FY 2022

Supply Chain Trust Issues and Recommendations

Ver2.0

MARCH 2023

JDTF SUPPLY CHAIN REFORM COMMITTEE

Change log

No	Date	Version	Changes
1	July 1, 2022	1.0	Initial release
2	Feb 24, 2023	2.0	Chapter I. Added assumed audience in the last paragraph; explained differences between White Paper 1.0 and White Paper 2.0. Chapter II. Clarified the wording of the scope in contrast to [METI '19]. Added a scope diagram. Section V-3. Added section V-3-2; added the concept for realization. Revised section V-3-3; clarified the overall picture of how to achieve this. Revised section V-3-4; clarified the meanings of “Trust Stores” and “Digital Evidence.” Section V-4. Added new information items: - “Trustworthiness Information,” - “Digital Evidence,” and - “Linkage Information.” Section V-5. Newly added images of the realization of the target image. Explained that the information items added to Section V-4 can achieve the goals in Section V-1. Chapter VI. Separated from the former Section V-4 and upgraded to Chapter VI. Clarified how to realize use cases. Chapter VIII. Additional updates added since the White Paper 1.0 version.

Contents

I. Introduction 3
II. Scope: supply chain trust for safety and security....7
III. Changes in environmental conditions/circumstances....9
IV. Issues to resolve....14
V. Measures to resolve the issues....16
1. Goals of supply chain trust 16
2. Requirements....17
3. Implementation methods....18
3-1. Classification of the trust formed in supply chains....18
3-2. Concepts for realization 19
3-3. Overall picture of the realization methods 21
3-4. Trust Store and Digital Evidence Store....23
3-5. Trust as a Service (TaaS) 26
3-6. Base Registry 27
4. Information items handled with the supply chain trust 28
4-1. “Trustworthiness Information” items....28
4-2. “Digital Evidence” items 30
4-3. “Linkage Information” Items....31
5. Visualization of the goals to be realized....32
5-1. Visualization of Goal 1 32
5-2. Visualization of Goal 2 33
5-3. Visualization of Goal 3 34
5-4. Visualization of Goal 4 35
VI. Use cases 37
1 Mechanisms to ensure the trustworthiness of data coming out of the equipment 37
2 Efforts to reduce carbon emissions throughout the supply chain 46
3 Identifying security measures throughout the manufacturing supply chain....54
4 Usage scenarios and effects of Trust as a Service (TaaS)....59
VII. Recommendations....61
VIII. Conclusions....63

I. Introduction

To address the various challenges faced by the international community in pursuing sustainable development goals, the Japanese government advocates the realization of Society 5.0,[1] a society that balances economic development with the resolution of social issues by incorporating digital technologies such as AI (Artificial Intelligence), 5G (5th Generation), and IoT (Internet of Things) into all industries and social life.

To realize Society 5.0, it is beneficial for various stakeholders to cooperate in establishing mechanisms that ensure trustworthiness through harmonization among countries, such as the European eIDAS (Electronic Identification, Authentication and Trust Services) Regulation,[2] to achieve international distribution of data. The Government of Japan has addressed the two key points of free and open data distribution and data security and safety as Data Free Flow with Trust.[3]

To realize the safe and secure society that Society 5.0 aims for, not only data, but also the supply chains that provide products and services to that society must be safe and secure. A supply chain is a set of resources and processes to which orders are directed; it includes vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and others involved in the manufacturing, supply, processing, handling, delivery, and provision of goods and related services. To make the supply chains safe and secure, the processes of providing products and services to consumers must also be safe and secure.

This white paper focuses on ensuring supply chain security and safety (supply chain trust) and describes the relevant challenges and recommendations.

The previous version of this document, White Paper Version 1.0, summarized the concepts and implementation methods for original equipment manufacturers (OEMs) and suppliers to make their supply chains safe and secure. This White Paper Version 2.0 fleshes out the realization methods.

Table I-1 lists the references and labels to which we refer in this paper.

---

[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] "New IT Policy Framework for the Digital Age," Comprehensive IT Strategy Headquarters, decided on June 7, 2019, available at: https://cio.go.jp/node/2534

Table I-1 References

No	Author	Document title	Label
1	World Economic Forum	"Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT) White Paper" (2021.3)	[WEF '21]
2	Industrial Internet Consortium	"Trustworthiness" (January 18, 2018) (https://www.iiconsortium.org/pdf/2017-12_4Q17_report_Trustworthiness_Final.pdf)	[IIC'18]
3	Robot Revolution & Industrial IoT International Symposium (RRI), Plattform Industrie 4.0, Germany	"IIoT Value Chain Security - The Role of Trustworthiness" (September 23, 2020)	[RRI '20]
4	Robot Revolution & Industrial IoT International Symposium (RRI), Plattform Industrie 4.0, Germany	"IIoT Value Chain Security - Chain of Trust for Organizations and Products" (2022.05.30)	[RRI '22]
5	METI	"Toward Ensuring the Trustworthiness of New Supply Chains (Value Creation Processes) in the Cyber and Physical Security Framework Society 5.0 Version 1.0" (April 18, 2019)	[METI '19].
6	ISO	"Security Management Systems for the Supply Chain - Best Practices for Implementing Supply Chain Security, Assessments and Plans - Requirements and Guidance" (2007)	[ISO 28001 '07]
7	Japan External Trade Organization (JETRO)	"Trade and Investment Consultation Q&A Differences between OEM and License Agreements: Japan" (2017.8) (https://www.jetro.go.jp/world/qa/04A-011247.html)	[JETRO '17]
8	ENISA	"Understanding the increase in Supply Chain Security Attacks" (July 29, 2021) (https://www.enisa.europa.eu/news/enisa-news/understanding-the- increase-in-supply-chain-security-attacks)	[ENISA '21]
9	Industrial Internet Consortium	"The Industrial Internet of Things Trustworthiness Framework Foundations, Version V1.00" (July 15, 2021)	[IIC '21]
10	JDTF Rule Formation Committee	"Digital Trust Council, Rule Formation Committee, White Paper, Version 1" (2021.12.07) (https://jdtf.jp/report/rm-com)	[TaaS WP '21]
11	Cabinet Office	"Priority Plan for the Digital Society, Appendix, Comprehensive Data Strategy" (June 18, 2021.	[Comprehensive Data Strategy '21]
12	Cabinet Office	"Society 5.0." (https://www8.cao.go.jp/cstp/society5_0/index.html)	[Society 5.0]
13	Ministry of the Environment	Cited from Green Value Chain Platform: Getting Started with Supply Chain Emissions Calculation (env.go.jp) (http://www.env.go.jp/earth/ondanka/supply_chain/gvc/supply_chain.html#no01)	[Ministry of the Environment Supply Chain Emissions Calculation]

Table I-2 provides a glossary of terms used in this paper.

Table I-2 Glossary of Terms

No	English term	Description
1	Trust Chain	A chain of trust connections built through repeated creation and proof of trust Definition in this document: a chain of "information that demonstrates trust" by showing conformity
2	Structuring a Trust Chain	Creating a chain of trust using "information that demonstrates trust" and "information that demonstrates connection"
3	Value Creation Process	Value-added creation activities that straddle both cyber and physical spaces and are composed of various objects and data that are dynamically connected
4	Trust	A credible expectation held by a user or other stakeholder that a product, system, or service will deliver value as intended; trustworthiness-based expectations
5	Trustworthiness	A system's ability to meet the expectations of its stakeholders through security, privacy, safety, reliability, resilience, and so on Reference: ISO/IEC JTC1/WG13 "For supply/value chain security and risk management, the term 'Trustworthiness' corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way."
6	Prove, Proof	Third-party confirmation that the necessary regulations for the six aspects of the value creation process (organization, people, things, data, systems, and procedures) have been met
7	Original Equipment Manufacturer	A manufacturer that produces or produces products under the consignor's brand.
8	Supply Chain	A series of resources and processes that are order-directed, beginning with the procurement of raw materials and continuing through the manufacturing, processing, and delivery of products and services to the consumer Note: Supply chain actors may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and others involved in the manufacturing, supply, processing, handling, delivery, and provision of goods and related services.
9	Procedure	[METI '19]. Procedures for a series of activities to achieve a defined objective [TaaS WP '21] Represents a series of interrelated or interacting activities or procedures for achieving an objective in an industrial activity, service, procedure, and so on
10	DX: Digital Transformation	The process of enabling companies to respond to disruptive changes in their external ecosystem (customers, markets) while driving change in their internal ecosystem (organization, culture, employees), using a third platform (cloud, mobility, big data/analytics, social technologies) to create new products and services, create value, and establish a competitive advantage by transforming the customer experience, both online and in the real world, through new business models
11	Mobility as a Service	Mobility as a Service (MaaS) is a service that provides search, reservation, payment, and others in a single package by optimally combining multiple public transportation and other transportation services to meet the trip-based transportation needs of individual local residents and travelers. It is an important means of improving the convenience of transportation and contributing to solving local issues by coordinating with non-transportation services such as sightseeing and medical services at the destination.

No	English term	Description
12	Trust Store	For every organization in a trustworthy supply chain, “Digital Evidence” (in this paper, implementation verification results) is published by each organization’s system in a shared information system called a Trust Store. The Trust Store keeps data on trustworthiness and makes them available to participants.
13	Trust as a Service	TaaS refers to the functionality to achieve the trust required in cyberspace to digitize procedures in a physical space, such as functions for counterparty trust level confirmation, remote type data integrity, remote type procedure and system validity, verification by any third party, and a mechanism to reduce the burden on the user (UX). This is provided as a service.
14	Base Registry	A database with 51 types of basic social data on people, corporations, land, buildings, qualifications, and others that is registered and published by public organizations and referred to in various situations. This database makes up the foundation for a society to have ensured accuracy and up-to-dateness.
15	Trust Service	A mechanism to check the legitimacy of people, organizations, data, and others on the Internet and prevent falsification, spoofing of transmission sources, and so on. Reference: Ministry of Internal Affairs and Communications, “Final Report of the Study Group on Platform Services,” https://www.soumu.go.jp/main_content/000668595.pdf
16	“Digital Evidence”	Information that provides evidence of the reliability of six aspects, namely, organization, people, things, data, systems, and procedures.
17	Digital Evidence Store	Database for storing, tamper-proofing, and retrieving “Digital Evidence”

II. Scope: supply chain trust for safety and security

As the Internet has come to permeate our economy and life in recent years, we see the arrival of Society 5.0, meaning a digital society led by data, including cloud services, AI, and IoT. Society 5.0 is a human-centered society that balances economic development and the resolution of social issues through a system that highly integrates cyberspace and physical space [Society 5.0].

In this regard, the Framework for Cyber and Physical Security Measures, formulated by the Ministry of Economy, Trade and Industry, states that in Society 5.0, supply chains will transform from being a routine and linear configuration in which a series of activities are developed in a fixed and stable sequence to becoming value-added activities in which various goods and data are dynamically connected across both cyber space and physical space [METI'19].

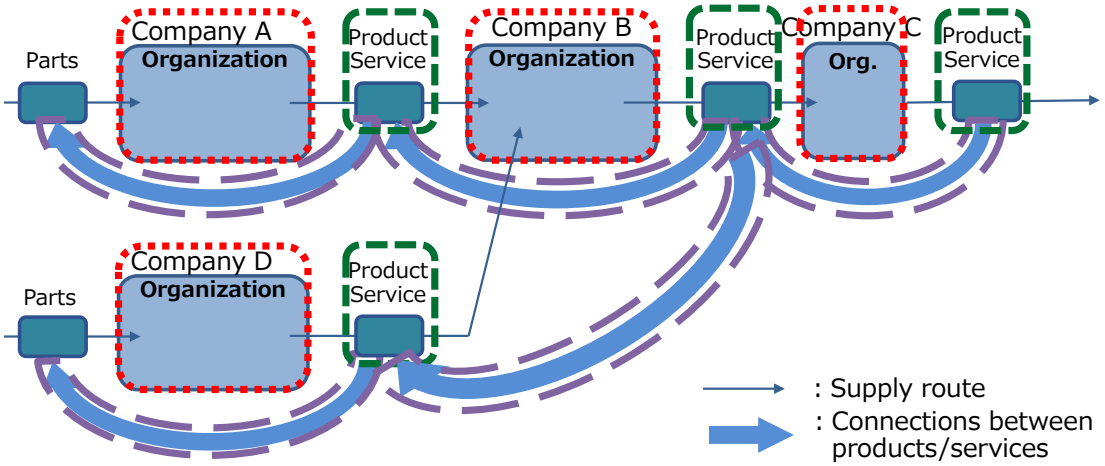
The scope of this white paper is to ensure trust as follows in "Society 5.0 supply chains," which consist of various goods and data dynamically connected across both cyber and physical space:

(Scope 1) The processes of value creation (products, services, data, etc.) in the supply chains are in line with expectations,

(Scope 2) The values (products, services, data, etc.) created in the supply chains are in line with expectations, and

(Scope 3) Continuous provision of value (products, services, data, etc.), including after-sales services, through the supply chains are in line with expectations.

The "Society 5.0 supply chains" covered by Scopes 1–3 are shown in Figure II-1.



	(Scope 1)	Product manufacturing process and service provision process of Company A, Company B, Company C, and Company D
	(Scope 2)	Products and services created by Company A, Company B, Company C, and Company D
	(Scope 3)	Connections between products and services created by Company A, Company B, Company C, and Company D

Figure II-1 “Society 5.0 supply chains” covered by Scopes 1–3

III. Changes in environmental conditions/circumstances

Based on the scope described in the previous section, changes in environmental conditions/circumstances regarding supply chains are summarized in Trends 1–4 below.

(Trend 1) Digitization of supply chains and after-sales services

Organizations in supply chains are increasingly digitizing business-to-business (Business-to-Business, BtoB) transactions, the manufacturing and delivery processes of products and services, maintenance, and after-sales services, including remote monitoring. New services such as operation, maintenance, and upkeep of facilities using data obtained from equipment, sensors, and other devices are also being offered at an accelerated pace.

(Case 1-1) Digitization of manufacturing processes

Machine tool manufacturers are increasingly digitizing their manufacturing processes, sharing data for machining and prototyping customer products, and conducting test machining and prototyping in a three-dimensional virtual space. Efforts are underway to increase business opportunities by connecting with customers through machining and prototyping in this virtual space.[4]

(Case 1-2) Digitization of business-to-business transactions

In 2019, the market size of BtoB e-commerce in Japan was 353 trillion yen, expanding 2.5% from the previous year. The ratio of the e-commerce market size to the value of commercial transactions (commercial transaction market size) is also on the rise, and the digitization of commercial transactions continues to progress.[5]

(Case 1-3) Digitization of after-sales services

Businesses based on industrial data collected from equipment and others are expanding. "i-Construction"—the process of accumulating and analyzing various data (e.g., work performance information from ICT construction equipment at construction sites and 3D measurement information of the topography of work sites from drones) systems that enable real-time management of the construction status and the sharing of

[4] DMG Mori Seiki to Digitalize 80% of its Processes: Prototyping Parts in Virtual Space: Nihon Keizai Shimbun (nikkei.com)
https://www.nikkei.com/article/DGXZQOFD0834A0Y1A800C2000000/

[5] Ministry of Economy, Trade and Industry (METI) Compilation of the results of a market survey on e-commerce. https://www.meti.go.jp/press/2020/07/20200722003/20200722003.html

progress—is being introduced, and the introduction of systems that enable real-time management of construction status and sharing of progress is advancing.[6]

Moreover, industrial and energy companies in the petroleum, chemical, and electric power and gas industries, as well as related providers of infrastructure such as elevators and buildings, are facing long-term human resource shortages and a decline in their ability to pass on technology and skills because of the aging of their facilities and personnel. In addition to these problems, recent years have seen increasingly severe disasters in Japan, and companies are faced with the demand for facilities with high safety features to cope with disasters. Services that use digital technology are being introduced to automate the diagnosis and monitoring of the necessary repair or replacement of equipment, using data from sensors in infrastructure-related equipment to ensure a high level of safety while saving manpower.[7]

(Trend 2) Continuous supply of product and service value in response to diversifying needs and changing external conditions

Various efforts are being made by organizations that make up supply chains to respond flexibly and quickly to diversifying consumer needs, external conditions, and other changes, and ensure the continuous supply of value in products and services.

(Case 2-1) Continuous supply of products and services that meet diversifying consumer needs

Business computers are highly customizable in terms of CPU, memory, HDD, and other components. To meet specific consumer requirements, business computer suppliers have established supply chains that accept detailed customization requests via purchase websites and assemble business computers one by one at a factory to meet such requirements.[8]

(Case 2-2) Continuous supply of products and services in response to changing external conditions

When the Great East Japan Earthquake struck, parts manufacturers in the Tohoku region were also hit, and automakers were unable to secure the parts they needed. It was

[6] Data Utilization Case Studies: Case03 Platformer①
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/data_jireisyu.pdf

[7] Basic Policy for Smart Security Guidelines, Ministry of Economy, Trade and Industry 2020
https://www.meti.go.jp/shingikai/safety_security/smart_hoan/pdf/kihon_hoshin.pdf

[8] monodukuri.com What is "BTO"? https://www.monodukuri.com/gihou/article_list/125/BTO

discovered at that time that the supply chain structure was not conventionally composed of affiliated suppliers with the OEM at the top, but rather single supplier belonging to multiple affiliates.[9] The automakers began to visualize the total supply chains, avoid regional risks, and monitor the status of facilities at partner plants to diversify risk so that the supply chains would not be disrupted in a crisis.

(Case 2-3) Utilization of open-source software as software components

In the field of software development, open-source software is increasingly being used for its functionality and convenience. In recent years, products traditionally provided as software products have increasingly become replaced by open-source software to respond flexibly and quickly to needs.

(Trend 3) Changes in the structure of supply chains, diversification of industries in which suppliers participate, and increased complexity of supply routes for products and services

In the supply chains, suppliers are entering diverse industries and supply routes for products, and services are becoming increasingly complex.

(Case 3-1) From a pyramid structure to a diamond structure

In some cases, automobile manufacturers have concentrated the supply of semiconductor chips, which are core components, to specific suppliers outside their own group as a result of their efforts to promote greater efficiency and lower costs in the supply of components. In such cases, the supply chain structure is a diamond structure with a horizontal division of labor, where one supplier belongs to multiple affiliates.[9]

(Case 3-2) A diamond structure including different industries and services

Telematics insurance services are being offered to reduce insurance claims for safe drivers by acquiring data from in-vehicle devices in automobile insurance. These services are not limited to traditional suppliers such as car manufacturers and insurance companies, but new suppliers have entered the market, and supply routes for products and services have become more complex.[10]

---

[9] Ministry of Economy, Trade and Industry (METI) "Manufacturing White Paper 2019 Part 1: Current State and Issues of Fundamental Manufacturing Technologies, Chapter 1: Manufacturing Industry in the Heisei Era and Changes in the Manufacturing White Paper"
https://www.meti.go.jp/report/whitepaper/mono/2019/honbun_pdf/index. html

[10] Ministry of Land, Infrastructure, Transport and Tourism, Promotion of the Japanese Version of MaaS:

(Trend 4) Acceleration of rule formation that requires compliance throughout the supply chain

While compliance with the rules at individual OEMs is a given, in recent years, all of the suppliers that make up the supply chain are now asked to account for their compliance with the rules. These rules are being formed one after another globally.

(Case 4-1) Personal data protection under General Data Protection Regulation

The General Data Protection Regulation (GDPR) has been in effect in the European Union since 2018; it is designed to give individuals back their right to control their personal data and to consolidate rules within the European Union. The GDPR also tasks data managers with accountability for GDPR compliance in processing data even in the case of an outsourcee processing personal data. Companies that violate the GDPR are subject to huge fines.[11] When companies are accountable for GDPR compliance, they must hold their suppliers accountable as well, and failure to do so across the board increases the risk of fines.

(Case 4-2) World Forum for Harmonization of Vehicle Regulations

Security requirements for self-driving vehicles were developed at the World Forum for Harmonization of Vehicle Regulations (WP29), where the participants agreed upon security requirements that automakers should include when designing, developing, and manufacturing self-driving vehicles.[12] Automakers need to explain that their products meet these security requirements. If the manufacturer's suppliers cannot explain how their products meet the security requirements of the WP29, the type designation necessary to reduce the man-hours required for inspections of mass-produced products may be revoked, or the mass production of vehicles may be prevented.

Formation of the MaaS Model
https://www.mlit.go.jp/sogoseisaku/japanmaas/promotion/model/index.html

[11] JETRO Business Brief, Two years after the start of GDPR application, clarifying the scope of extraterritorial application, https://www.jetro.go.jp/biznews/2020/06/c81164d22cfa1274.html

[12] Ministry of Land, Infrastructure, Transport and Tourism Press Release "Introduction of International Standards for Automated Driving Technology, etc.: Partial Revision of Safety Standards for Road Vehicles, etc., and Notifications, etc., that Specify Details of Safety Standards" (Japanese only)
https://www.mlit.go.jp/report/press/jidosha10_hh_000242.html

(Case 4-3) Sustainable Development Goals

The Sustainable Development Goals (SDGs), which are international development goals to be achieved by 2030, were adopted by the United Nations in 2015. They consist of 17 goals and 169 targets to be achieved, and companies are encouraged to set, disclose, and continuously work toward the targets for these goals.[13] It is becoming increasingly important for companies to explain their commitment to the SDGs to demonstrate their social corporate value. To explain their commitment to the SDGs, OEMs must not only explain their own commitment to the SDGs, but also their suppliers' commitment to the SDGs throughout their supply chains.

(Case 4-4) Environment, Society, and Governance

In recent years, attention has gathered around "ESG investment,"[14] which means making investments by analyzing companies from three perspectives: the environment, society, and governance (ESG). When receiving investments, it is becoming increasingly important for companies to explain their ESG initiatives as an indication of their future corporate value, through examples of ESG initiatives such as the use of materials and energy with low environmental impact and the reduction of environmental impact in the disposal process. Not only the OEMs, but also all suppliers and the entire supply chains, must explain their ESG initiatives.

[13] Ministry of Economy, Trade and Industry SDGs https://www.meti.go.jp/policy/trade_policy/sdgs/

[14] Ministry of Economy, Trade and Industry ESG Investment
https://www.meti.go.jp/policy/energy_environment/global_warming/esg_investment.html

IV. Issues to resolve

The previous chapter described the following four trends and changes in supply chains:

(Trend 1) Digitization of supply chains and after-sales services;

(Trend 2) Continuous supply of products and services of value in response to diversifying needs and changing external conditions;

(Trend 3) Changes in the structure of supply chains, diversification of industries in which suppliers participate, and increased complexity of supply routes for products and services; and

(Trend 4) Acceleration of rule formation that requires compliance throughout the supply chain.

To ensure supply chain trust in this context, this chapter describes Issues 1–4 that need to be resolved.

(Issue 1) Data security threats associated with digitization

Among organizations that make up the supply chain, factories and plants are expected to handle large amounts of data autonomously, and the trustworthiness of manufacturing and data-based services will become highly dependent on the "trustworthiness of data." Digitized data are constantly exposed to security threats, and it is difficult to confirm the date, time, place, and origin of data generation, or to confirm that the data have not been tampered with or replaced during the course of exchanges. Furthermore, as services become digitized, the data used in the process are also exposed to threats, and it is difficult to confirm the source, date, and time of data generation, and that the data have not been tampered with or replaced. Design data and process data generated in the process of manufacturing products and providing services, BtoB transaction data, and infrastructure facility data are closely related to real-world products and services, BtoB transactions, and facility operating conditions. Therefore, ensuring the trustworthiness of data affects the trustworthiness of real-world products and services, BtoB transactions, and facility operations. However, because there is no consensus standard or guideline for what constitutes "trustworthy data" in Japan, there is a risk that some services may operate under inappropriate standards compared with international and technological trends.

(Issue 2) Difficulty of reconfiguring suppliers to meet diversifying customer needs and changing external conditions

In order for the organizations in supply chains to respond to new needs and changing external conditions, supply chains must be reconfigured to incorporate new suppliers. To

determine whether a supplier's products or services can meet new needs or changing external conditions, it is necessary to check the supplier's track record, capabilities, and whether it is properly managed, which is a time-consuming and costly process. Even if a new supplier claims to be able to provide a product or service with better functionality or convenience, it is time-consuming and costly to verify whether the claim is true.

(Issue 3) Increasing complexity of supply chains, which makes it difficult to identify the causes and scope of impact when problems occur

As the industries of suppliers become more diverse and supply routes more complex, it becomes difficult for organizations in the supply chain to identify where in the supply chain the causes lie when a problem is discovered with a final product or service. Furthermore, it is difficult to determine properly whether the causes of the problem affect other products or services (scope of impact). If it takes time to identify the causes of the problem and to understand and specify the scope of impact, product provision and service restoration will be delayed and potentially lead to loss of business opportunities and damage to the corporate image.

(Issue 4) Explanation of the status of compliance with rules and new value created throughout the supply chains

Organizations in a supply chain must follow the relevant rules imposed on the entire supply chain, as they are formed one after another. To comply with these rules, OEMs must develop their own rules that apply to their supply chains, and their suppliers must follow these rules in their business activities. Failure to account for compliance throughout the supply chain can lead to lost business opportunities and penalties.

Furthermore, to achieve sustainable growth for society, companies must take the initiative to enhance new social and environmental values such as SDGs and ESG. To enhance their corporate image and corporate value, companies must be able to explain appropriately that they are working to improve social and environmental values by formulating their own rules and regulations applicable to their supply chains, and are accommodating the aforementioned rules.

In this white paper, the term "regulations" refers to all rules, procedures, and rules that must be followed in a supply chain, manufacturing process, or service provision process; it is not limited to any specific subject or scope.

Measures to address these issues are described in the next chapter.

V. Measures to resolve the issues

1. Goals of supply chain trust

Considering the issues described in the previous chapter, the following is a description of what establishing trust aims to achieve in a supply chain.

(Goal 1) Easily verify the trustworthiness of data generated and exchanged throughout the supply chain

This means that organizations in a supply chain could easily verify the origin of the data and subsequently confirm that no tampering has occurred, as with the data used for services, as well as the trustworthiness of real-world products and services that are provided based on the data.

(Goal 2) Be able to select appropriate suppliers in response to changes in needs and the external environment

This means that organizations in a supply chain could check the performance and capabilities of new suppliers and whether they are managing production and sales appropriately, without spending too much time and money. This would allow organizations to select suppliers appropriately and easily reconfigure their supply chains to include new suppliers. This way, the company could respond to diverse needs and changes in the external environment.

(Goal 3) Easily understand the structure of the supply chain

This means that even though suppliers come from diverse industries, and supply routes are becoming more complex, organizations in a supply chain could easily identify where in the supply chain the causes of a problem lie when one is discovered in a final product or service. Furthermore, it could be easily and appropriately determined whether the causes of the problem affect other products or services (scope of impact). Easily identifying the causes of the problem and the scope of impact makes it possible to resume product supply and restore services quickly, thus helping to avoid lost business opportunities and damage to the corporate image.

(Goal 4) Be able to explain compliance with rules throughout the supply chain

This means that organizations in a supply chain could explain their compliance with the rules that are imposed on the entire supply chain as they are formed one after another. They could avoid lost business opportunities and penalties by establishing their own rules

that apply to their supply chains and conducting their business activities in accordance with these rules.

Furthermore, the company could explain its efforts to improve new social and environmental values, such as SDGs and ESG, for the sustainable growth of society. To enhance corporate image and corporate value, the company could develop higher goals applicable to the supply chain as a regulation, implement the regulation, and explain how the higher goals have been achieved.

The aforementioned mechanisms for ensuring data trustworthiness throughout supply chains and easily demonstrating the trustworthiness and legitimacy of business activities without loss of time or costs would further provide the following values.

Value 1: Strengthening the competitiveness of the industry

In the increasingly diverse and complex supply chains of Society 5.0, ensuring the trustworthiness of data exchanged among organizations and companies, and visualizing the trustworthiness and legitimacy of business activities would enhance global competitiveness, with trust as a strength and the differentiating factor in the industry.

Value 2: Creating new innovations

The reduction of insecurity, distrust, and risk in business activities would enhance the value creation, transactions, and integration of companies within the supply chains as well as accelerate innovation creation across different organizations, companies, and industries.

2. Requirements

In the previous section, we described supply chain trust goals. In this section, we describe requirements 1–3 to achieve goals 1–4.

(Requirement 1) Easily verify the trustworthiness of data exchanged in the supply chain

(Requirement 1-1)	It is easy to verify the date, time, location, and source of data generated and exchanged in the supply chain, and that the data have not been tampered with or switched.
(Requirement 1-2)	The trustworthiness of the source of the data can be verified. For example, it is easy to verify that the organization, person, or component generating the data is not fraudulent.
(Requirement 1-3)	It can be confirmed that the data existed at a certain point in

time.

(Requirement 2) Be able to check easily the regulations imposed on the processes of manufacturing products and providing services, and that the processes have been implemented in accordance with the regulations

(Requirement 2-1) The regulations imposed on the process of manufacturing products and providing services can be easily identified.

(Requirement 2-2) It is easy to verify that the processes have been implemented in accordance with the regulations.

(Requirement 3) Easily see the connections among the organizations, products, and services that make up the supply chain

(Requirement 3-1) The connections among the organizations that make up the supply chain can be easily identified.

(Requirement 3-2) The generation and supply routes for products and services can be easily identified.

3. Implementation methods

3-1. Classification of the trust formed in supply chains

The extent to which trust is formed in a supply chain depends on "the extent to which it can verify the ability to meet expectations." The scope of trust formation can be classified into (1) and (2) below, depending on the scope of the entity (organization or person) performing the verification.

(1) Private trust

This refers to the trust formed by being able to verify the ability to meet expectations among entities within a specific limited scope. Examples are the relationships within an organization, between organizations (e.g., client–order taker), and industry associations, especially those with a participation/withdrawal process.

(2) Public trust

This refers to the trust formed by being able to verify the ability to meet an entity's expectations without limiting the scope. Examples are national, international, and other levels that are public in nature and have no explicit participation/withdrawal process.

3-2. Concepts for realization

The Cyber Physical Security Countermeasures Framework [METI '19] realizes trust in supply chains through the following ways:

- Decomposing the process of manufacturing products and providing services into six elements: "organization," "people," "components," "data," "procedures," and "systems";
- Confirming with "Digital Evidence" that each of the six elements is "as expected," that is, "implemented in accordance with regulations"; and
- Ensuring that confirmation results can be queried and shared within the supply chain.

In this white paper, based on the requirements presented in section V-2, the following items must be implemented to realize trust in the supply chain (Figure V-1):

(1) Verify that each aspect has been implemented in accordance with the various regulations,(Note)

(2) Make it possible for a third party to query the results of (1) and the "Digital Evidence," and

(3) Make it possible to create connections with and trace item (2) above.

(Note: The "regulations" here are assumed to be appropriate and correct, and agreed upon to the extent that they form trust.)

In this white paper, not only the process of manufacturing products and providing services, but also their outputs, products and services, are assumed to consist of the six elements.

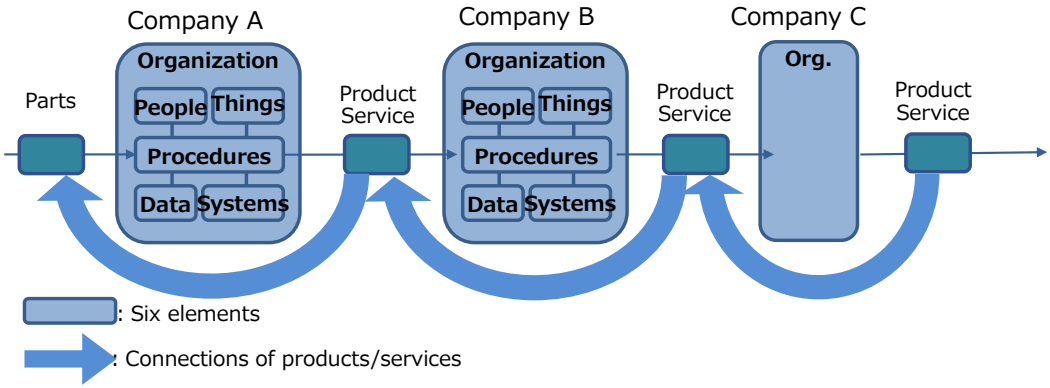


Figure V-1 Visualization of a supply chain consisting of six elements

Concrete examples of the six elements that make up the supply chain “as expected” and “implemented according to regulations” (see Figure V-1)are presented below.

(Examples)

Organization, people:	Companies and individuals qualified and authorized to perform work or operations
Components, systems:	Components that are calibrated and inspected, systems that are authorized
Data:	Data (manufacturing schematics, transaction data, etc.) that have not been falsified
Procedures:	A series of tasks and operations that are performed according to predefined procedures

Scopes 1–3, presented in Chapter II, are explained again below in terms of the aforementioned six elements.

(Scope 1) The process of value creation in the supply chain is in line with expectations

⇒ Implement the six elements that make up the process of manufacturing products and providing services, indicated by the red box (dashed lines) in Figure V-2, in accordance with the regulations, and allow verification that they have been implemented so.

(Scope 2) The value created in the supply chain is in line with expectations

⇒ The products and services generated in the supply chain, indicated by the green box (dashed lines) in Figure V-2, function according to specifications, and the defined quality is ensured or can be confirmed.

(Scope 3) Ensure that value continues to be delivered as expected throughout the supply chain

⇒ The linkage of products and services, indicated by the purple box (dashed lines) in Figure V-2, and the relationship between supply and demand are maintained, and products and services continue to be provided.

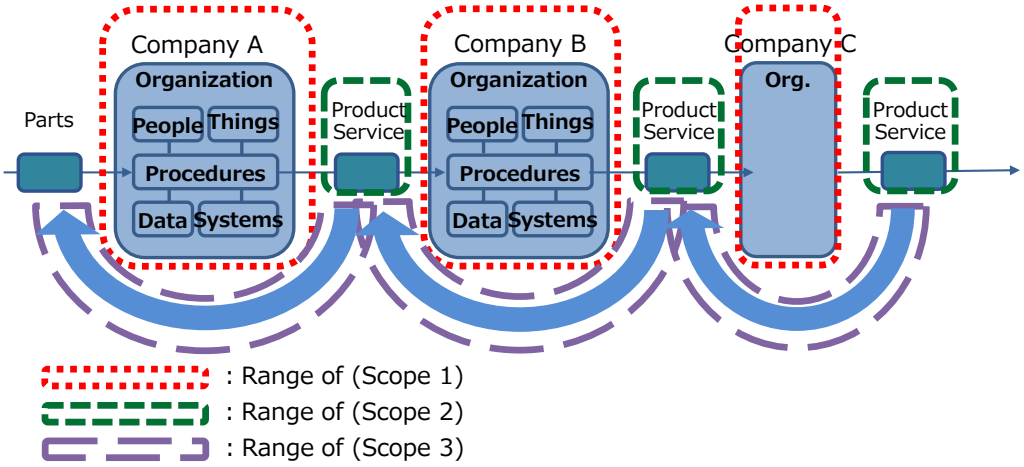


Figure V-2 Ranges of Scopes 1–3

3-3. Overall picture of the realization methods

Table V-1 shows the information required to realize Requirements 1–3 as described in Section V-2.

Table V-1 Information required to realize Requirements 1–3

Information	Role
"Trustworthiness Information"	This refers to information indicating that a product or service has been implemented in accordance with regulations in the product manufacturing or service provision process. This information is disclosed to the supply chain members.
"Digital Evidence"	This refers to information providing evidence that the relevant rules have been implemented accordingly. This information can be found under "Trustworthiness Information."
"Linkage Information"	This refers to configuration information that shows the connection between products and services provided by OEMs, suppliers, service providers, and others, and the parts and services that make them up. The composition of products and services can be traced throughout the supply chain.

Next, the overall structure of trust in a supply chain is shown in Figure V-3 and the various elements are shown in Table V-2. The overall configuration consists of a "Trust Store," "Digital Evidence Store," "Trust as a Service (TaaS)," and "Base Registry," and is realized as follows.

- Organizations in the supply chain record information showing evidence that

products and services have been manufactured and provided in accordance with the regulations, which constitutes “Digital Evidence,” and store such information in a Digital Evidence Store.

- “Trustworthiness Information,” which indicates that the product/service was manufactured and provided in accordance with the regulations, and “Linkage Information,” which indicates the composition of the product/service, are stored in the Trust Store.
- By sending and receiving data to and from each other through TaaS, the authenticity and integrity of the data, as well as the existence of the person, organization, person, or product from which the data were generated, could be verified.
- In addition, the Base Registry would be used to ensure the accuracy and up-to-dateness of highly reusable data that are registered and published by public organizations and referenced in a variety of situations.

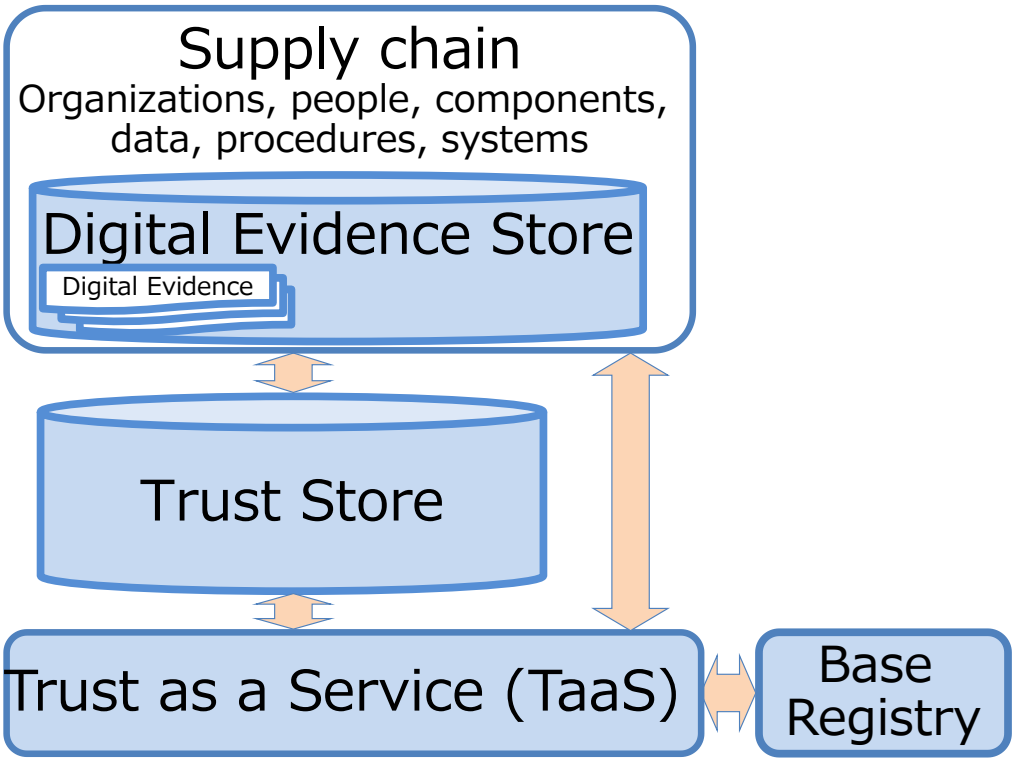


Figure V-3 Overall structure of trust in a supply chain

Table V-2 Elements of trust in a supply chain

Element	Features
Trust Store	This stores the “Trustworthiness Information” of organizations, people, components, data, procedures, and systems required for manufacturing and providing products and services, as well as the “Linkage Information” of products and services. The “Trustworthiness Information” in the supply chain can be searched by tracing the “Linkage Information.” In principle, the stored information would be made publicly available to those involved in the supply chain but may be kept private depending on the use case.
Digital Evidence Store	This stores information (“Digital Evidence”) that serves as the basis for confirming the implementation results in accordance with previously agreed-upon rules and regulations. This could be referred to by following the “Trustworthiness Information.” In principle, the stored information is not public, but it may be disclosed to the requester upon request.
TaaS	This connotes being able to verify the authenticity and integrity of the data and being able to verify the existence of organizations, people, and products.
Base Registry	Data that are registered and published by public organizations and reusable in a variety of situations are stored here. The accuracy and up-to-dateness of the stored data is ensured.

3-4. Trust Store and Digital Evidence Store

The Trust Store and Digital Evidence Store in the realization methods shown in the previous section are similarly described in an existing document [IIC '21] as a way to achieve trust in a supply chain. The contents are presented below.

(1) Outline

An overview of the supply chain trust realization methods described in the existing document [IIC '21] is shown in Figure V-4. The Trust Store and Digital Evidence Store described in the previous section are synonymous with the Trust Store and “Digital Evidence” in [IIC '21].

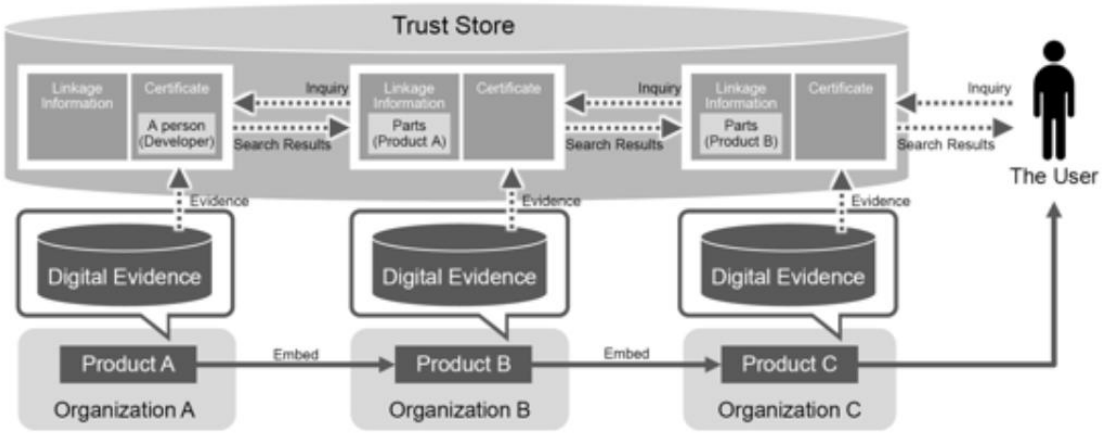


Figure V-4 Overview of Trust Store and Digital Evidence Store [IIC '21] Figure 4-8

Note: "Digital Evidence" is referred to as Digital Evidence Store in the text.

According to [IIC '21], a supply chain is constructed over the life cycle of a product or service, including its manufacturing and delivery processes, BtoB transactions, and maintenance and servicing. The Trust Store stores certificates (Certificate in the figure) indicating that the organizations comprising the supply chain (Organizations A, B, and C in the figure) provide products or services (Products A, B, and C in the figure) as output in line with expectations. In addition, the Trust Store stores "Linkage Information" (Linkage Information in the figure) that shows the linkage of transactions between organizations, of components and materials of products, and of supply and demand of services, and traces the linkage of certificates for organizations, products, and services. The Digital Evidence Store stores "Digital Evidence" (Digital Evidence in the figure) that provides evidence that the product manufacturing and service provision processes were carried out as expected.

(2) Realization methods

Specific ways to achieve trust in a supply chain based on (1) above are shown in Figure V-5. For simplicity, this figure shows only a portion of the supply chain.

In the figure, each organization confirms with the log recorded in the manufacturing process that it has been implemented in accordance with the regulations and stores the "Digital Evidence." Then, "Trustworthiness Information," which is the information showing that the product/service was implemented in accordance with the regulations in the product manufacturing or service provision process, and "Linkage Information,"

which shows the composition of the parts/products confirmed in the implementation check, are stored in the Trust Store. The “Trustworthiness Information” of the parts/products manufactured by each organization is linked with the “Linkage Information.” In addition, “Digital Evidence” that supports the “Trustworthiness Information” is traceable from the “Trustworthiness Information.”

In this way, it is possible to confirm with the “Trustworthiness Information” that each organization has followed the regulations, and have “Digital Evidence” that is the basis of the “Trustworthiness Information.” Then, by tracing the “Linkage Information,” it is possible to confirm that the entire supply chain has followed the regulations.

The Trust Store manages and makes searchable the linkage of the “Trustworthiness Information” based on the “Linkage Information” that indicates the composition of each component and product. This Trust Store allows the user to trace the connections upstream and downstream in the supply chain.

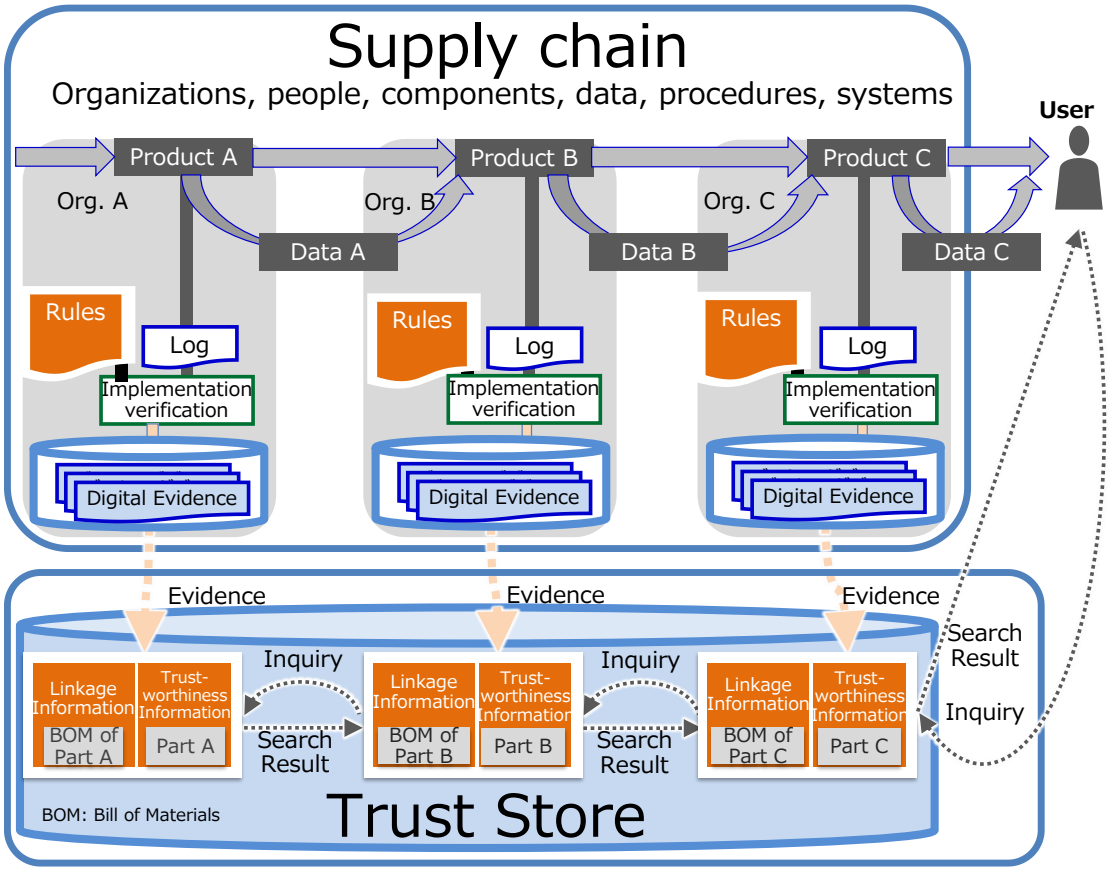


Figure V-5 How to use the Trust Store ([IIC '21] Additions to Figure 4-8)

In addition, Figure V-4 and Figure V-5 describe a single Trust Store, but a Trust Store

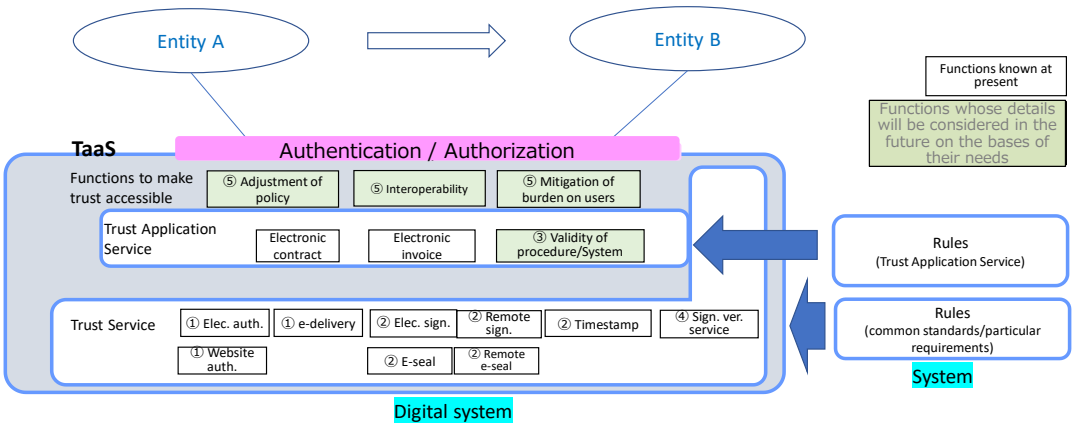
may be composed of multiple entities, such as a company unit or industry unit, and not limited to this implementation form. Even in such a case, it must be possible to achieve the same thing as above across companies and industries.

3-5. Trust as a Service (TaaS)

(1) Outline

In the "White Paper Version 1 (2021.12.7)" [TaaS WP '21] issued by the Rule Formation Committee of the Digital Trust Council, the following paragraph defines TaaS as shown in Figure V-6.

TaaS is built on top of trust services such as electronic authentication, digital signatures, remote signatures, eSeals, and time stamps that enable trust of data in cyberspace. Trust services support the institutional effectiveness of the digitization of documents and seals. In addition, TaaS has an ease-of-use function that enables organizations, people, components, and systems that use TaaS to realize remote services and other ease-of-use functions, thereby achieving robustness. The ease-of-use function is linked to the trust service to realize robustness supported by institutional effectiveness. In addition, it has a trust application service, which provides services related to specific operations such as electronic contracts and e-procurement. This trust application service, in conjunction with the trust service or the ease-of-use function, achieves accuracy and certainty supported by institutional effectiveness with respect to specific operations targeted by the trust application. This TaaS can be used to ensure authenticity, i.e., that the data has not been switched, integrity, i.e., that the data has not been tampered with, and realism, i.e., that the counterparty is real.



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

TaaS: Trust as a Service
Elec. auth.: Electronic authentication
Sign. ver.: Signature verification

Figure V-6 How Trust as a Service works (adapted from [TaaS WP '21] Figure 15)

(2) Realization methods

Requirement 1, described in the previous section on supply chain trust, is realized using TaaS. Organizations and consumers in the supply chain use TaaS to verify the authenticity and integrity of data generated and exchanged in the supply chain, data emitted from components, and the "Trustworthiness Information" stored in the Trust Store. In addition, TaaS is used to verify the existence of the organizations, people, and components that generate the data. In this way, TaaS can be used to verify easily the authenticity of data exchanged in the supply chain and the source of data generation.

3-6. Base Registry

(1) Outline

Base Registry is defined in the "Comprehensive Data Strategy" [Comprehensive Data Strategy '21] as "a database of society's basic data on people, corporations, land, buildings, qualifications, etc., registered and published by public organizations and referred to in various situations, with ensured accuracy and up-to-dateness, which is the foundation of society."

(2) Method of use

Figure **V-7** shows how to use the Base Registry to achieve trust in a supply chain. The Base Registry is used by organizations and consumers in the supply chain via TaaS. For

example, by checking the Base Registry of a corporation, it is possible to check accurate and up-to-date information, especially highly reusable data such as the existence of trading partners, attribute information such as privacy marks, and data used in the purchasing process.

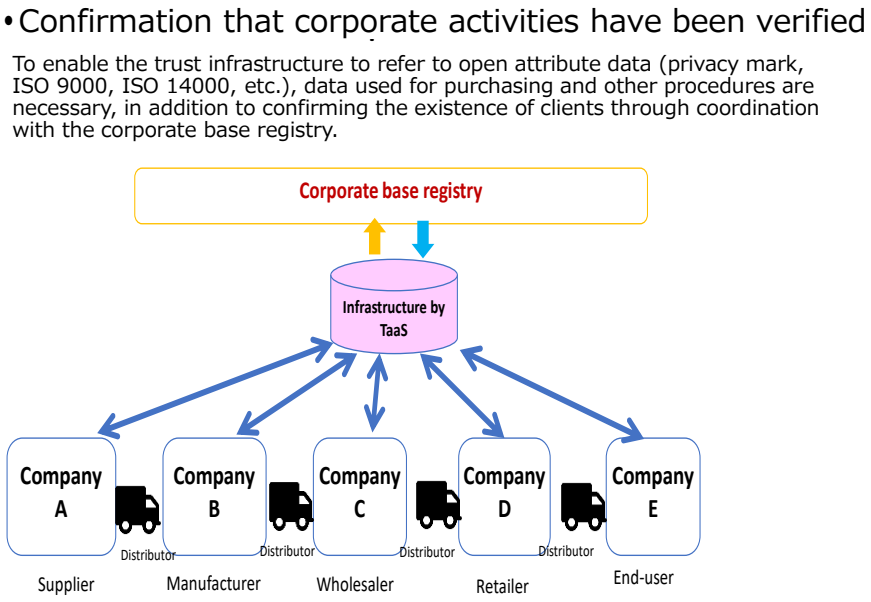


Figure V-7 How to use a Base Registry to achieve trust in the supply chain (adapted from [TaaS WP '21] Figure 25)

4. Information items handled with the supply chain trust

This section presents specific items of the "Trustworthiness Information," "Digital Evidence," and "Linkage Information" that are necessary to realize trust in the supply chain. These items, listed in V-2, are necessary to fulfill the requirements indicated in Section V-2, and it is from this list that items should be selected for use, depending on the use case.

4-1. "Trustworthiness Information" items

The "Trustworthiness Information" items are shown in Table V-3.

Table V-3 “Trustworthiness Information”

No	(Data) Item	R1	R2	R3	Description
(a)	Object identifier	○	○		- Information identifying the object of the “Trustworthiness Information”
(b)	Generation date information	○	○		- The date and time when the “Trustworthiness Information” was generated after the originator confirmed that the product or service was manufactured and provided in accordance with the regulations - The originator may be the organization that manufactured or provided the product, or it may be a third-party organization.
(c)	Generated location and source information	○	○		- Information identifying the organization, person, or component from which the “Trustworthiness Information” originates - For example, if the source is a third-party organization, this refers to information identifying the organization or person in the third-party organization.
(d)	Information confirming that data have not been falsified or switched	○	○		- Information confirming that the data in the “Trustworthiness Information” have remained original and unaltered by anyone from the date and time these were generated to the date and time these were verified
(e)	Information verifying that the originator is not fraudulent	○	○		- Information confirming that there is no fraudulent origin of the “Trustworthiness Information”
(f)	Information confirming that the data existed at a certain point in time	○	○		- Information confirming the existence of “Trustworthiness Information” at the date and time of generation
(g)	Regulation reference information		○		- Information that identifies the regulations to be followed in the supply chain for products and services
(h)	Reference information for information as evidence of conduct in accordance with the regulations		○		- Information identifying the “Digital Evidence” that serves as the basis for the implementation in accordance with the regulations - This information includes information that identifies the organizations, people, and components that manufactured and provided products and services in accordance with the regulations.

(Legend) R1: Requirement 1, ○: Items to be selected according to the requirements to be fulfilled for each use case

4-2. “Digital Evidence” items

“Digital Evidence” items are shown in Table V-4.

Table V-4 “Digital Evidence” items

No	(Data) Item	R1	R2	R3	Description
(a)	Object identifier	○	○		- Information identifying the object of the “Digital Evidence”
(b)	Generation date information	○	○		- The date and time when the “Digital Evidence” was generated after the originator confirmed that the product was manufactured or the service provided in accordance with the regulations - The originator may be the organization that manufactured or provided the product, or it may be a third-party organization.
(c)	Generated location and source information	○	○		- Information identifying the organization, person, or component from which the “Digital Evidence” originated - For example, if the source is a third-party organization, this refers to information that identifies the organization or person in the third-party organization.
(d)	Information confirming that the data have not been falsified or switched	○	○		- Information confirming that the data in the “Digital Evidence” have remained original and unaltered by anyone from the date and time these were generated to the date and time these were verified
(e)	Information verifying that the originator is not fraudulent	○	○		- Information confirming that there is no fraudulent origin of the “Digital Evidence”
(f)	Information confirming that the data existed at a certain point in time	○	○		- Information confirming the existence of “Digital Evidence” at the date and time of generation
(g)	Regulation reference information		○		- Information identifying the regulations to be followed in the supply chain for products and services

(i)	Reference information for information as evidence of conduct in accordance with the regulations		○		- Information providing the basis for the product manufacturing or service provision process that has been carried out in accordance with regulations

(Legend) R1: Requirement 1, ○: Items to be selected according to the requirements to be fulfilled for each use case

4-3. "Linkage Information" Items

"Linkage Information" items are shown in Table V-5.

Table V-5 "Linkage Information" items

No	(Data) Item	R1	R2	R3	Description
(a)	Object identifier	○		○	- Information identifying the object of the "Linkage Information"
(b)	Generation date information	○		○	- The date and time when the "Linkage Information" was generated after the originator confirmed that the product or service was manufactured and provided in accordance with the regulations - The originator may be the organization that manufactured or provided the product, or it may be a third-party organization.
(c)	Generated location and source information	○		○	- Information identifying the organization, person, or component from which the "Linkage Information" originated - For example, if the source is a third-party organization, this refers to information that identifies the organization or person in the third-party organization.
(d)	Information confirming that data have not been falsified or switched	○		○	- Information confirming that the data in the "Linkage Information" have remained original and unaltered by anyone from the date and time these were generated to the date and time these were verified
(e)	Information verifying that the originator is not fraudulent	○	○		- Information confirming that there is no fraudulent origin of the "Linkage Information"

(f)	Information confirming that the data existed at a certain point in time	○	○		Information confirming the existence of the "Linkage Information" at the date and time of generation
(j)	Information showing connection to the organization			○	- Information indicating the relationship between the organizations with which one does business
(k)	Information indicating supply routes for products and services			○	- Information indicating what parts, materials, services, and others a product or service consists of, and where parts, materials, services, and others are supplied from and to

(Legend) R1: Requirement 1, ○: Items to be selected according to the requirements to be fulfilled for each use case

In addition, in Table V-3 to V-5, (a) Object identification information is information that identifies the object of each piece of information. For example, it may be information that identifies "product/service (red dashed line)" itself in Table V-2 and the "process (green dashed line)" that manufactures/provides the product/service.

5. Visualization of the goals to be realized

This section presents concrete images for realizing Goals 1–4 described in section V-1, namely,

(Goal 1) Easily verify the trustworthiness of data generated and exchanged throughout the supply chain,

(Goal 2) Be able to select appropriate suppliers in response to changing needs and external environment,

(Goal 3) Easily understand the structure of the supply chain, and

(Goal 4) Be able to explain compliance with rules throughout the supply chain.

5-1. Visualization of Goal 1

Goal 1 is achieved by assigning digital signatures to data and verifying the assigned digital signatures. The granting and verification of digital signatures is realized using TaaS. The trustworthiness of the data, as follows, can be easily verified:

- No tampering occurred after Supplier A generated the data,
- The source of the data is Supplier A, and
- The data existed at a certain point in time.

Specifically, these are achieved through the following items of information:

(d) Information confirming that the data have not been falsified or switched,

(e) Information verifying that the originator is not fraudulent, and

(f) Information confirming that the data existed at a certain point in time.

How to check the trustworthiness of data using TaaS is explained in Figure V-8 (1)–(3).

(1) Supplier A provides a digital signature to the data.

(2) Supplier A sends the data and digital signature to Supplier B.

(3) Supplier B verifies that the digital signature is that of Supplier A.

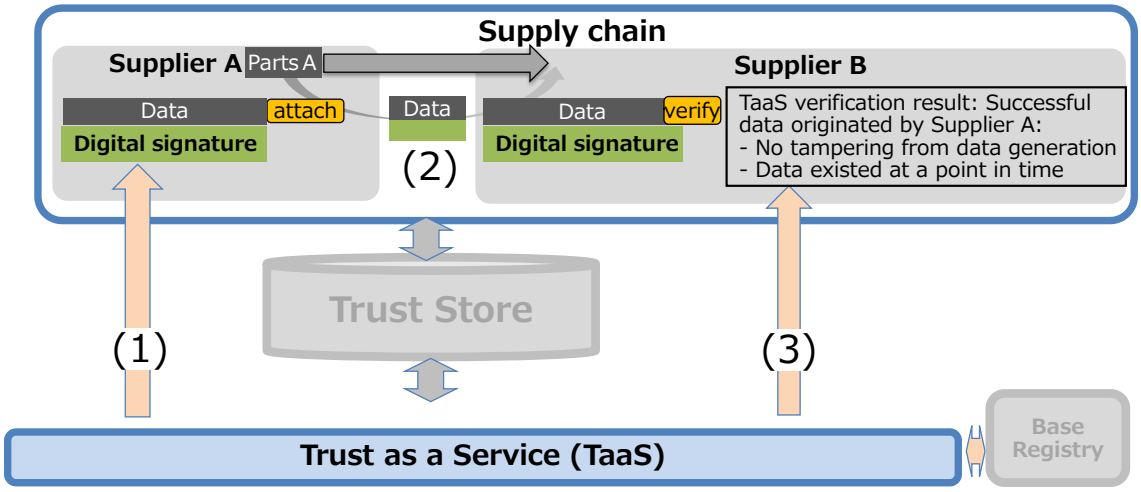


Figure V-8 Visualization of the realization of Goal 1

5-2. Visualization of Goal 2

Goal 2 is to realize that the products manufactured by suppliers and the services they provide have been implemented in accordance with the regulations, including the product manufacturing and service provision process, by confirming the "Digital Evidence." Specifically, "Digital Evidence" is evidence that can be verified by the following items:

(g) Regulation reference information and

(i) Reference information for information as evidence of conduct in accordance with the regulations.

How the supplier's product manufacturing and service provision processes can be verified by the "Digital Evidence" is explained in Figure V-9 items (1) through (2). The assumption is that Supplier B is familiar with the product manufacturing and service provision processes of Supplier A with whom it has already done business.

(1) Supplier B traces and obtains Digital Evidence D from Supplier D's "Trustworthiness Information D" in order to check that Supplier D is able to implement the same processes as Supplier A does in accordance with the regulations.
(2) Supplier B can confirm through Digital Evidence D that Supplier D's processes can be performed in accordance with the regulations.

The items above allow Supplier B to select Supplier D in response to changes in its needs and the external environment.

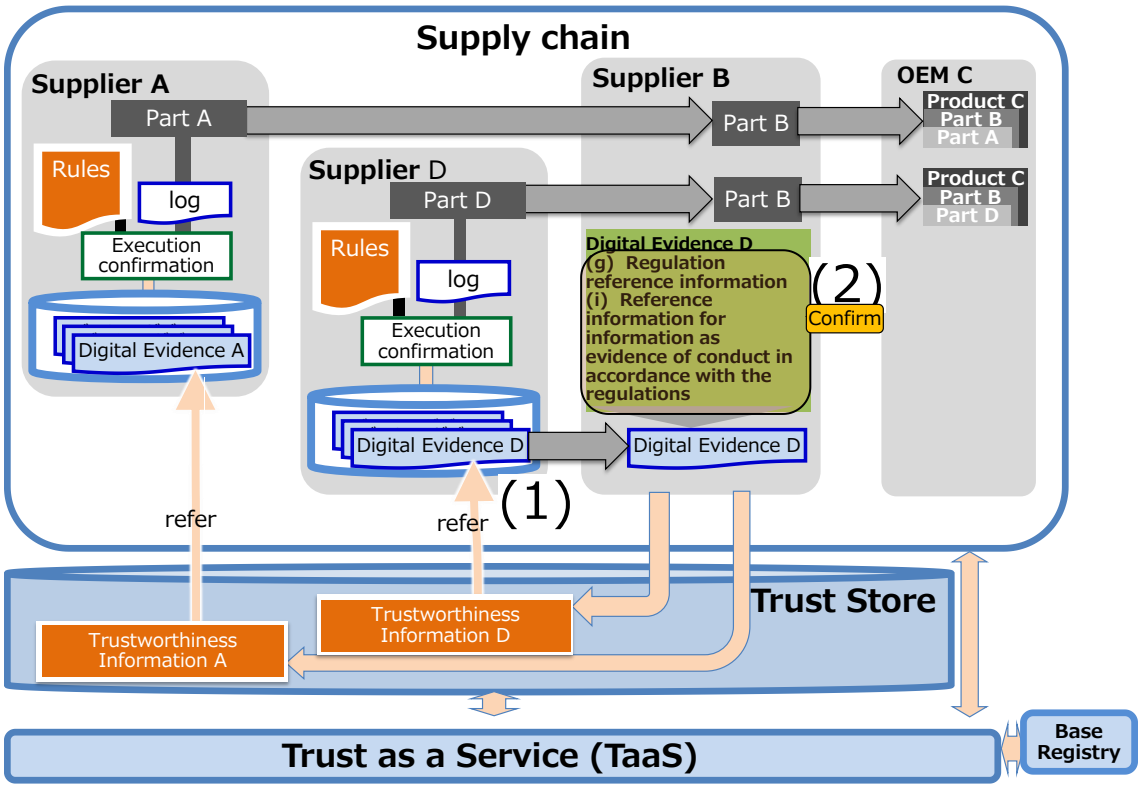


Figure V-9 Visualization of the realization of Goal 2

5-3. Visualization of Goal 3

Goal 3 is achieved by narrowing down the scope of influence of the cause of a problem in the supply chain by tracing the supply route of the parts or services that caused the problem. Specifically, the following items of the "Linkage Information" are used to narrow down the scope of influence:

(j) Information showing connection to the organization and
(k) Information indicating the supply routes for products and services.

The “Linkage Information” allows us to narrow down the scope of impact. Figure V-10 : Explanation of the “Linkage Information” illustrates how the scope of influence can be narrowed down. Assume that a problem occurs in product C manufactured by OEM C, and that the cause of the problem has been identified as component A.

The problem is caused by component A.

(1) OEM C queries the Trust Store for the part that uses part A. From the “Linkage Information E,” OEM C confirms that supplier E’s part E uses part A.

(2) OEM C queries the Trust Store for products that use part E. From the “Linkage Information F,” OEM C confirms that OEM C’s product F uses part E, that is, part A.

The items above confirm that OEM C’s Product F uses part A and that the problem with part A spills over to product F.

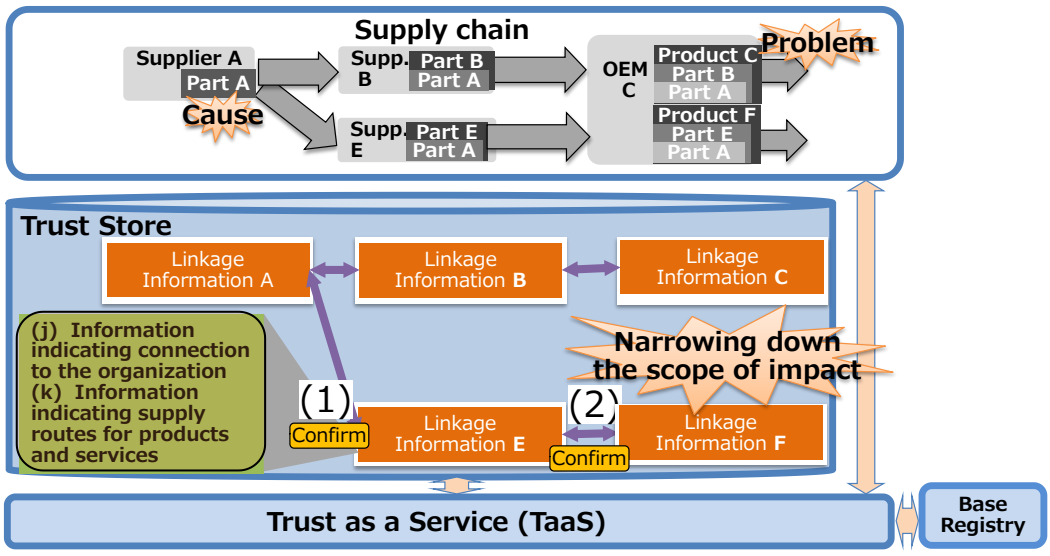


Figure V-10 Visualization of the realization of Goal 3

5-4. Visualization of Goal 4

Goal 4 is achieved by tracing the supply route of each product or service, to confirm that it has been implemented in accordance with the regulations in the product manufacturing and service provision processes of the entire supply chain. Specifically, “Trustworthiness Information,” “Linkage Information,” and “Digital Evidence” are used to confirm that the entire supply chain has been implemented in accordance with the regulations in the product manufacturing and service provision processes.

How the entire supply chain can confirm that the regulations have been implemented in accordance with the regulations is explained in Figure V-11 items (1) through (2) and below. The assumption is that there are rules and guidelines that apply to the entire supply chain, and that OEM C is familiar with the fact that its manufacturing and supply processes follow these rules and guidelines.

(1) To understand the upstream suppliers, OEM C first traces "Linkage Information C" to "Trustworthiness Information B" and then to Digital Evidence B to confirm the basis on which Supplier B manufactured products according to the regulations.
(2) OEM C traces the information from "Linkage Information B" to "Trustworthiness Information A" and further to Digital Evidence A, and confirms the evidence that Supplier A manufactured the product in accordance with the regulations. Thereafter, the confirmation is repeated in the same manner.

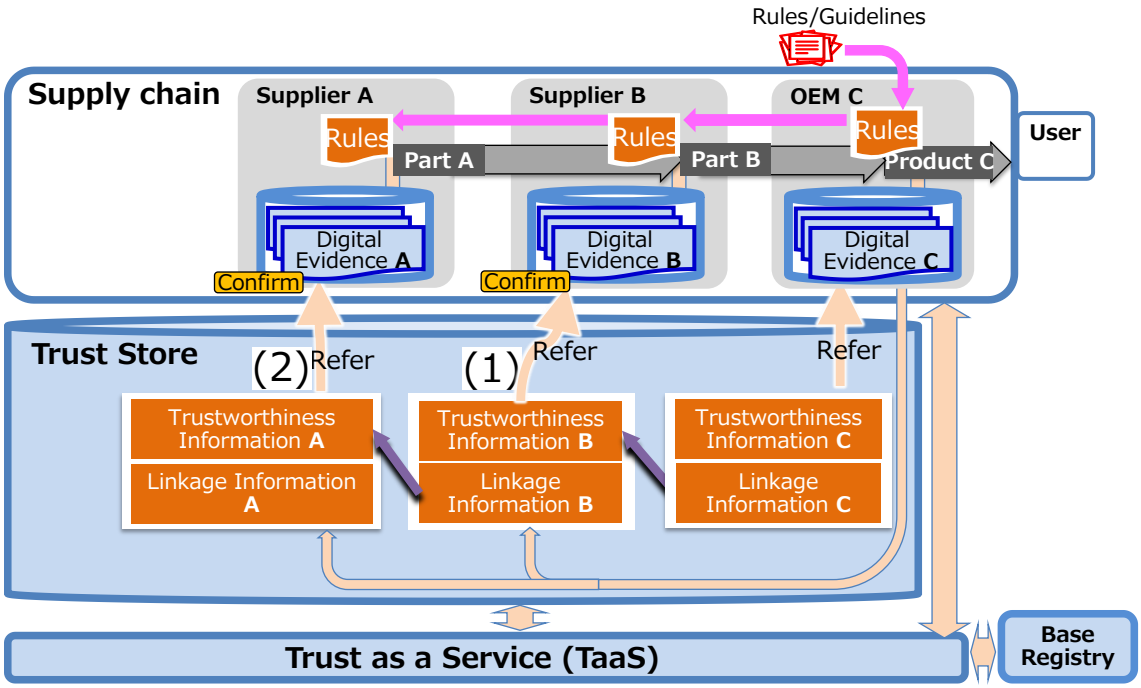


Figure V-11 Visualization of the realization of Goal 4

For example, if the visualization above is applied for the use case of carbon dioxide emissions calculation, the "Trustworthiness Information" can confirm that the carbon dioxide emissions are from Suppliers A and B and that they have not been falsified. The correctness of the carbon dioxide emission values can also be verified with the "Digital Evidence" from Suppliers A and B.

VI. Use cases

Use cases are described below.

1 Mechanisms to ensure the trustworthiness of data coming out of the equipment

Overview of Trust

In recent years, social infrastructure such as oil, electric power, and gas, as well as buildings and factories, have been increasingly applying new technologies such as IoT and AI to monitor and diagnose the status of component and facilities constantly from remote locations to improve safety and efficiency. For example, manufacturers deliver their products to businesses and have a predictive detection system that remotely monitors the products and analyzes the data emitted from the products to detect abnormalities at a predictive stage. This predictive detection system helps prevent failures and accidents before they occur and identifies maintenance and tune-up services, thereby allowing an accurate prediction of the remaining life of a component and the implementation of repairs and replacements at the appropriate time. In such cases, if the destination of data acquisition, timing of data acquisition, or data generated from the product is incorrect, the diagnosis results would also be incorrect. If an inappropriate response based on incorrect diagnostic results causes a work stoppage, trust in the maintenance and tune-up services would also be lost. Therefore, it is important for manufacturers to ensure the trustworthiness of the data produced by their products.

Before (issues)

Manufacturers are unable to confirm or verify whether data obtained from products used by their businesses are trustworthy data. For example, in providing the maintenance and tune-up services indicated above, there are currently no standards or guidelines to determine what aspects or requirements must be met for data to be considered trustworthy, or what level of trustworthiness is required. In addition, manufacturers cannot demonstrate or verify to third parties that the services they provide based on the data obtained from their products are supported by trustworthy data. Hence, there is a risk that some services may be operating under standards that are inappropriate compared with international and technological trends.

After (goals)

Manufacturers and businesses can show or verify to third parties, based on guidelines

issued by governments and other organizations, that the work or services they perform according to data obtained from the products they use are supported by trustworthy data. The guidelines present the level of trustworthiness required according to the industry sector and business type, and specify the requirements and standards necessary for each level, so that companies can provide services whose trustworthiness is ensured.

Realization methods

An illustration of the realization of "trustworthy data" is shown below using the case of maintenance service. Figure VI-1 shows how to realize "Trustworthy Data" in the Trust realization methods using TaaS in the supply chain shown in Figure V-3.

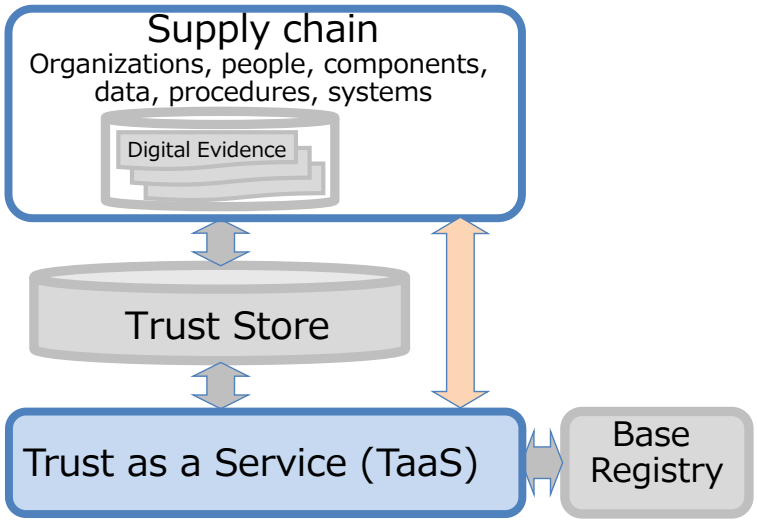


Figure VI-1 How supply chain trust is realized in this use case

The aspects necessary for the trustworthiness of the data coming out of the equipment are defined, and a use case is presented below in which the service provider provides a service that satisfies these aspects.

Manufacturer A delivers Product A' manufactured by itself to Business Operator B, remotely monitors Product A', and provides maintenance services based on the data emitted from Product A'. Business Operator B defines and implements the aspects necessary for trustworthiness of the data from Product A' equipment. The aspects necessary for trustworthiness are items (i) and (ii) below.

(i) Definition of the aspects necessary for the trustworthiness of the data coming out of equipment

The existing document [Comprehensive Data Strategy '21] describes “aspects of data trust” to replace physical space with data in the cyber world. In the section on “Aspects of Data Trust,” it is mentioned that the components of physical space, such as who (subject/intention), what (facts/information), and when (time), must be correctly reproduced as “aspects of trust” in cyberspace as well.

Therefore, to ensure trust by replacing data from a piece of “equipment” in physical space with data in the cyber world, trust in the details regarding (a) who, (b) what, and (c) when with respect to the equipment, as described below, are considered necessary.

(a) The user (organization) of the equipment is correct.

- The “organization” using the equipment is correct (ensuring the trustworthiness of the entity using the equipment).
  Example) Use of electronic signatures.

(b) The equipment is correct, as determined through:

- Confirmation of the existence of the equipment and assurance of the trustworthiness of the equipment,
- Assurance by the manufacturing vendor who produced the equipment (that the component specifications [including security], manufacturing process, versions/updates, and so on are valid),
- Trustworthiness of the products, that is,
  (α) Products are made by trustworthy manufacturers and
  (β) Products contain a private key corresponding to a certificate that can only be produced by a trusted manufacturer.
  Example) Key for data is set on a secure chip or other component using a key for activation that is embedded prior to shipment by a trusted manufacturer
  Example) Use of eSeals (to be listed in the extended area of the digital certificate for eSeals)
  *The entity issuing the ID of the equipment depends on the use case and the level of trust required (see below).

(c) “Existence and time,” which refers to the correct time of data generated by the equipment.

- Proof that it existed at a certain point in time and has not been tampered with since.
  Example) Time-stamping

Data from each sensor is time-stamped using TaaS.

(ii) Trust models according to the level of trust required to ensure trustworthiness

Regarding the mechanism for ensuring trust in the "components" and the mechanism for ensuring trust, which is necessary to ensure the trustworthiness of data from a piece of equipment as described in (1) above, trust is classified into two categories: (1) private trust and (2) public trust, as described in Section V-3.

Private trust in (1) can be classified into the following four types, including public trust, depending on whether it is secured within an organization, between organizations, or at the community level, such as industry associations (with participation and withdrawal procedures) for shipping, medical care, and so on.

(a) Local private trust

Trust is secured through certificates issued by the company's own certification authority (CA) for products manufactured by the company.

(b) Peer trust

Trust is ensured between two parties: the business that manufactures the product and the business that uses the product.

(c) Community trust

Trust is secured through certificates from the community, such as trade associations to which the company manufacturing the product belongs.

(d) Public trust

Trust is secured through a certificate from an official body.

Following are Cases 1 and 2 regarding ensuring trustworthiness.

(Case 1)(a) Example of local private trust

Step 1: Issuance of certificates

Concrete examples of the items of information to be generated in Step 1 are shown in Table VI-1.

Table VI-1 Concrete examples of items of information to be generated in Step 1

No	Information items		Concrete examples
1	"Trustworthiness Information"		Certificate for Services
2		(e) Information confirming that the originator is not fraudulent	Identifiable name of the private certification authority (CA) that issued the certificate for the service

Currently, many institutions use their own CA. The use of manufacturer A's own CA (hereinafter, "private CA") operated by manufacturer A improves the trust for remote monitoring and remote maintenance. Manufacturer A's private CA holds the private CA's certificate and corresponding private key, and issues certificates for activation (certificates used for license authentication when activating product features) and for services (certificates used to verify digital signatures granted to data generated by services provided by the product).

Step 2: Digitally sign the data

Concrete examples of the items of information to be generated in Step 2 are shown in Table VI-2.

Table VI-2 Concrete examples of items of information to be generated in Step 2

No	Information items		Concrete examples
1	"Trustworthiness Information"		Digital signature
2		(a) Object identification information	Product A'
3		(b) Generation date and time information	Output date and time of events, logs, and alerts
4		(c) Location of generation and source information	Business B
5		(d) Information confirming that the data have not been falsified or switched	Digital signature with certificate for service
6		(e) Information confirming that the originator is not fraudulent	N/A
7		(f) Information confirming that the data existed at a certain point in time	N/A

When Manufacturer A manufactures Product A' using parts procured from suppliers whose manufacturing processes and so on are trustworthy, and further installs Product A' at Operator B and collects data from Product A', it does the following:

1. Manufacturer A incorporates the certificate for activation issued by the private CA and the corresponding private key into product A';
2. Manufacturer A installs Product A' at Service Provider B and performs the activation process using the private CA certificate and the certificate for activation. If the activation process is successful, the certificate for service and the corresponding private key issued by the private CA are incorporated into Product A'; and
3. Product A' digitally signs its own output data, such as events, logs, and alerts, with the private key corresponding to the certificate for service and sends it to manufacturer A.

Step 3: Digital signature verification

Concrete examples of the items of information to be generated in step 3 are shown in Table VI-3.

Table VI-3 Concrete examples of items of information to be generated in Step 3

No	Information items		Concrete examples
1	"Trustworthiness Information"		Digital signature with certificate for service
2		(d) Information confirming that the data have not been falsified or switched	Digital signature verification results

Manufacturer A verifies the digital signature assigned to the output data using the certificate for service assigned to product A'. If the verification result of the digital signature is successful (i.e., the feature value of the output data and the signature value match), the output data is accepted as trustworthy and used for the remote maintenance service. If the verification result is not successful, the output data is assumed to be untrustworthy and is not used for the remote maintenance service, and a log of the acceptance of the untrustworthy output data is recorded.

Steps 1 through 3 describe (a) the case for ensuring trustworthiness in private trust.

Note that (a) if only private trust is valid, this means that business operator B does not trust the certificate issued by manufacturer A's private CA. Therefore, with the method

described above, there is an issue that business entity B cannot technically verify the trustworthiness of the data. However, it can be said that sufficient trust is ensured when manufacturer A limits the purpose to maintenance and so on, of the products it has manufactured.

(b) If peer trust is valid, then business operator B can trust the certificate issued by manufacturer A's private CA. Therefore, in the manner described above, business B can also technically verify the trustworthiness of its products and data. However, individual verification, contracts, and so on are required to confirm that the private CA is trustworthy.

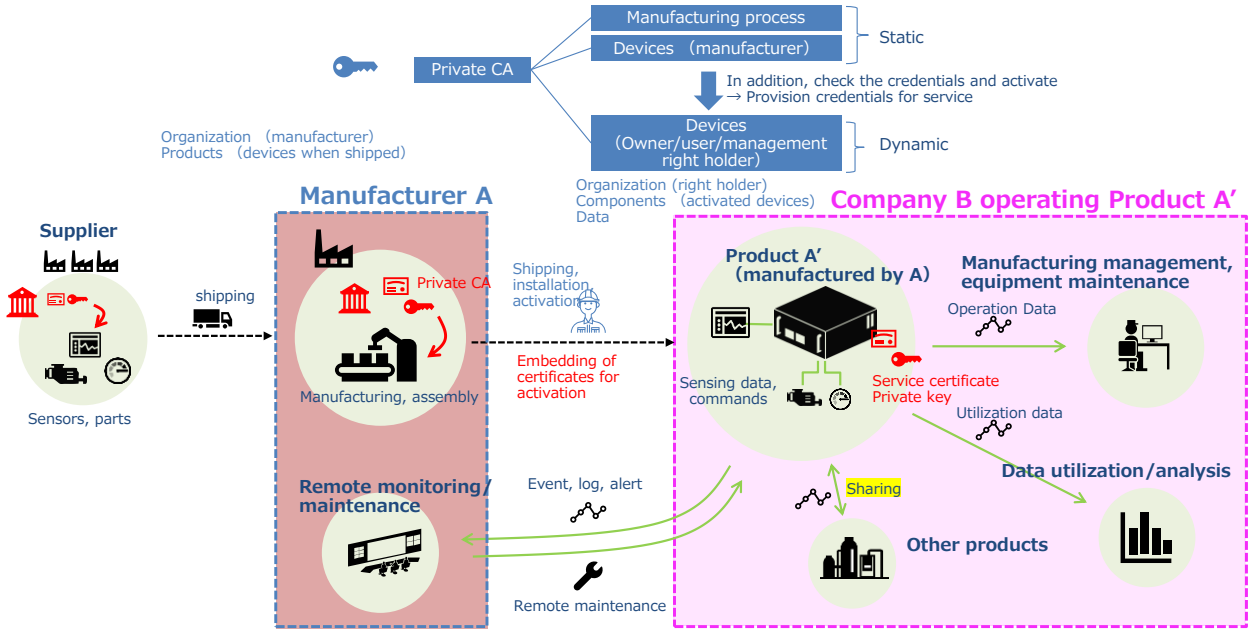


Figure VI-2 Examples of peer trust application (current status)

By additionally verifying the certainty of the data generation process, it is also possible to demonstrate the correctness of the particular data, which can contribute to improving the quality of maintenance and tune-up services.

(Case 2) (d) Example of public trust

Step 1: Issuance of certificate

Concrete examples of the items of information to be generated in Step 1 are shown in Table VI-4.

Table VI-4 Concrete examples of information items to be generated in Step 1

No	Information items		Concrete examples
1	“Trustworthiness Information”		Certificate for Services
2		(e) Information confirming that the originator is not fraudulent	Identifiable name of the third-party CA that issued the certificate for the service

It is expected that in the future there will be cases of using third-party trust services. The use of an intermediate CA operated by manufacturer A improves trust for remote monitoring and remote maintenance. Manufacturer A is assigned the intermediate CA’s certificate and corresponding private key, and the intermediate CA is assigned the root CA and corresponding private key. The intermediate CA issues a certificate for activation and a certificate for service.

Step 2: Digitally sign the data

Concrete examples of the items of information to be generated in Step 2 are shown in Table VI-5.

Table VI-5 Concrete examples of items of information to be generated in Step 2

No	Information items		Concrete examples
1	“Trustworthiness Information”		Digital signature
2		(a) Object identification information	Product A'
3		(b) Generation date and time information	Output date and time of events, logs, and alerts
4		(c) Location of generation and source information	Business B
5		(d) Information confirming that the data have not been falsified or switched	Digital signature with certificate for service
6		(e) Information confirming that the originator is not fraudulent	eSeal
7		(f) Information confirming that the data existed at a certain point in time	Time-stamping

The remaining steps are the same as in Step 2 of (Case 1).

Step 3: Digital signature verification

Same as step 3 in (Case 1).

Steps 1–3 describe item (d) use of public trust to ensure trustworthiness.

If (c) community trust within a community, such as an industry association, is established, manufacturer B can trust the intermediate CA operated by manufacturer A through the root CA if manufacturer A and operator B belong to the same community.

Furthermore, if (d) public trust is established, manufacturer B can trust the intermediate CA operated by manufacturer A through the root CA, even if manufacturer A and operator B do not belong to the same community. Therefore, it can be expected that barriers to services using products and data will be lowered, thus encouraging the emergence of new services.

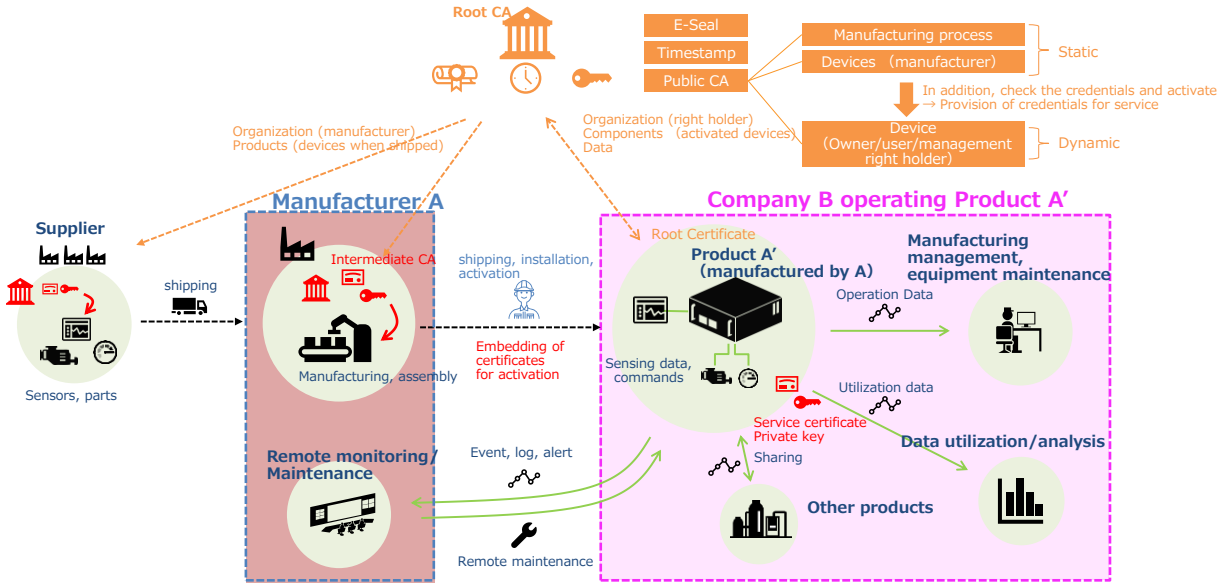


Figure VI-3 Examples of public trust application

Which type of trust model out of (a), (b), (c), and (d) to use should be flexible, as the level of trust required depends on the business type, scale, and field.

For (i)-(a) "correctness of the user (organization) of the component (proof of the organizations of service providers A and B)" in Cases 1 and 2 above, it is possible to use an eSeal issued to service provider B by the root CA and so on (to be listed in the extended area of the digital certificate for eSeal). In addition, for (i)-(c) "existence and time," a time stamp may be used to verify that the information on time of data generated by the

component is correct. Moreover, it is necessary to consider the development of a system that encourages business operators A and B to use external (third-party) trust services such as eSeals and time stamps (trust services being one of the components of TaaS), and incentives such as subsidies for the CA operating costs of CA certification authorities. Furthermore, it is necessary to consider various measures, such as entering into the framework of businesses that have already achieved peer trust, so that small and medium-sized enterprises (SMEs) and other entities that have difficulty establishing private CAs will not be left behind in this mechanism.

By applying the realization methods discussed above, it can be easily verified that the component indicated by the data from the product actually exists and that it is not fraudulent, which can be used to diagnose the timing of maintenance and servicing. In addition, by additionally verifying the certainty of the data generation process, it is possible to demonstrate the correctness of the particular data, which can contribute to improving the quality of maintenance services.

2 Efforts to reduce carbon emissions throughout the supply chain

Overview of Trust

This use case describes the situation of a vehicle manufacturer that illustrates the results of a calculation of carbon dioxide emissions throughout the supply chain of a product to demonstrate to society its efforts to reduce to zero the carbon dioxide emissions in its supply chain.

To combat global warming, companies have a social responsibility to decarbonize their operations. Carbon dioxide emissions are measured by the Green House Gas Protocol (GHG Protocol),[15] and as shown in Figure VI-4, supply chain emissions are defined as Scope 1 (direct emissions), Scope 2 (indirect emissions), and Scope 3 (emissions other than Scopes 1 and 2 under 1-15 in Figure VI-4). Emissions are calculated by multiplying the activity amount by the emissions intensity. The amount of activity is the amount related to the scale of the business's activities, for example, the amount of fuel burned by the business in Scope 1, the amount of electricity used by the business in Scope 2, and the amount of cargo transported and waste disposed of in Scope 3. When considering the amount of fuel or electricity used by the company, it is sufficient to measure the consumption of fuel or electricity. However, when considering the amount of activity

[15] Greenhouse Gas Protocol, URL=https://ghgprotocol.org/

related to the transportation and delivery of cargo at other companies, it is necessary to grasp the fuel consumption and loading capacity of transportation trucks as well, and the calculation process must be confirmed along with the values of these activity quantities.

With regard to the calculation of such emissions, there is a movement in Europe called the Life Cycle Assessment LCA Regulation,[16] which evaluates the environmental impact throughout the product life cycle, and it is expected that businesses operating in Europe will need to take action, including third-party certification.

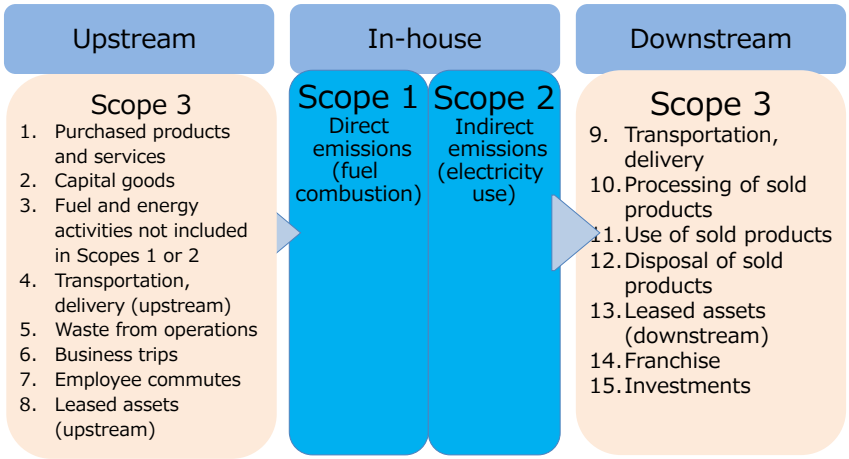


Figure VI-4 Classification of supply chain emissions into Scopes 1–3 (figure taken from the Ministry of the Environment Supply Chain Emissions Calculation)

Before (issues)

According to the Ministry of the Environment's guidelines,[17] in addition to the conventional supply chain activities, it is necessary in Scope 3 to ascertain the amount of activities specific to the calculation of emissions, such as the amount of cargo transported and waste treated; this is time-consuming and labor-intensive. In the future, the emissions calculation process is expected to require third-party certification and more accurate emissions values than in the past, owing to LCA regulations and other factors. To comply with these requirements, businesses must accurately calculate emissions, and a third party must confirm with evidence the calculation of emissions for the entire supply

[16] European Platform on Life Cycle Assessment (LCA), URL=https://ec.europa.eu/environment/ipp/lca.htm

[17] Ministry of the Environment, Green Value Chain Platform: For those starting to calculate supply chain emissions (env.go.jp) http://www.env.go.jp/earth/ondanka/supply_chain/gvc/supply_chain.html

chain, which requires time and man-hours for the calculation process. If the measurement method, conditions, or data falsification of the data used for the calculation is even partially suspected, it will be difficult to ascertain and explain the actual situation.

After (goals)

Organizations in the supply chain can achieve the following by establishing regulations for the processes involved in determining the amount of activity to calculate carbon dioxide emissions, and by keeping records of implementation in accordance with those regulations:

- Make it easy to confirm that the calculation process of activity amounts is trustworthy by collecting implementation records,
- Be able to maintain records that can be verified for tampering with the implementation records,
- Easily and remotely explain with evidence the process of calculating the carbon footprint of the entire supply chain and use it for third-party certification, and
- Depending on the level of confidence required for the amount of activity, establish a system that enables not only verification of the process and its implementation records, but also verification of measurement components and measurements, and the presentation of data to ensure a higher level of confidence.

Realization methods

The realization methods are explained while showing the information items for this use case in Section V-4.

Step 1: Prepare regulations

Concrete examples of the items of information to be generated in Step 1 are shown in Table VI-6.

The vehicle module manufacturer shall define the manufacturing process of the Electronic Control Unit (ECU) in advance as module manufacturing regulations. The manufacturing regulation shall include the calculation of carbon dioxide emissions associated with the manufacturing activities. In the following sections, the rules are referred to in (g) Reference information to rules.

Table VI-6 Concrete examples of items to be generated in Step 1

No	Information items		Concrete examples
1	“Trustworthiness Information”		CO2 reduction certificate
2		(g) Reference information to regulations	Document number corresponding to the module manufacturing regulations to reduce carbon dioxide emissions to the prescribed target

Step 2: Generate “Digital Evidence”

Concrete examples of the items of information to be generated in Step 2 are shown in Table VI-7.

Table VI-7 Concrete examples of items of information to be generated in Step 2

No	Information items		Concrete examples
1	“Digital Evidence”		Implementation Confirmation Result
2		(g) Regulation reference information	Document number to module manufacturing regulations to reduce carbon dioxide emissions to the prescribed target
3		(i) Reference information for information as evidence of conduct in accordance with the regulations	Verified module manufacturing implementation records

As shown in Figure VI-5, modules are manufactured in accordance with the regulations, and the actual amount of various types of activity and the amount of carbon dioxide emissions calculated by multiplying the amount of activity by the emission unit are recorded as the implementation record. The module manufacturing regulations and the module manufacturing implementation records are compared to confirm that the module manufacturing was carried out in accordance with the regulations. This verification process shall be performed by the vehicle module manufacturer or a third party. Once it has been confirmed that the module has been implemented in

accordance with the regulations, items (g) and (i) shall be recorded as "Digital Evidence" for in-house verification.

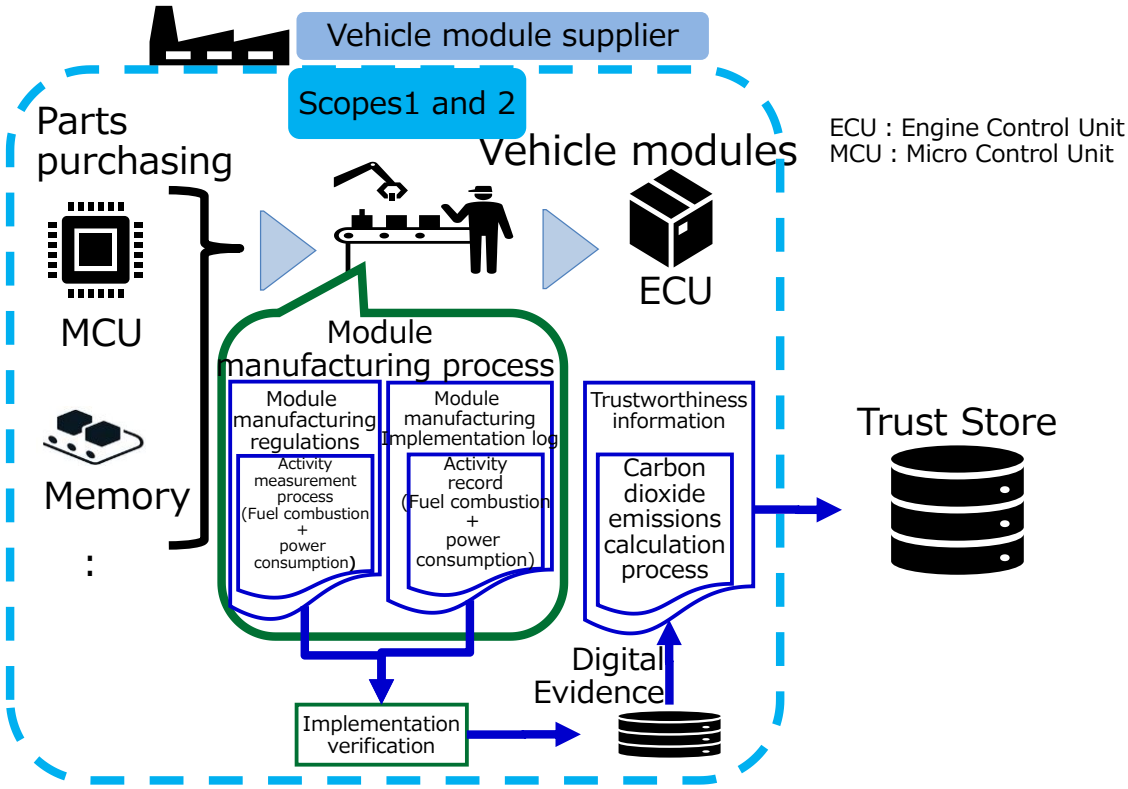


Figure VI-5 Generating "Digital Evidence"

Step 3: Generate “Trustworthiness Information”

Concrete examples of the items of information to be generated in step 3 are shown in Table VI-8.

Table VI-8 Concrete examples of items to be generated in Step 3

No	Information items		Concrete examples
1	“Trustworthiness Information”		CO2 reduction certificate
2		(a) Object identification information	ECU Serial Number
3		(b) Generation date and time information	Date of ECU production
4		(c) Location of generation and source information	Vehicle Module Supplier Factory Name
5		(d) Information confirming that the data have not been falsified or switched	Digital signature by a person who has verified the implementation
6		(e) Information confirming that the originator is not fraudulent	eSeal
7		(f) Information confirming that the data existed at a certain point in time	Time-stamping
8		(g) Regulation reference information	Document number to module manufacturing regulations to reduce carbon dioxide emissions to the prescribed target
9		(h) Reference information for information as evidence of conduct in accordance with the regulations	Document number to be recorded in the verified module manufacturing implementation record

The “Trustworthiness Information” is information that indicates the accuracy of the carbon dioxide emissions emitted during the manufacturing process of the vehicle module ECU. Items (a), (b), and (c) represent information that identifies the target ECU, the date and time the “Trustworthiness Information” was generated, and the organization that generated the “Trustworthiness Information,” respectively. To indicate the accuracy of the carbon dioxide emissions, “Digital Evidence” is made available for reference by items (g) and (h). The trustworthiness of these data is ensured by items (d), (e), and (f).

Step 4: Generate “Linkage Information” (Bill of Materials, BOM of ECU) and store it in the Trust Store

A Concrete example of the items of information to be generated in step 4 is shown in Table VI-9.

Table VI-9 Concrete examples of items to be generated in Step 4

No	(Data) items		Concrete examples
1	“Linkage Information”		ECU Parts List
2		(j) Information showing connections to the organization	N/A
3		(k) Information indicating supply routes for products and services	CO2 reduction certificate number for each ECU component

Figure VI-6To be able to calculate the carbon dioxide emissions extended to the entire supply chain as shown in Figure VI-6, items (j) and (k) are added and stored in the Trust Store along with the “Trustworthiness Information.”

Step 1–4 above allow the accuracy of Scopes 1 and 2 of carbon dioxide emissions to be demonstrated, as well as the accuracy of Scope 3 of carbon dioxide emissions for the entire supply chain. The “Trustworthiness Information” and “Linkage Information” stored in the Trust Store allow for easy remote verification with evidence and are also compatible with third-party certification.

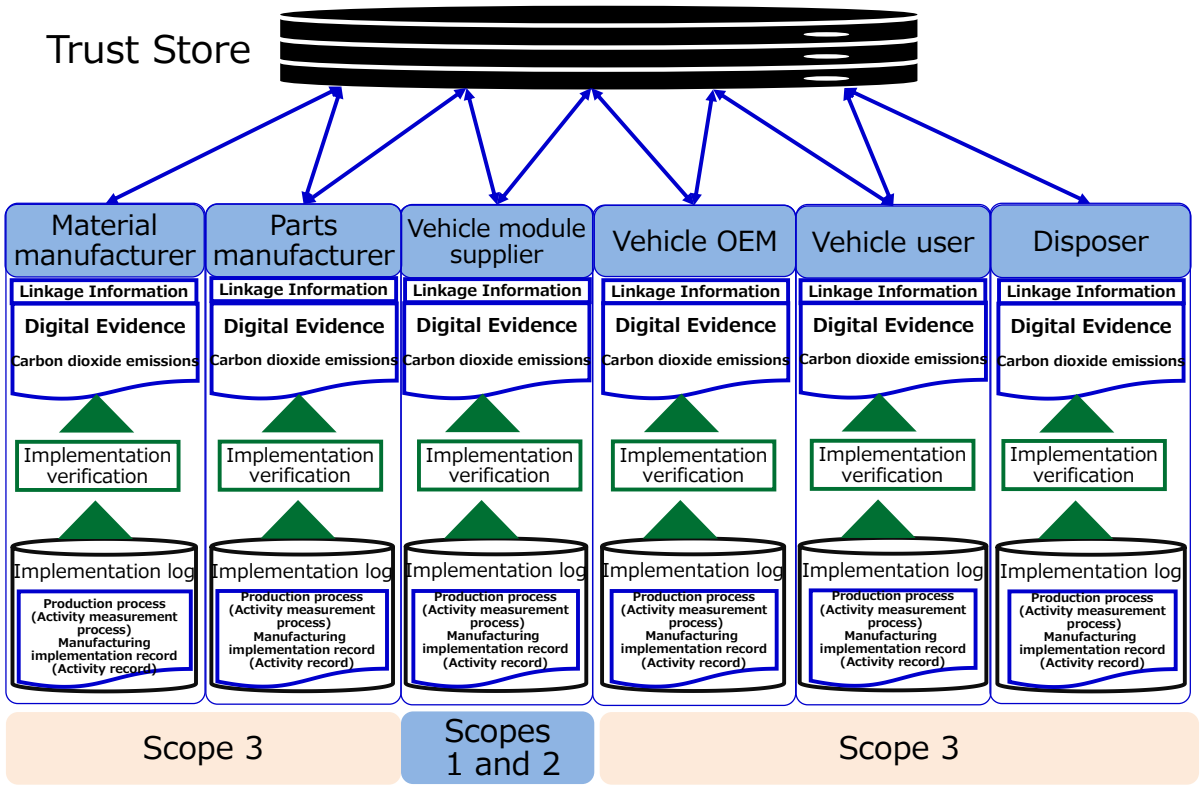


Figure VI-6 Managing carbon emissions throughout the supply chain

As a supplement to the “Digital Evidence” in Step 2, it is also expected that there will be cases where organizations in the supply chain will be required to have higher levels of trustworthiness depending on the type of business and level of trustworthiness required by the application case and the level of trustworthiness required by the regulations.

For example, in ascertaining the amount of activity, digital data measured using trustworthy sensors is more trustworthy than data collected visually by humans, in the sense that it is free from human error. Furthermore, the trustworthiness can be further enhanced by guaranteeing that the “activity amount” (data) itself measured using sensors has not been tampered with.

In other words, in use case (VI-1), a mechanism to ensure the trustworthiness of the data coming out of the component and a mechanism to guarantee the “activity figures” by establishing criteria for trusting the figures output by the sensors can be confirmed to improve the trustworthiness further. Such a guarantee mechanism can be easily and inexpensively implemented through the use of TaaS. It is then desirable to be able to select the appropriate means and level of trustworthiness depending on the nature of the supply chain.

3 Identifying security measures throughout the manufacturing supply chain

Overview of Trust

This use case is an example of checking the security of the entire manufacturing supply chain. Based on contracts with product suppliers, organizations in the supply chain are obligated to deliver products with the contracted quality, delivery date, and price (the so-called QCD). In addition to QCD, the supply chain organization is also required, for example, to implement security measures in the manufacturing process of the product.

In the case of the automotive manufacturing industry, an example is that German automakers require organizations in the manufacturing supply chain to take security measures to ensure that prototype vehicle design information is not leaked from contractors.

Before (issues)

To confirm that organizations in the manufacturing supply chain have implemented security measures in the manufacturing process, it is necessary to check the manufacturing regulations against what has been implemented based on those regulations, and it takes a lot of time and man-hours to confirm that the security measures are appropriate. It then takes even more time and man-hours to confirm that the security measures implemented throughout the entire manufacturing supply chain are appropriate.

After (goals)

The processes related to security that should be implemented by organizations comprising the manufacturing supply chain should be defined as regulations; records of implementation according to the regulations should be kept, and by collecting the records, it can be easily verified that security measures have been implemented according to the regulations. In addition, the records of the implementation results should be managed from the time they are recorded so that they can be later verified for tampering. This makes it easy to confirm remotely, without spending time and man-hours, that security measures implemented throughout the manufacturing supply chain have been carried out in accordance with the regulations.

Realization methods

The realization methods are explained while showing the information items for this use case in Section V-4.

Step 1: Prepare regulations

Concrete examples of the items of information to be generated in Step 1 are shown in Table VI-10.

Table VI-10 Information to be generated in Step 1

No	Information items		Concrete examples
1	"Trustworthiness Information"		Manufacturing supply chain security certificates
2		(g) Regulation reference information	Document numbers to security checklists to be implemented in the manufacturing supply chain

The vehicle module manufacturer defines the manufacturing process of the vehicle module in advance as module manufacturing regulations. The manufacturing rules include security rules for the manufacturing process. The rules are referred to in (g) Reference information to rules in the following sections. The security rules include a list of daily security checks during the manufacturing process.

Step 2: Generate "Digital Evidence" (checklist results verified by a third party)

Concrete examples of the items of information to be generated in Step 2 are shown in Table VI-11.

Table VI-11 Information to be generated in Step 2

No	Information items		Concrete examples
1	"Digital Evidence"		Checklist results verified by a third party
2		(g) Regulation reference information	Document numbers corresponding to security checklists performed daily in the manufacturing supply chain
3		(i) Reference information for information as evidence of conduct in accordance with the regulations	Checklist results

As shown in Figure VI-7, modules are manufactured according to the regulations, and the results of security checks conducted in the module manufacturing process are recorded as the implementation records. By comparing the module security regulations with the module manufacturing implementation records, security checks are conducted in accordance with the security regulations. The vehicle module manufacturer or a third party shall confirm the implementation of the security check. Once it is confirmed that the security checks have been conducted in accordance with the regulations, item (g)(i) should be recorded as "Digital Evidence" so that it can be checked in-house.

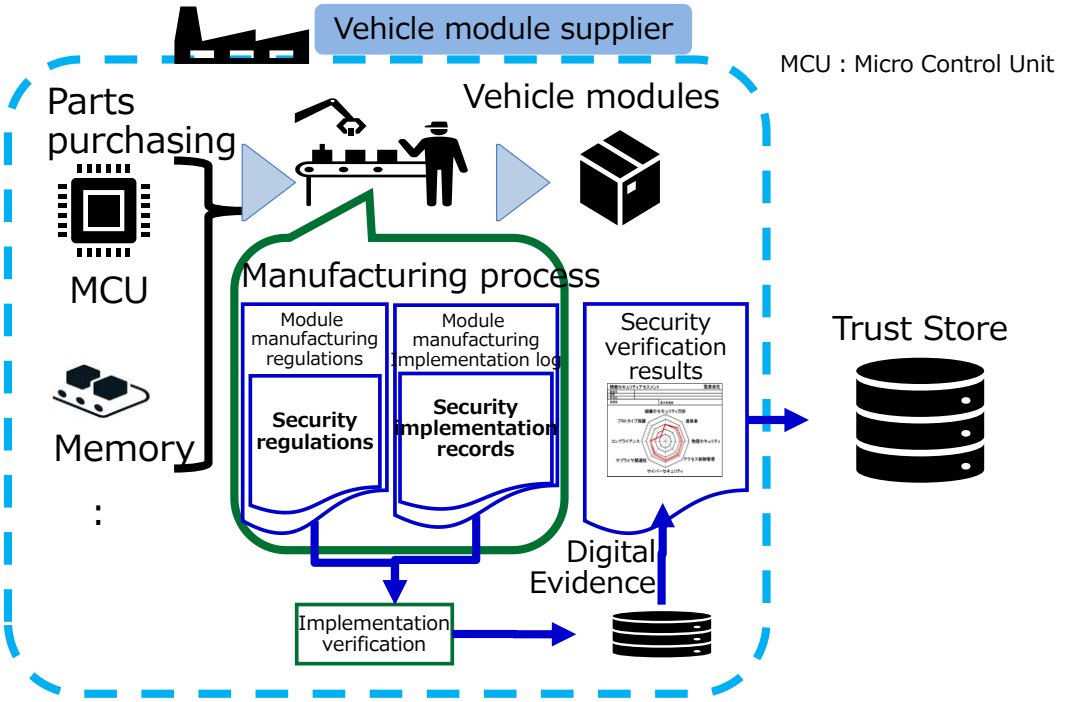


Figure VI-7 Generating "Digital Evidence"

Step 3: Generate "Trustworthiness Information" (security certificates for the manufacturing supply chain)

Concrete examples of the items of information to be generated in step 3 are shown in Table VI-12.

Table VI-12　Information to be generated in Step 3

No	Information items		Concrete examples
1	“Trustworthiness Information”		Manufacturing supply chain security certificates
2		(a) Object identification information	ECU Serial Number
3		(b) Generation date and time information	Date of ECU production
4		(c) Location of generation and source information	Vehicle Module Supplier Factory Name
5		(d) Information confirming that the data have not been falsified or switched	Digital signature by a person who has verified the implementation
6		(e) Information confirming that the originator is not fraudulent	eSeal
7		(f) Information confirming that the data existed at a certain point in time	Time-stamping
8		(g) Regulation reference information	Document numbers to security checklists performed daily during the manufacturing process
9		(h) Reference information for information as evidence of conduct in accordance with the regulations	Reference information to confirmed security checklist results

The “Trust Indication Information” is information indicating that security checks have been correctly performed during the manufacturing process of a particular vehicle module. Items (a), (b), and (c) are respectively the identification of the target vehicle module, the date and time of generation of the “Trustworthiness Information,” and the organization that generated the “Trustworthiness Information.” The “Digital Evidence” in items (g) and (h) shall be available for reference to indicate that the security check was performed correctly. The trustworthiness of these data is ensured in items (d), (e), and (f).

Step 4: Generate “Linkage Information” (list of trading partners in the supply chain) and store it in the Trust Store

Concrete examples of the items of information to be generated in step 4 are shown in Table VI-13.

Table VI-13 Information to be generated in Step 4

No	Information items		Concrete examples
1	“Linkage Information”		List of supply chain trading partners
2		(j) Information showing connections to the organization	Trading partners of each component
3		(k) Information indicating supply routes for products and services	N/A

As shown in Figure VI-8, items (j) and (k) should be added and stored in the Trust Store along with the “Trustworthiness Information” to enable confirmation that security measures have been implemented throughout the supply chain.

Steps 1–4 above enable vehicle manufacturers to confirm the correctness of security measures implemented in the manufacturing process, not only at the manufacturing process of the vehicle module manufacturer from whom the vehicle manufacturer receives supplies, but also at the upstream parts and component suppliers. With the “Trustworthiness Information” and “Linkage Information” stored in the Trust Store, it is easy to confirm remotely that the security measures implemented throughout the manufacturing supply chain are in compliance with the regulations, without spending so much time and man-hours.

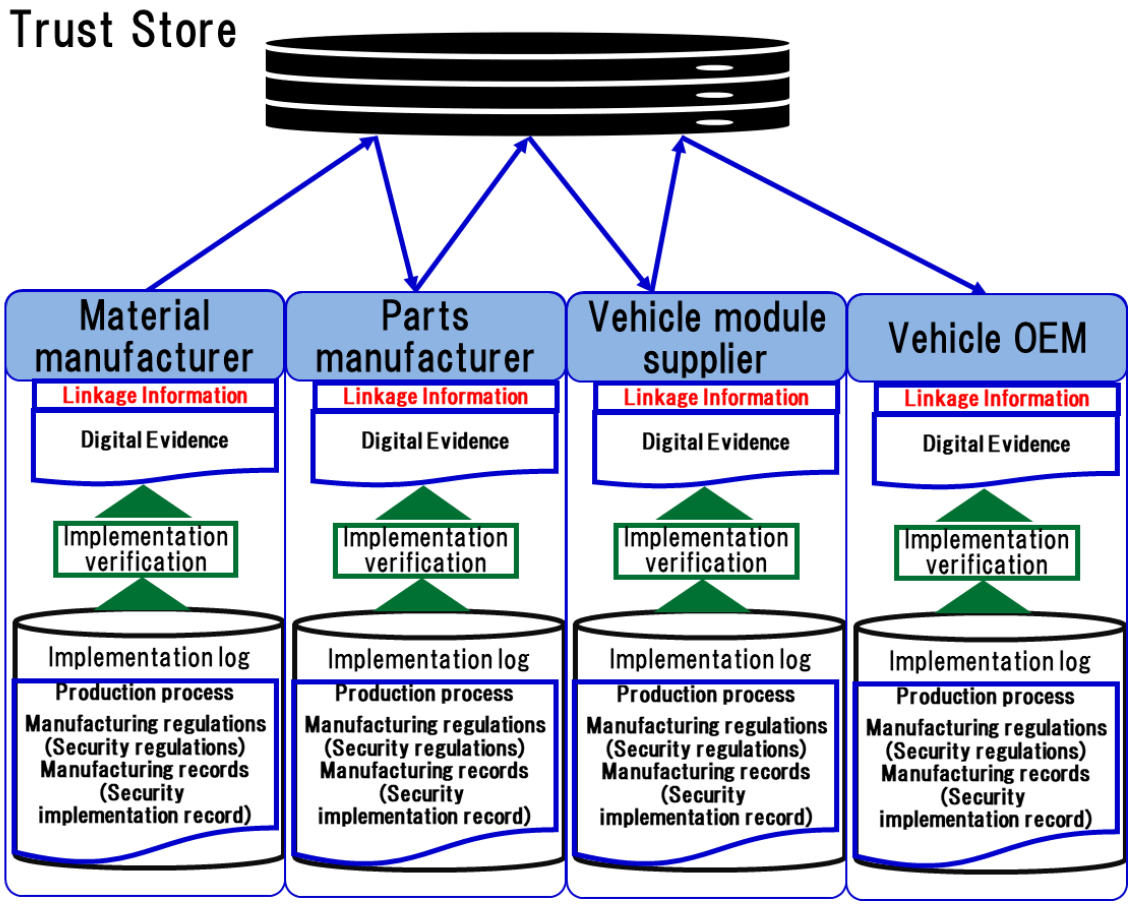


Figure VI-8 Managing security measures throughout the manufacturing supply chain

4 Usage scenarios and effects of Trust as a Service (TaaS)

Table VI-14 shows the effects of having TaaS in the use case (section VI-2).

Table VI-14 Use cases from having Trust as a Service (TaaS, section VI-2)

The Role of TaaS	Usage scenarios in use cases, (Scope 3)	Effects
Sender confirmation	Used to identify registered companies when registering carbon dioxide emissions data with the Trust Store	Identification that the company in question is the same company that issued the procurement contract/invoice (e.g., statement, invoice, and delivery note)
Remote type data integrity (digital signature/remote signature)	Used to record carbon dioxide emissions data and its confirmation results in the Trust Store	After recording, one can see that the data have not been rewritten.

Legitimacy of the procedure system (e.g., digital signature, remote signature, and time stamp)	Used to confirm the activity measurement process in the manufacturing supply chain and the activity volume results based on that process	The activity results of other companies used to calculate carbon dioxide emissions are calculated based on the correct process, and the order of activities in the supply chain can be traced.
Verification	Carbon emissions data recorded in the Trust Store is used by organizations in the supply chain for verification.	Results of third-party verification of carbon dioxide emissions can be reused by other third parties.
User burden reduction (ease of implementation and operation)	Used to build a system to take charge of the activity measurement process	For System Engineers in various sites and processes in the supply chain, it is possible to establish an activity measurement process with less time and man-hours, even without expertise in digital signatures and signature verification.

Trust services do not guarantee the correctness of the data, but rather the authenticity of the organization, person, or thing that issued the data, the non-falsifiability of the data after it is issued, and the non-repudiation that the data was issued by the originator. To estimate whether the data are correct, it is important to show the attributes and context information of the organization, person, thing, procedures, or systems from which the data originated according to the purpose, to facilitate the evaluation of the trustworthiness of the originator. For example, even if data that differ from the actual data are intentionally generated at the time of data generation and protected by a trust service, the data user will not know whether the contents of the data are incorrect, but by issuing the data through a checking mechanism using correct procedures, incorrect operations on the data can be prevented. Such other means are necessary to evaluate the correctness of data contents; using “Digital Evidence” and a Trust Store, listed under the realization methods in section V-3, are examples of such methods. It is also desirable to consider a platform that can combine such attribute proofing services with conventional trust services and provide them as an integrated TaaS.

VII. Recommendations

To establish the mechanism to realize trust in supply chains, which are widely used in society, we provide recommendations in terms of consensus building with various stakeholders and dissemination of the system.

Recommendation: Building consensus and ensuring international consistency to achieve supply chain trust

- What society expects from supply chains include contributions to society and the environment, such as SDGs and ESG, and compliance with globally formed regulations and rules. To meet society's expectations and demands, we should actively promote efforts such as setting up a forum to embody the following points and reach a consensus as an industry group:
  - -Rules and regulations imposed on the entire organization comprising the supply chains as well as standards and guidelines to determine how far to go in implementing them;
  - -The level of trustworthiness required for each industry and business type, and the concept of trust formation;
  - -Standards and guidelines to demonstrate to third parties the trustworthiness of data exchanged along the supply chains;
  - -Standards and guidelines to ensure the trustworthiness of data coming out of equipment; and
  - -Standards and guidelines for the smooth establishment of private trust.

- Considering the global spread of supply chains in the product manufacturing and service provision processes, the three requirements, arrangements for trust formation and confirmation, and ideas presented under Section V. "Measures to resolve the issues" in this white paper must be internationally accepted in the future. Therefore, Japan should take the lead in ensuring international consistency among the relevant standardization bodies and industry associations involved in industrial IoT.

Recommendations: Institutional support for the diffusion of supply chain trust and the formation of ecosystems

- Achieving supply chain trust will increase costs for organizations in the supply chain, especially SMEs. Furthermore, even if only some organizations implement the system, trust for the entire supply chain will not be realized. To solve these issues, it is necessary

to materialize benefits that are commensurate with the costs and incentives for all organizations in the supply chain to work together.

In addition, to sustain trust, it is necessary to modernize the realization mechanisms and ensure that they operate continuously. Specifically, it is important to form an ecosystem in which the organizations that make up the supply chain invest on their own to achieve benefits that exceed their own investments and grow their respective businesses.

To materialize such incentives and create an ecosystem, there should be a forum to discuss and formulate specific milestones and roadmaps, and examine what institutional support and measures are possible in the short, medium, and long terms.

- In realizing a supply chain-wide initiative, it is necessary to examine the technical feasibility and consistency across the various organizations and industries that comprise the supply chain, and embody the value and effectiveness of the supply chain trust. To this end, reference implementation of various functions should be conducted, and a forum should be created where various industries can collaborate to verify and demonstrate the technology and value, and put them to practical use through demonstrations.

VIII. Conclusions

This document builds on the previous version, White Paper Version 1.0, by concretizing the items of information handled in the supply chain and illustrating how these items are applied in specific use cases.

To realize trust in supply chains, it will be necessary to define use cases and target industries, and flesh out the contents and technical specifications of this white paper, such as:

- Shared descriptions of regulations and expectations, and details of implementation checks;
- Information to evaluate trustworthiness and how much risk of trust is acceptable;
- Concrete specifications for Trust Store and "Digital Evidence" utilization interface;
- Interface specifications for coordination between Trust Stores to enable multiple Trust Stores to function together;
- Concrete specifications for overall coordination technology, including TaaS and Base Registry;
- Management technology for public key certificates for equipment, including ID management methods for equipment; and
- Secure key management technology for equipment.