CPSEC-WP-20210001

# Building Trust in Supply Chains

Report Three:
Supply Chains Achieved by Trust-building Technology and Interoperability

October 2020
Cyber Physical Security Research Center
National Institute of Advanced Industrial Science and Technology (AIST)

## Abstract

In recent years, there have been many reported incidents involving damage to the trust in supply chain products and services. In Report One of this White Paper, we analyzed such incidents, showed that compliance with rules is the key to trust, and presented basic ideas for building trust. In Report Two of this White Paper, we explained trust-building technology for building trust in an entire supply chain. This technology consists of trust-related requirements specified when issuing an order, digital evidence of satisfying the requirements from a supplying organization, a certificate generated from the digital evidence, and a chain of certificates. In Report Three, we first overview the nature of the supply chains achievable when trust-building technology has become widespread. To achieve this, it is necessary to ensure interoperability. Thus, we will also investigate what kind of interoperability will be needed, and discuss the steps to be taken to this end.

## 1. Supply chains achievable by trust-building technology

As described in Reports One and Two, in supply chains using trust-building technology, trust requirements, which include not only trust-related but also functional requirements, will be presented at the time of ordering; and at the time of product or service delivery, certificates, and evidence if necessary, will also be supplied, to provide a basis for judging trust in the related products or services. Certificates will be stored in a 'trust store', which is a storehouse of certificates, at the same time.

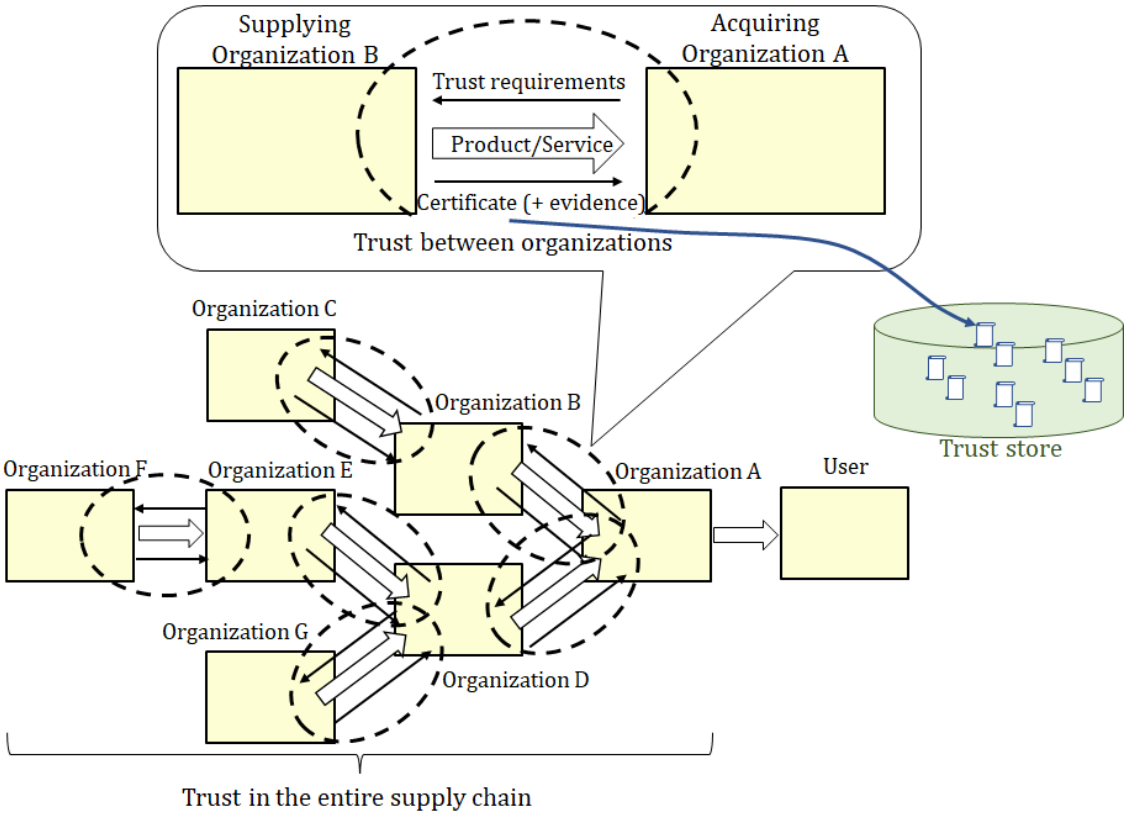


Figure 1 Supply chains interconnected by trust-building technology

As trust-building technology becomes more widespread, trust requirements and certificates will be transferred, to and from supplying and acquiring organizations, for all product and service orders in a given trust-oriented supply chain.
As a result, trust requirements and certificates will become communication tools for issuing and receiving orders in organizations that value trust. This provides the following advantages:

- Supplying organizations can view trust requirements to determine whether their products and services can adapt to the trust requirements.
- Acquiring organizations and users can determine whether products and services meet certain trust requirements by looking at relevant certificates.

These aspects provide more flexibility in determining desired suppliers in a supply chain where trust is important.
Ordering organizations and users can learn more extensively about organizations that offer products or services that meet certain trust requirements, by, for example, presenting the trust requirements in an e-marketplace or searching through certificates stored in a trust store. While order-and-supply relationships in supply

chains have, in the last decade or so, generally been reorganized from being based on fixed relationships, much of the reorganization has focused on changing suppliers for cost reasons. However, cost is not the only important factor in ordering parts and other items, or services, in a supply chain; trust is also important. Both trust requirements and certificates have the effect of visualizing trust in order-and-supply relationships, and this in turn increases the degree of freedom in identifying desirable suppliers when trust is important.

For a supplying organization that values trust, on the other hand, trust-building technology can be a tool to publicize the organization's commitment to trust, and increase the possibility of being selected as a supplier. Specifically, when a supplying organization delivers an ordered product or service, it simultaneously stores a certificate in a trust store, so that all organizations authorized to access the trust store can view the certificate. Traditionally, the trustworthiness of a product or service was invisible and could only be judged by actually using it or based on references. While empirical judgments and references are important, certificates, as an element for visualizing trust in an organization's products and services, provide an objective measure of trustworthiness. The presence of a trust store also allows trustworthiness to be openly measured. Information about the trustworthiness of products and services gained through experience has traditionally been communicated from person to person. Therefore, transmission of such information tends to be localized. If people have access to a trust store, however, they can know the trustworthiness of products and services from anywhere in the world. Trustworthy products and services have the potential to expand organizations' markets worldwide, regardless of the size of the organization, due to the presence of the trust store.

Further, the visibility of trust through trust requirements and certificates will lead to more emphasis on trust as a criterion for selecting products and services. The price of a product or service is important not only because the price directly affects the earnings of the organization that purchases it, but also because prices can easily be compared on a numerical scale. There is no doubt that trust is important to organizations. Traditionally, however, there has been no valid measure of trust that allows the use of trust as an evaluation item. Trust requirements and certificates are not as straightforward as numerical values, but they give a partial solution to the problem of trust comparison; and if such a measure is provided, it will be easier to use and focus on trust as an evaluation item. Moreover, if trust becomes a key selection criterion, organizations will be more proactive in improving their trustworthiness. As a result, society as a whole will be able to improve the

trustworthiness of products and services, and a more safe and secure society will be achieved. In this way, trust-building technology will make a significant contribution to society.
The issuance of a certificate is supported by the generation and storage of digital evidence in the value creation process (VCP), as discussed in Report Two. The generation and storage of digital evidence of the process of creating products and services add momentum to the improvement of trustworthiness; and trust-building technology contributes to improving the overall trustworthiness within society. As aforementioned, trust requirements and certificates can be a tool for communication between supplying and acquiring organizations. However, for this to happen, the tool must be interoperable among different supply chains; otherwise, the related communication will not be effective. In supply chains, even a single order can involve multiple industries. Therefore, the abovementioned interoperability should be achieved across industries. In the following, then, we discuss the nature of such interoperability.

## 2. Framework for achieving interoperability of trust-building technology

As interoperability is the most important factor in trust requirements and certificates, we need a framework that encompasses these latter elements, and will refer to this as a trust-building framework in this report. This section provides an overview of the framework.

### 2.1. Trust-building framework

Before describing the trust-building framework, we review the trust-building technology described in Report Two.
Trust-building technology aims to ensure that the intended values of products and services will be provided, by creating a machine-readable model for a VCP, which is the process of creating a given product or service (henceforth, both products and services will be referred to as 'products', for simplicity), including relevant rules; verifying that the VCP is being properly conducted according to the VCP model; generating digital evidence; and finally generating a certificate. The focus is on verifying that the rules have been properly implemented when performing product creation.
There is no universal framework, extant or proposed, for verifying that rules have been implemented properly. However, if the subject is the product itself rather than the rules, we have the Common Criteria (CC), which is a framework for security evaluation and certification. The CC has a variety of tools for evaluating product

security; that is, there are a security functional requirement catalog and a security assurance requirement catalog, to ensure that security functions are properly implemented, and requirements are extracted from these catalogs to produce product requirement definitions (i.e., Security Targets (STs)). Since it may be difficult to compare the STs of different products, there is an available method to define common requirement definitions (i.e., Protection Profiles (PPs)) for each product field, enabling the creation of an ST in accordance with the PP. Products are evaluated and certified according to the ST and the common evaluation methodology (CEM), which is an evaluation methodology based on the CC, and then a certificate is issued. A product for which an ST has been created according to a PP will be clearly marked on the certificate, to indicate compliance with the PP. The trust-building framework makes reference to the CC system. It can be said that the trust-building framework is a result of replacing the security functions of the product being evaluated by the CC with the rules for the creation, etc., of the product.

### 2.2. Trustworthiness criteria

The trustworthiness criteria correspond to the CC. They are evaluation criteria to objectively evaluate and certify compliance with rules for trustworthiness in providing products and services. What the trustworthiness criteria should indicate is that the given organization's processes are in compliance with the rules. In light of the CC, the equivalent of functional requirements is rules, and the equivalent of assurance requirements is the means of showing compliance with the rules. Analogously to the CC, we refer to these requirements as trustworthiness functional requirements and trustworthiness assurance requirements, respectively. Trustworthiness assurance requirements specify how evidence should be configured, generated, and managed, and specify different levels according to the rigorousness of the assurance.

There is also a need for a trustworthiness evaluation methodology, to evaluate whether a product or service meets these requirements, as discussed below in Section 2.4.

### 2.3. Specific trustworthiness requirements

A specific trustworthiness requirement corresponds to an ST in the CC. Specific trustworthiness requirements are recorded in a document that defines a set of trustworthiness functional requirements, and a set of trustworthiness assurance requirements, for a given product or service, with regard to the processes of design,

procurement, manufacturing, test, delivery, operation, and maintenance, according to the conditions and environment of the supplying organization. As the name implies, specific trustworthiness requirements are a set of requirements defined for a specific product or service. Therefore, there are as many sets of specific trustworthiness requirements as there are products and services.
As stated above, the entirety of the trustworthiness functional requirements that a product or service must meet comprises a set of rules to realize the value of the product or service. Each item in the rules constitutes an individual set of trustworthiness functional requirements. The rules within an organization are not disclosed, because they are trade secrets stored in the organization. However, the trustworthiness functional requirements are to be shared, and thus are abstracted to the extent that they do not reveal trade secrets but nonetheless convey what must be done for trustworthiness.

### 2.4. Trustworthiness evaluation methodology

The trustworthiness evaluation methodology is equivalent to the CEM in the CC. It defines procedures for evaluating rule compliance and evaluation functions, and a framework for checking and auditing by a third party organization for the provision of products and services. This includes how to verify trustworthiness assurance requirements based on evidence.

### 2.5. Common trustworthiness requirements

A common trustworthiness requirement corresponds to a PP in the CC. These requirements encompass differences across products, industries, regions, and nations, and express trustworthiness criteria as a set of trustworthiness functional requirements, and a set of trustworthiness assurance requirements, that can be shared among different products, industries, regions, and nations. Based on the common trustworthiness requirements, specific trustworthiness requirements can be defined according to the given industry, product, and regional or national circumstances.
The figure below shows how the trustworthiness criteria, etc., in the abovementioned trust-building framework, are related to trust requirements and certificates.

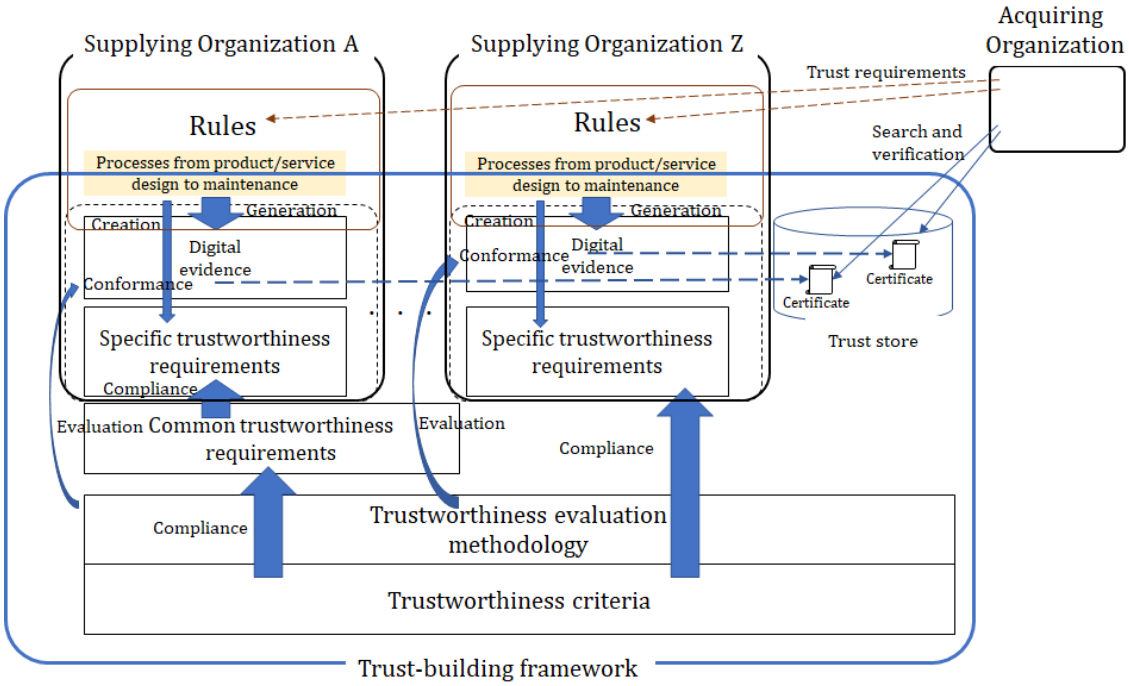


Figure 2 Overview of the trust-building framework

Products and services with specific trustworthiness requirements derived from the same common trustworthiness requirements can be considered equally reliable, because they share a common set of trustworthiness functional requirements and a common set of trustworthiness assurance requirements; that is, they share the same rule-compliance requirements.

A PP in the CC is a profile created for each product field, such as IC (integrated circuit) cards and firewalls. Different product fields will require different PPs because PPs include requirements for product security functions. In contrast, common trustworthiness requirements are a set of requirements for compliance with rules. Common trustworthiness requirements may be applicable across industries, because there is typically commonality in organizations' manufacturing and other rules, even if the product fields differ. In other words, common trustworthiness requirements can have a broader field of application than the PPs in the CC.

In the same way that a PP in the CC is developed by an industry association, common trustworthiness requirements will be developed by an industry association that is familiar with the production of products and services in the relevant field. As noted above, common trustworthiness requirements created in

one industry can be expected to be reused across different fields of products and services; and new common trustworthiness requirements created in this way may increase the scope of reuse. Additional common trustworthiness requirements may be created outside the scope of reuse (Figure 3).

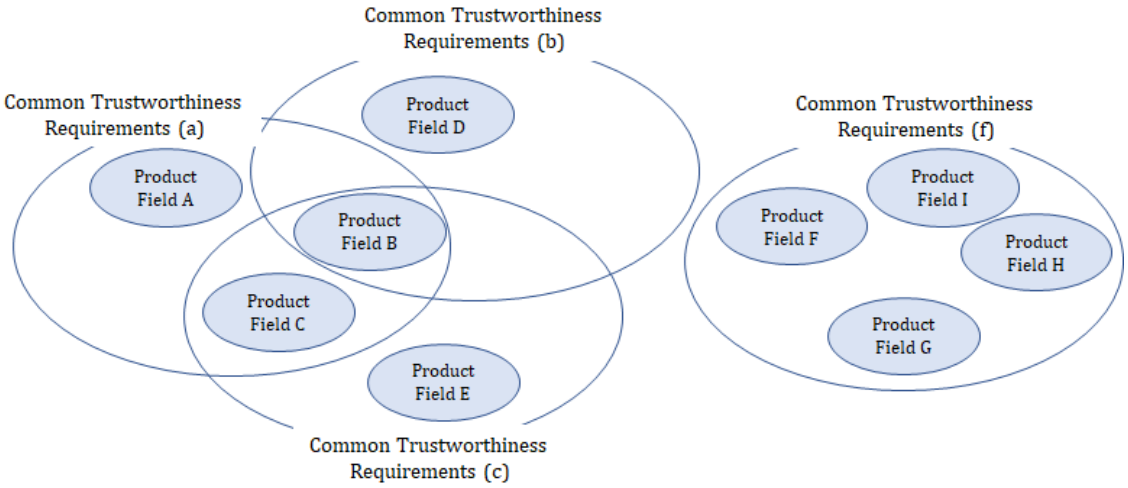


Figure 3 Schematic diagram showing the relationship between product fields and common trustworthiness requirements

## 2.6. Standardization of trustworthiness criteria

As noted above, trustworthiness functional requirements are elements of rules that are abstracted such that they do not reveal trade secrets. Specific trustworthiness requirements can be created by combining trustworthiness functional requirements, which are abstracted elements of rules.

With the abstraction of rules, specific trustworthiness requirements may be reused in other organizations and business areas; and in this case, specific trustworthiness requirements can also be considered as common trustworthiness requirements. Once common trustworthiness requirements are created in this way, new common trustworthiness requirements may be derived from them.

Once the abstracted trustworthiness functional requirements have been combined, they will constitute the Trustworthiness Criteria Part 2, which is a trustworthiness functional requirement catalog, as in the case of the CC Part 2. The rules depend on the given business sector, but their dependence is not as profound as the dependence of product and service functions on the business sector.

Trustworthiness Criteria Part 2 will be created for each business sector or business

sector group, and then will be combined and abstracted to form the final Trustworthiness Criteria Part 2, which will be independent of the respective business sectors.
Trustworthiness functional requirements are abstracted rules forming part of specific trustworthiness requirements. Among other things, the trustworthiness assurance requirements are a means of indicating whether the abstracted rules are being followed, and the content of the related digital evidence, as well as the certificate, will be determined based on the rigorousness of these requirements. This rigorousness will be more useful if its level is classified in a way similar to the Evaluation Assurance Level (EAL) of the CC. These elements will be systematically combined to form the Trustworthiness Criteria Part 3, which, like the CC Part 3, will be a trustworthiness assurance requirement catalog.

3. Standardization of trust requirements

The common trustworthiness requirements consist of a set of trustworthiness functional requirements and a set of trustworthiness assurance requirements, in other words a set of rule-compliance requirements, for a given product or service field. In addition, as noted in Section 2.5, they may be applicable across industries, and are thus provided as a document understandable not only to supplying organizations but also to acquiring organizations. Therefore, they are appropriate for use in ordering products and services, and for specifying the relevant trust requirements.
When using the common trustworthiness requirements for trust requirements, it is not necessary to present the former as a document each time. Since they are promulgated in advance, it is sufficient to provide an identifier for them, and simply present this identifier when necessary. We have already mentioned that the development of common trustworthiness requirements (i.e., standardization) should be done by industry associations. The same is true for the standardization of identifiers for the common trustworthiness requirements. Although any form of identifier is acceptable as long as it is machine-readable, it should be ensured that conflicts will not occur if and when the use of such identifiers becomes widespread. To this end, a registration authority is needed, to ensure the uniqueness of each identifier. International standardization may also be necessary, along with these identifiers.
As discussed in Report Two, trust requirements are requirements at the time of ordering, including requirements related to trust as well as functions. For trust-related requirements, common trustworthiness requirements and their

identifiers can be standardized, as described above. Although basically beyond the scope of this report, other requirements, such as functional requirements, are also discussed briefly below.

Trust requirements are exchanged between supplying and acquiring organizations. In many cases, a given organization deals with more than one acquiring organization and more than one supplying organization; and the relationship between product acquirers and suppliers is typically a many-to-many relationship. If all the trust requirements have different forms, supplying organizations will need as many ways of handling them as there are acquiring organizations, resulting in a huge burden on both supplying and acquiring organizations. As much as possible, then, trust requirement forms should be common across the industries involved.

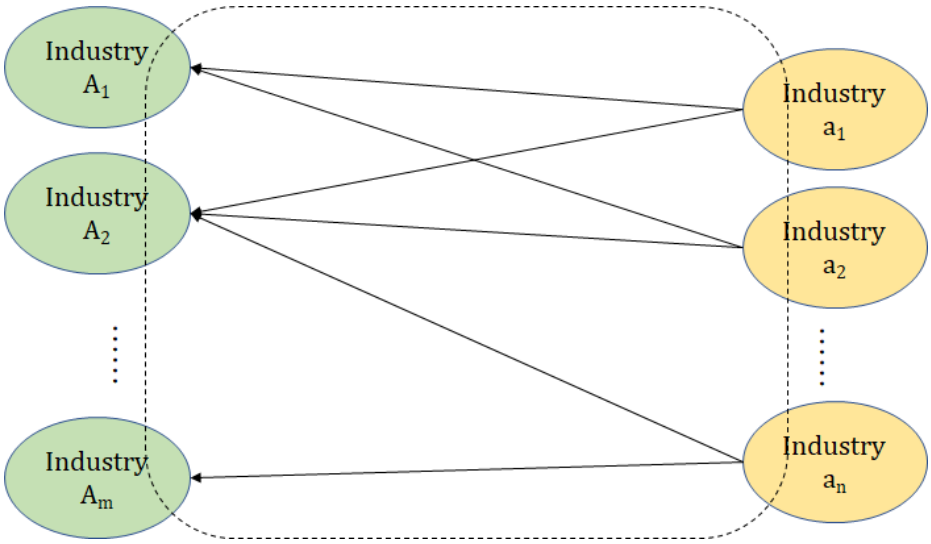


Figure 4 Cross-industry transfer of trust requirements

The two arrows emerging from Industry $a_1$ in Figure 4 indicate that acquiring organizations in Industry $a_1$ place orders with organizations in Industries $A_1$ and $A_2$. In this case, the trust requirement format should be common for Industries $a_1$, $A_1$, and $A_2$. Given that the industries connected by arrows are similar to each other, trust requirements are exchanged between Industries $A_1$/$A_2$ and industry $a_2$, between Industry $A_2$ and Industry $a_n$, and between Industry $a_n$ and Industry $A_m$; and the form of the respective trust requirements should be common between the relevant industries. Identifying relevant industries in this way will determine the range of industries that should have a common form of trust requirements.

An organization in industry $A_1$ may, however, itself become an acquiring

organization, if it orders a product as a component in the creation of the product ordered by an organization in industry $a_1$. Similarly to the creation of Figure 4 above, we would then obtain a diagram similar to Figure 4 but with Industry $A_1$ on the *right* side; which would, in turn, determine a range of industries that should share a different form of trust requirements than in Figure 4. However, if Industry $A_1$ appeared on *both* sides in Figure 4, we would obtain the same diagram as in Figure 4, not a new one. If we apply the above operation to all the supply chains in which relevant industries participate, we can determine forms of trust requirements that should be made common (Figure 5). There is no need to consider other supply chains that have not appeared in the previous operations, because such additional supply chains do not involve order-and-supply relationships with the organizations relevant to the supply chains that appeared in those previous operations.

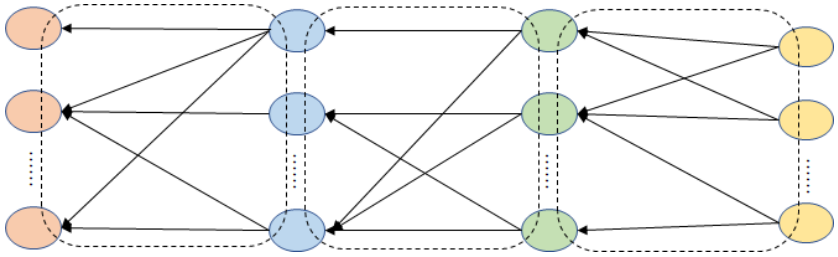

Figure 5 Development of common trust requirement formats in relevant supply chains

4. Standardization of certificates

A certificate consists of data paired with a set of trust requirements. Thus, the scope of industries subject to standardization is similar to that in the case of trust requirements. Downstream organizations may refer to upstream certificates in addition to the certificates they receive. In light of this, it is desirable that the format of certificates be common across the industries that appear in Figure 5.

5. Standardization of digital evidence

As stated in Report Two of this White Paper, digital evidence is not, in principle, to be disclosed to third parties. This fact may imply that the format of such evidence could be unique to each organization. Such uniqueness, however, would not be desirable. Report Two of this White Paper states: "However, if a dispute, etc. arises due to an incident involving trust, it is anticipated that the digital evidence would be disclosed in accordance with the request of a third party such as an appropriate

institution, etc., and used as evidence of the conformity of the executed business." Therefore, it is desirable, if not essential, that at least part of the digital evidence should be common across the industries involved. Although much remains to be done before it is achieved, we will now consider an ideal form of commonality in digital evidence.

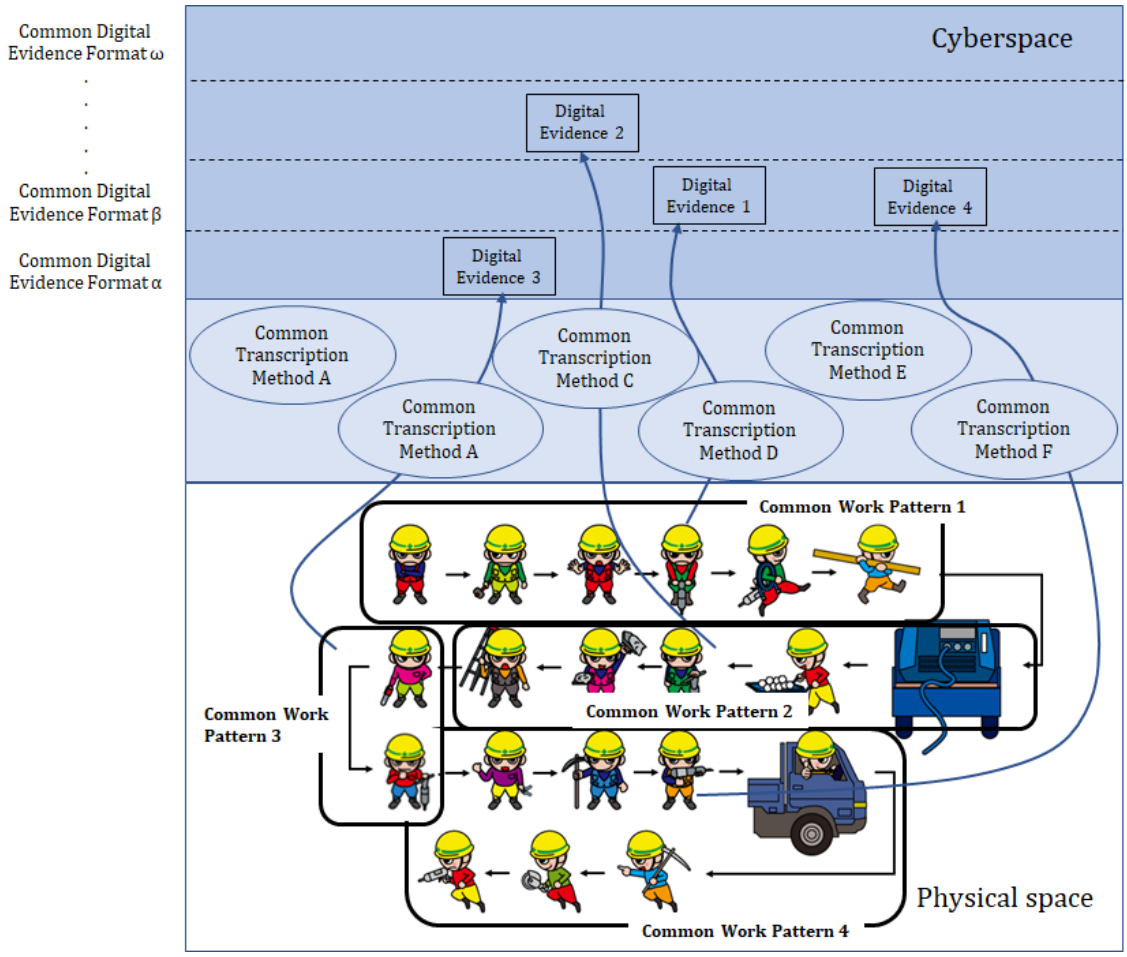


Figure 6 Commonized pattern of trust-building (conceptual diagram)

Given the commonality of digital evidence, it is desirable that the collection of work from which digital evidence is derived, the transcription method from the collection of work to the digital evidence (e.g., how image data is acquired by surveillance cameras), and the format of the digital evidence, be common across organizations. This is exemplified by the common work patterns, common transcription methodologies, and common digital evidence formats in Figure 6. For these things

to be common across organizations, they must first be common within each organization. Just as common trustworthiness requirements are based on specific trustworthiness requirements, commonality across organizations will be based on commonality within the respective organizations.
For Common Work Pattern 1 in Figure 6, digital evidence is stored in Common Digital Evidence Format β using Common Transcription Method D. For Common Work Pattern 4, digital evidence is stored in Common Digital Evidence Format β using Common Transcription Method F. If the content of work is different, there may be additional data to store; in which case, Common Work Pattern 1 and Common Work Pattern 4 can each store additional digital evidence by each defining an extension area in Common Digital Evidence Format β, as shown in Figure 7.

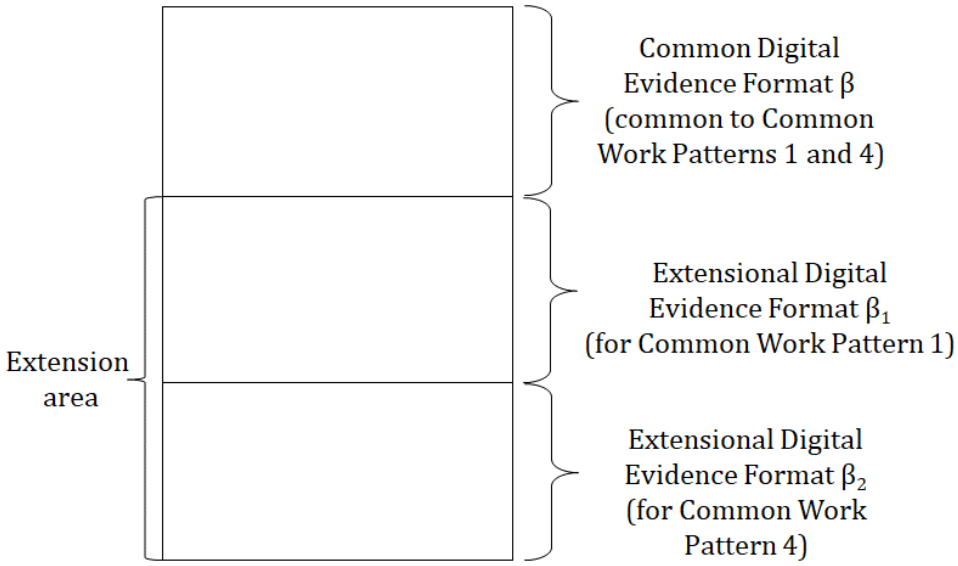


Figure 7 Common digital evidence format extension area (example)

We have thus far discussed the commonality of formats for trust requirements, certificates, and digital evidence. The scope of industries where it is desirable to have common trust requirements and certificates is described in Section 3. In the case of digital evidence, it is, in principle, appropriate to achieve commonality within a given industry. However, in the case of digital evidence referenced in certificates, it is desirable to achieve commonality among all the industries to which the acquiring organizations belong. Whether it is trust requirements, certificates, or digital evidence, there will be data items that are common across industries, and items that are industry-specific. It is important to classify and define these items for

interoperability, as shown in Figure 8.


Figure 8 Differentiation of cross-industry common data items, and industry-specific data items, of trust requirements, certificates, and digital evidence

## 6. International standardization

As discussed above, data format commonality will be difficult to achieve unless industries make the necessary effort. Industry associations must work toward common data formats; and given the global nature of supply chains, international industry associations, rather than the industry associations of individual countries, should spearhead this effort. Whether it is trust requirements, certificates, or digital evidence, it is necessary to discuss common data formats across industry associations. It may be difficult, however, for industry associations to address such a matter, and therefore international standardization organizations such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) may need to discuss the issue. The same is true for the trustworthiness criteria described in Section 2.

The widespread use of trust-building technology will increase the amount of relevant data. However, though the evolution of IT has made it possible to accumulate vast amounts of data, the growth in the amount of data should still be controlled. The increase in the amount digital evidence data, for example, should be controlled. While trust requirements may not need to be preserved, certificates and digital evidence will be preserved. These latter, however, will not be stored uniformly, but rather according to the extent to which they meet the trustworthiness assurance requirements; thus, for example, if trustworthiness assurance requirements are not rigorously met, the data size of certificates and digital evidence will be reduced.

A protocol would be defined in which, for trust requirements, digital evidence in a common digital evidence format is generated from each common work pattern by a common transcription method, and a certificate is returned as a result. The international standardization of this protocol will enable the establishment of

trust-building technology that meets diverse needs, and in turn enables trust to be promoted by society as a whole.

## 7. Acknowledgment

This research is partly supported by the Cross-Ministerial Strategic Innovation Promotion Program (SIP) "Cyber-Physical Security for an IoT Society," led by the Cabinet Office of the Government of Japan and managed by the New Energy and Industrial Technology Development Organization (NEDO).

## References

[1] National Institute of Advanced Industrial Science and Technology. "Building Trust in Supply Chains, Report One: Analysis of Incidents that Damage Trust and Basic Approach to Trust-building," October 2019, https://www.cpsec.aist.go.jp/achievements/Building%20Trust%20in%20Supply%20Chains%20One[1291].pdf

[2] National Institute of Advanced Industrial Science and Technology. "Building Trust in Supply Chains, Report Two: Trust-building Technology," January 2020, https://www.cpsec.aist.go.jp/achievements/Building%20Trust%20in%20Supply%20Chains%20Two[1292].pdf