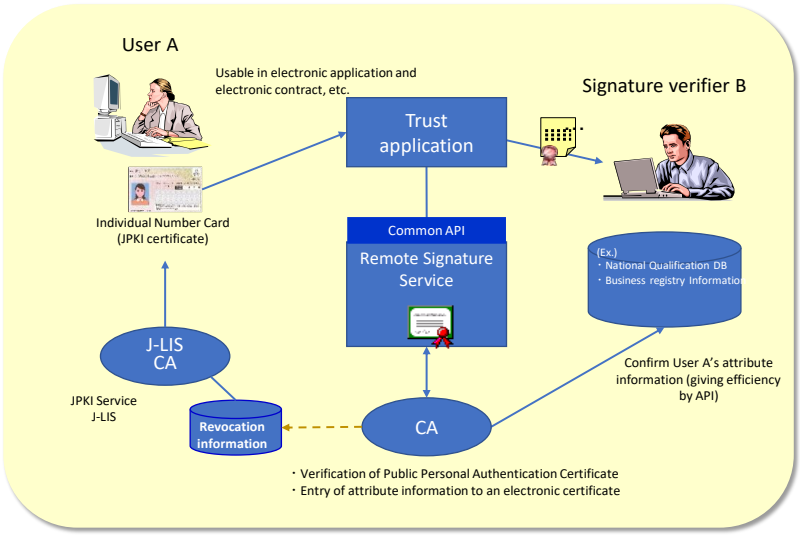


Figure 17 Example of enhancement of both identity check level and accessibility (remote signature)[38]

Figure 18 below illustrates the relationship between ID scheme and electronic certificate. In the definition of Article 1 in ”Provisions on the Use and Cross-border Recognition of Identity Management and Trust Service” issued by UNCITAL, "Identity" is defined as "a set of attributes information that allows a person to be uniquely distinguished within a particular context"[39], as similarly defined in the eIDAS Regulation. The most distinctive feature of identity, i.e. ID, manipulated in TaaS is surely linked with natural person, organization, equipment, etc. in real society, and its integrity is secured, because it is stored as the subject's attribute information in a public key certificate. Also, the identity is secured by electronic signature or online authentication with private key, and the assurance level is specified with reference to Identity Assurance Level (IAL) of NIST SP 800-63.

[38] Extracted from Attachment 4 for "The MIC's Meeting on consideration for installing My Number Card's functions in smart phone, etc.", https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/02ryutsu02_04000356.html

[39] “Identity” means a set of attributes that allows a person to be uniquely distinguished within a particular context.

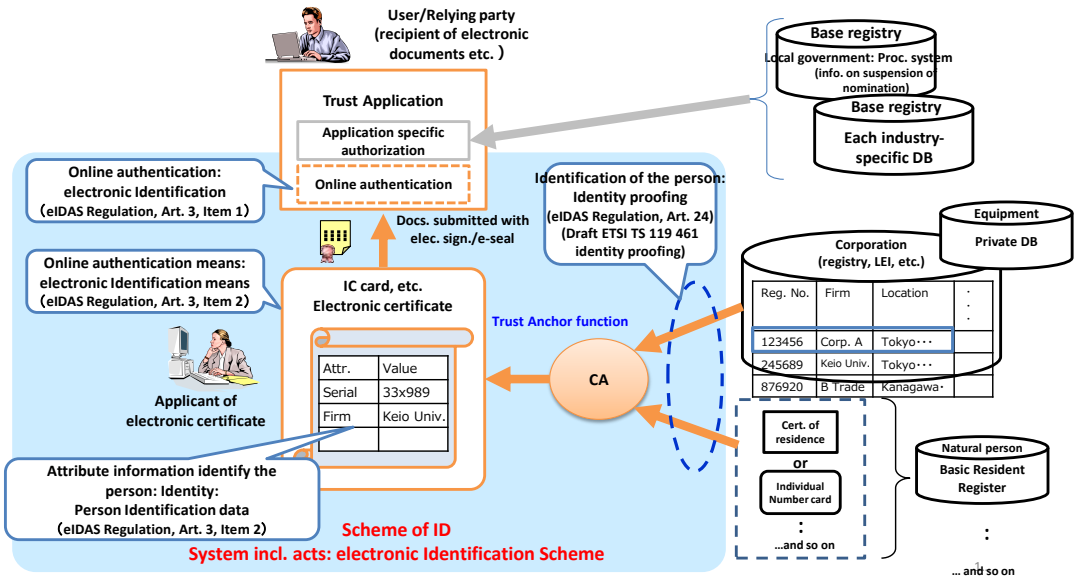


Figure 18 Relationship between ID scheme and electronic certificate

On the other hand, IDs used in general websites, such as Google, Amazon, Facebook, Apple, are not strictly linked with individuals in the real society, but with their payment information (credit card, etc.) are used as required.

6 Use Case of TaaS

This chapter describes the expected use cases how users use TaaS.

For servitization, TaaS make the functions from ① to ④ in Figure 11 to API and allow the commonly access through trust application, data linkage infrastructure, etc. By This, TaaS can be used as cloud service regardless of service or type of business. In addition, these APIs should be cogitated to allow users to use TaaS without thinking about its complicated process.

(1) Opening a corporate bank account

Figure 19 illustrates the procedures for opening a corporate bank account used for explanations in Figure 1 and Figure 5, which summarize the current case of using paper documents and the case using transaction by TaaS.

In the current procedure, the paper documents are seal-stamped by their issuer to secure their trustworthiness and submitted to a bank. After a bank receive the documents, a person in charge checks them. If TaaS is used for this procedure, a corporation can digitally request the bank to open its account

and a request to disclose corporate information is sent to the public agency at the same time. Then the corporation can continue the request to open the bank account with the information provided by the agency. With this, the bank that receive the information can judge its accuracy on the basis of all the machine-readable information without human intervention. In short, both the public agency and the bank can go through procedure correctly and efficiently without human intervention.

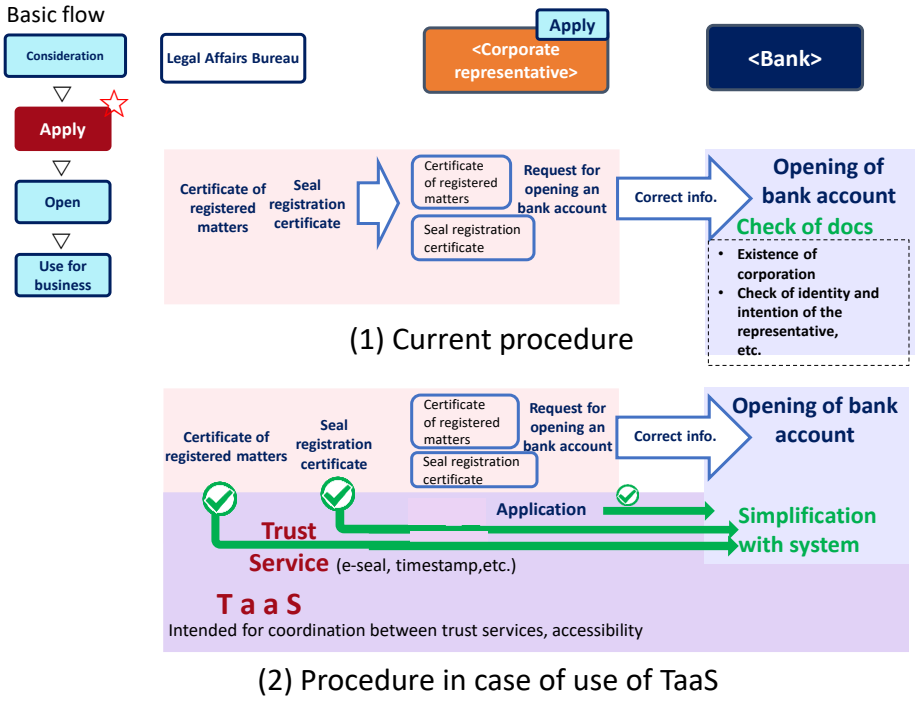


Figure 19 Comparison between the procedures for opening a corporate bank account

(2) Digitization of invoice

Figure 20 illustrates the use case of TaaS regarding digitization of invoice, taking into account how the functions from ① to ⑤ should be used.

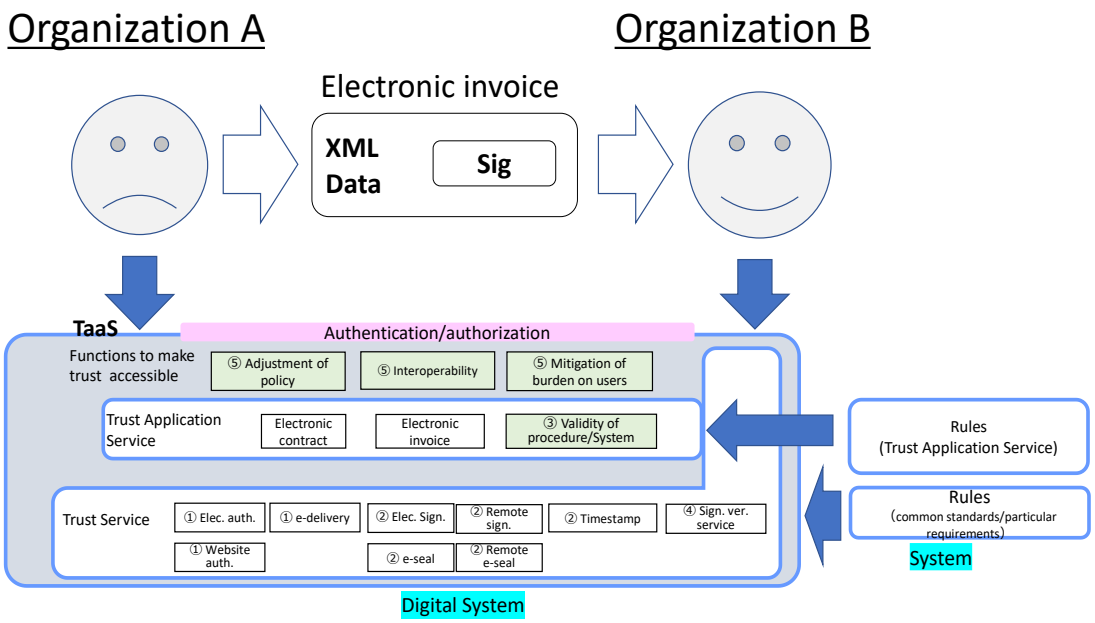


Figure 20 Use case of TaaS for electronic invoice

Figure 20 shows a use case where an invoice is prepared by a person in charge who belongs to Organization A and delivered to Organization B. Most of digitized invoices employs a data format like XML, and in many cases, it can incorporate electronic signature due to its specification. For generation and receipt of data, its proof is given and verified from the five viewpoints for suggestion of functions. In short, they realize: (1) checking who is involved in the process; (2) preventing tampering of data; (3) (if Organization A declares the procedure for contract/work) checking in what procedure the data was prepared; (4) checking the basis of trust, and (5) check it is not relying on human skills.

[Resulting benefits]

The functions of TaaS provide certainty of issuing and receiving procedure of electronic invoice for both Organization A and B (Effect 1), improved efficiency of issuing and receiving task of electronic invoice for both Organization A and B (Effect 2) and declaration that Organization A performs its task according to specified procedure (Effect 3), when Organization A charges a large amount of money, or the like.

In addition, such a payment process linked with billing is also effective for payment of insurance claim. For instance, even if the payer take out insurance service but the addressee not, a voluntary third party verification is available by ④ and similar effect is expected.

(3) Form of coordination of TaaS (decentralized TaaS interaction)

As shown in Figure 1 and 2 of Chapter IV, various procedures are established across services of diverse organizations. To deal with them as digitized procedures, coordination of these are required while using data possessed by each of them.

The form of realization of TaaS in which the examples in Figures 1 and 2 to be realized should not be one centralized TaaS, but each TaaS existing in the national and private sectors must coordinate with each other. Figure 21 illustrates the picture of coordination of TaaS between the national, local government and financial institution (decentralized TaaS).

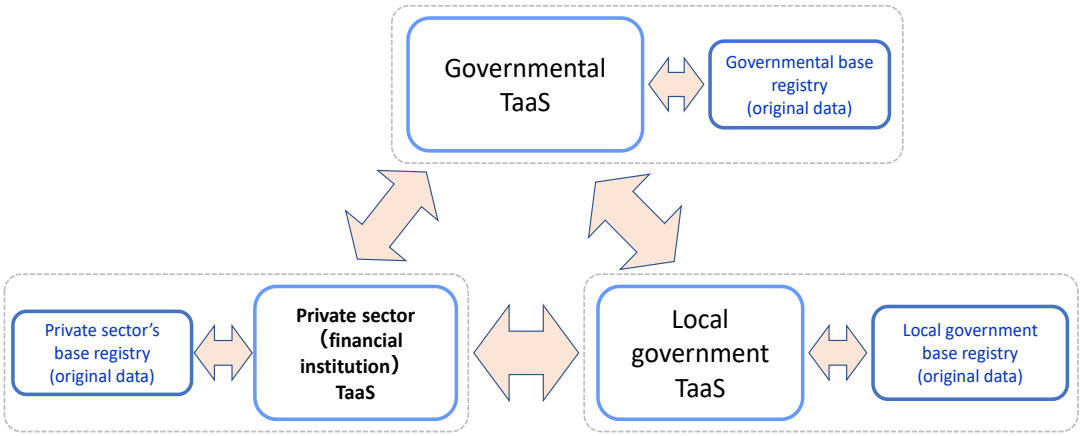


Figure 21 Picture of form of coordination of TaaS

Based on this image, the following describes use cases of interaction with base registries of the government and municipality.[40]

[40] It is assumed that protection of personal information and that of confidentiality are separately considered in TaaS and base registry (including interaction of base registries). In interaction between TaaSes, however, the important thing is to realize compatibility as a mashup type service (a new service by combination of several services) to avoid occurrence of conflict between the policy of protection of personal information and that of confidentiality protection, resulting in unintended access in case of access to the base registry.

(4) Governmental system and base registry

Figure 22 explains the form of use of TaaS with an example of the governmental system and base registry.

In Figure 22, the governmental base registry storing various kinds of attribute information coordinate with TaaS. Providing electronic seal for information in the base registry brings assurance that the original data in the governmental base registry has not been tampered, and achieve Digital Trust essential to rapid transition from physical space to cyberspace.

Also, TaaS can be used to add information from governmental agencies to the governmental base registry or to update it, and to ensure that the addition or updating is made by proper application and procedure (relating to ③ validity of procedure/system). In addition, it serves to ensure the integrity (relating to ② data integrity) that the data source in the base registry (relating to ② data integrity) is not tampered.

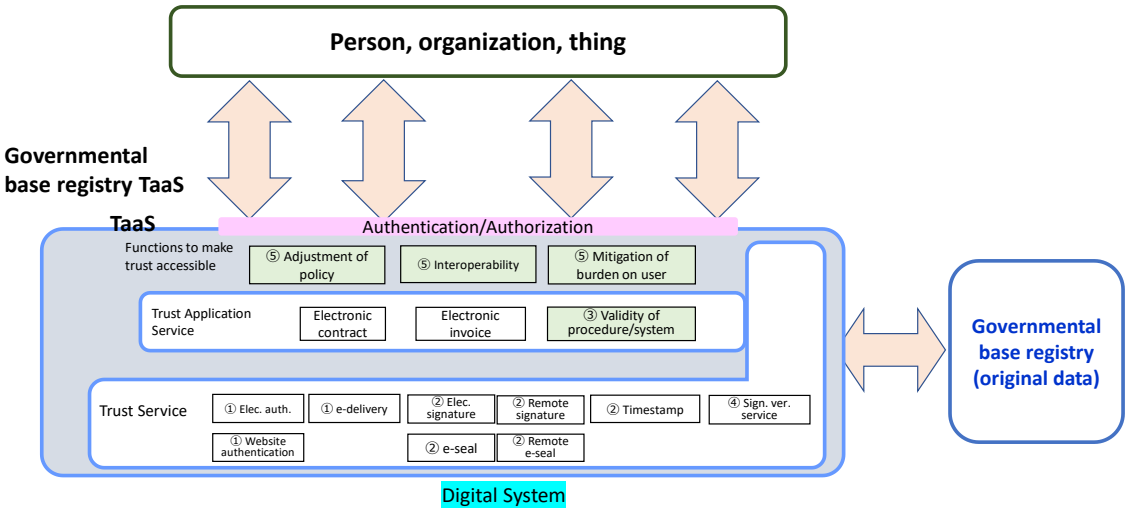


Figure 22 Coordination between the governmental system and TaaS

(5) Cooperation between the national and private sector's system and between the national and local government system

Figure 23 explains forms of cooperation of TaaS with an example of coordination of private TaaS system, governmental TaaS system and governmental base registry.

As a form of realization of TaaS, there is not one centralized TaaS, but it is assumed that multiple TaaS coordinate each other as shown in Figure 23. For example, multiple governmental TaaS and private TaaS are considered to be operated separately, and a social system is configured in decentralized TaaS environment.

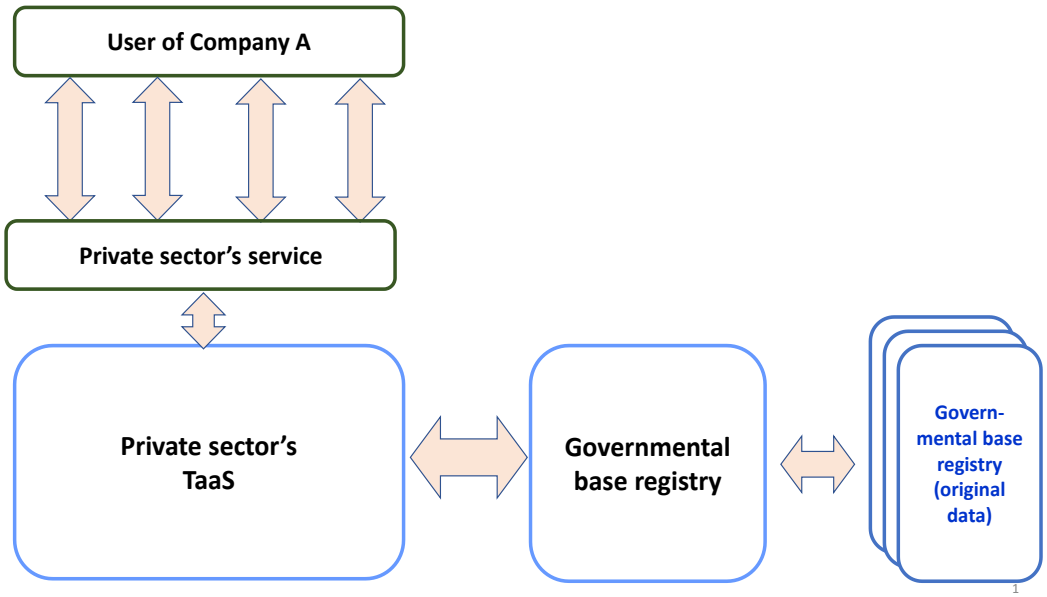


Figure 23 Cooperation of the public and private sectors through TaaS

In this environment where TaaS is decentralized, if, for example, Company A receives a request of information possessed by the government (e.g. information stored in the governmental base registry), it is possible to obtain necessary information by coordination of private TaaS with the TaaS of governmental base registry as necessity.

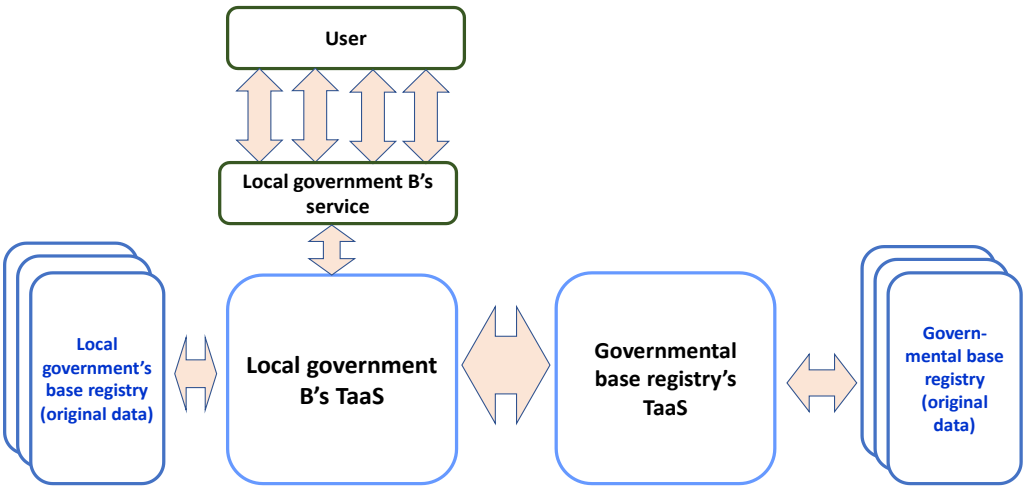


Figure 24 Cooperation between the national and local government through TaaS

As shown in Figure 24, the similar configuration can also apply to the cooperation between the national and local government. This ensures the integrity of information possessed by the national and local government respectively and can achieve Digital Trust for connected one-stop approach, providing efficient and certainty processing of various procedures.

(6) Confirmation of corporate activities by using corporate base registry

Figure 25 illustrates the use cases of confirmation of corporate activities by using corporate base registry. Interaction between TaaS and corporate base registry and confirmation of published attribute data (privacy mark, ISO 9000, ISO 14000, etc.) establish an infrastructure for confirmation of corporate activities by reference to the published attribute data, data used for purchasing procedure, etc.

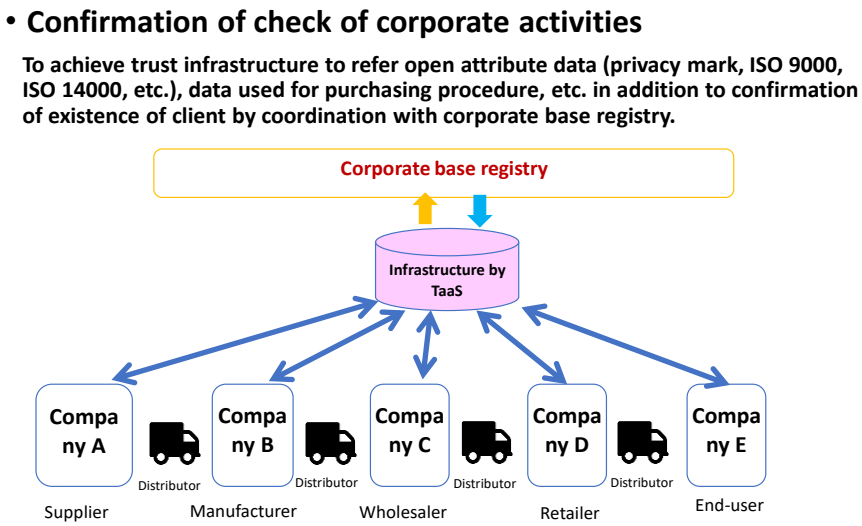


Figure 25 Check of corporation activities with coordination of base registries

[Resulting benefits]

The functions of TaaS realize efficient check of doubts on client corporation through online service (Effect 4 and 2). In addition, recording of negotiation process, while using "⑤ Accessibility to trust" offers accessibility, thus certainty to business and contracting activities (Effect1).

(7) Coordination of information by TaaS in financial institutions

In some cases, financial institution must make professional decisions with various kinds of public and private information such as credit examination for financing.

For instance, for real-estate registration information for placing a mortgage, it is digitized at present and available on the Internet through registration information service. However, the information is "read-only" and does not prove its contents while certificate of registered matters does so. Then, coordination of base registry and TaaS enables the digital distribution of real-estate registration information, which naturally requires certainty of information.

Moreover, coordination of TaaS with public information such as income information from year-end adjustment/final tax declaration, relationship with anti-social force can improve the reliability of professional decisions.

This coordination will also improve the convenience of exchange of reliable information between private sectors, e.g. results of real-estate evaluation, coordination of information with insurance companies, notice of result, etc., as shown in Figure 26.

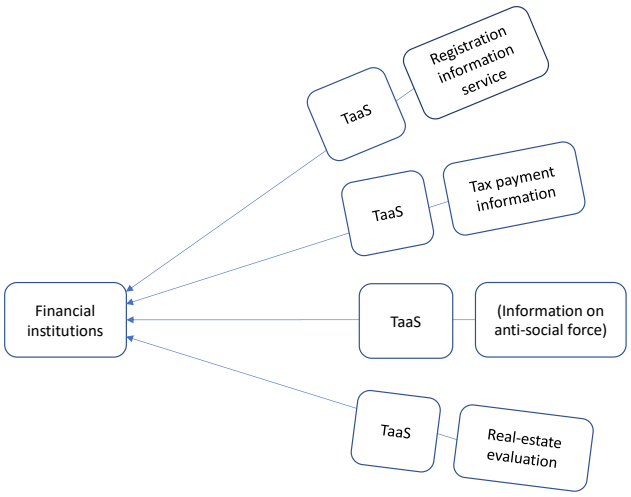


Figure 26 Coordination of information by TaaS in financial institutions

(8) Records of negotiation process in business and contracting activities

In business negotiation from sales activity to conclusion of contract, we often prepare more than one quotation or review the contract conditions. During such negotiation, if it is required to proceed with conclusion of contract with the party of concern about unfaithfulness for performance of contract or insufficiently preparation of control system, one of possible measures to claim the validity leading to the conclusion and restrict the cost and loss arising from the problem is to record the information on negotiation process for the contract while taking great care to its contents.

As shown in Figure 27 below, since the use of TaaS secures the correctness of originator of information on negotiation process and its contents and makes them verifiable by third party, it is possible to strengthen the claims and count on a breaking effect on the counterparty not to do unfair acts.

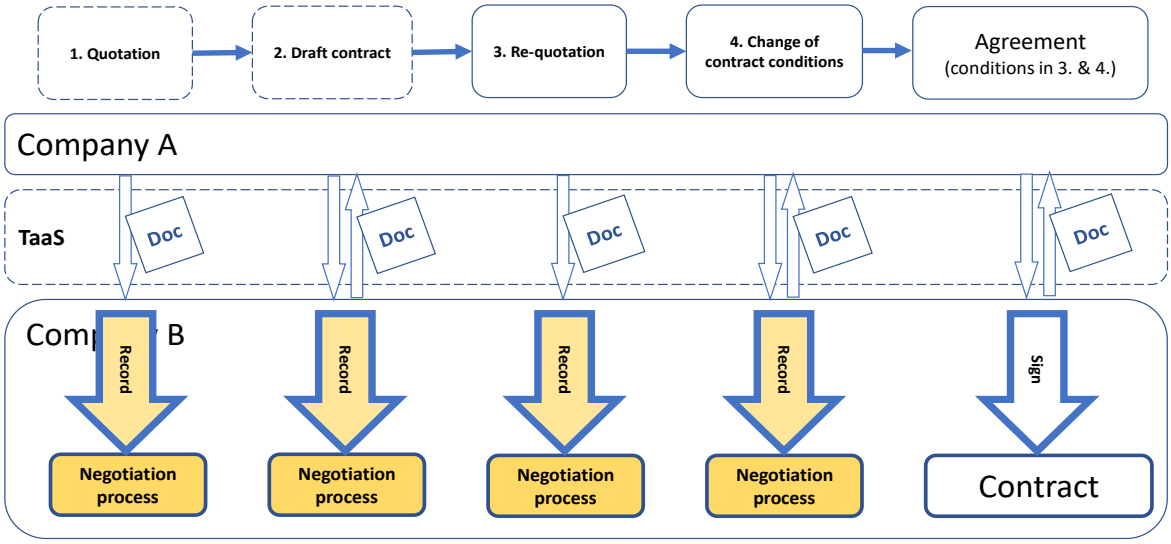


Figure 27 Records of negotiation process in business and contracting activities

[Resulting benefit]

With the functions of TaaS, the records of negotiation process in business and contracting activities will allow Company B to check any doubt on the negotiation process (Benefit 4). In addition, recording of negotiation process in conjunction with "⑤ Facilitation of use of trust service" will enhance the accessibility, leading to bringing certainty to business and contracting activities (Benefit 1).

VI Considerations for future

1 Considerations toward publication of next White Paper

- We plan to publish an upgraded White Paper making the system aspects clearer in future. To accelerate dissemination, we want to find the use cases and needs.
  - ➢ We will further review the suggestions on functions in Chapter V and refine them.
    - ✧ Refinement of various kinds of solution relating to function to make trust accessible (adjustment of policy, interoperability and mitigation of users' burden), etc.

- Aftertime, we will consider the requirements for ensuring the trustworthiness of digitization by TaaS between organizations or sectors (public, quasi-public, private) and in consideration of international cooperation.
  - ➢ Ideal way of authentication/authorization of TaaS API: We must consider the ideal way of authentication/authorization on the basis of data owner's policy, nature of data, etc. as well as the viewpoints of person, organization and thing using TaaS.
  - ➢ Concept of trust anchor with interaction between TaaS, and ideal way of API: We must consider how the trustworthiness is established between TaaS operated in different organizations, and in doing so, how and what data is authorized between them, on the basis of data owner's policy, nature of data, etc.

- We plan to consider for what procedure and at what assurance level trust application services and trust services are required.

- We also plan to consider a comprehensive framework to cover any technical innovation to achieve Digital Trust and detailed plans capable of ensuring business continuity for users.

2 Actions to be taken for social implementation

For the purpose of social implementation of Digital Trust, the following is required from the viewpoints of preparation of environment for use and rulemaking.[41]

- Development of scheme of comprehensive trust infrastructure (TaaS infrastructure)

We should immediately consider the scheme of trust infrastructure securing integrity of various kinds and large amounts of data and supporting trustworthy interaction and distribution of data which connect highly integrated persons, organizations, things and systems by Society 5.0, from the following viewpoints:

- legislation of effects of proof of intention by each trust service (electronic signature), proof of origin (electronic seal), proof of existence (timestamp), etc.;
- drafting of technical/operational standards according to assurance level and creation of accreditation scheme after sorting out common/particular requirements horizontal and cross-sectional for each trust service;
- establishment of agency who drafts, maintains and updates the above technical standards along with Japanese policies;
- institutionalization of verification of machine-readable trust anchor (trusted list) capable of automatic verification of a large amount of flowing data using trust.

For dissemination, we should immediately consider the following.

- Improvement of usability of trust services
  - data retrieval on condition that certification of origin is secured by base registry, and programmable interaction
    (e.g. when information such as attributes of the corporate's representative, corporate registration is retrieved from the base registry, granting electronic seal of base registry operating agency allows to use the data with secured certification of origin. In addition, improvement by automatic interaction with subsequent system can be expected with acquirement through API).
  - Promotion of dissemination of cloud type trust application service
  - Interaction with trustworthiness between various applications

[41] These viewpoints are based on the arguing points of "framework of trustworthiness" in the first summary in the Data Strategy Task Force below and further advanced.
・Attachment 1 for the 7th meeting of Data Strategy Task Force, the Cabinet Secretariat, IT Comprehensive Office (May 26, 2021) https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou1.pdf

- Interoperability of trust services
  - international mutual recognition of equivalence of system to confirm legal aspects, supervision/assessment by nation, standard technique and trust anchor to enable interoperability of trust services
  - Presentation of international cooperation policy aiming at harmonization with foreign countries and road map

- Drafting technical specifications for user's verification of accredited trust service, preparation of exclusive marking scheme of qualified mark and consideration of TaaS registration scheme for using accredited trust services, etc.