仮訳
Provisional Translation

# Guidelines on e-Seal

## (Second Edition)

**April 2024**

## Ministry of Internal Affairs and Communications

# Table of Contents

## Purpose of This Guidelines

This Guidelines aim to provide technical and operational standards that should be referenced by certification authorities and other parties engaged in providing certification business for e-Seal by presenting the ideal state for e-Seal certification business[1] in Japan.

## Background to the Formulation of This Guidelines

There is a significant increase in the volume of data flowing on Japan's networks due to improvements in communications infrastructure and the spread and diversification of digital services. Especially, real space and cyberspace are highly integrated in Society 5.0, and various paper- and face-to-face-based exchanges that take place in real space must be easily realized electronically in cyberspace as well.

In this context, a foundation that allows the safe and secure distribution of electronic data is indispensable, and trust services, a mechanism that prevents falsification of electronic data, impersonation of the sender, etc., are expected to be utilized. Above all, as the volume of electronic data issued by companies is increasing, using "e-Seal" to verify the issuer of electronic data from companies, etc., is expected to improve operational efficiency and productivity.

The government's "Priority Policy Program for Realizing Digital Society," approved by the Cabinet on June 9, 2023, states that "To foster economic growth and address societal challenges through data utilization, securing trust that underpins the integrity of data distribution infrastructure is important, and the need for such trust is becoming even greater with the advancement of digitalization." and "In the future, an anticipated escalation in the demand for verification of issuers in online transactions and processes is expected. Therefore, we will also work on developing standards for evaluating the reliability of private e-Seal services and realize conformity assessment." The program stipulates the importance of trust services, including e-Seal, toward the advent of Society 5.0 and the realization of DFFT (Data Free Flow with Trust), advocated by Japan.

In June 2021, the Ministry of Internal Affairs and Communications (MIC) formulated the "Guidelines on e-Seal" (Formulated by MIC on June 25, 2021. Hereinafter referred to as "Previous Guidelines"), which prescribed certain technical and operational standards for e-Seal, following discussions at the "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations," which began in April 2020. From the viewpoint of promoting the further spread and utilization of e-Seal, a "Study Group on e-Seal" has been held since September 2023. The study group concluded that it would be appropriate for the Minister for

[1] Refers to the operations of certifying organizations that generate e-Seal. The same shall apply hereinafter.

Internal Affairs and Communications to establish a certification system for e-Seal and decided to revise the previous Guidelines following the establishment of this certification system.

## Application of this Guidelines and Previous Guidelines

The previous Guidelines shall apply until the commencement of operation of the certification system for e-Seal, and this Guidelines shall apply after the commencement of operations.

# Chapter 1　What is an e-Seal?

## 1.1 Definition of an e-Seal

An e-Seal is used to verify the issuer of electronic data from companies, etc., and to prove that the electronic data has not been falsified (hereinafter referred to as “Ensuring trust”). This makes it possible to check for impersonation of the issuer or falsification of electronic data and is expected to be effective in preventing these issues.

The definition of e-Seal in Japan is as follows.

The term “e-Seal” means electronic data that is assigned to or logically associated with information recorded in an electromagnetic record (a record of information made by an electronic, magnetic, or any other method not recognizable by human perception, used for information processing by a computer. The same shall apply hereinafter), and that meets the following requirements.

(i) Indicates the source or origin of the relevant information;

(ii) Can verify whether the relevant information has been altered.

## 1.2 Differences Between e-Seal and Electronic Signatures

Both e-Seal and electronic signatures are the same as they are used to verify that there has been no falsification of the relevant electronic document after encryption or other measures have been implemented. The difference lies in the fact that an e-Sealerves to verify the issuer of electronic data, and an electronic signature serves to prove that the principal created the electronic document and that the relevant principal declared intent in the electronic document. The definition[2] of an electronic signature is stipulated in the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000. Hereinafter referred to as “Electronic Signatures Act”). It assumes that only a natural person may declare intent and only a natural person may issue an electronic signature.

Since an electronic signature is proof of the signatory’s declaration of intent, it is used, for example, in electronic contracts, electronic applications, and other purposes that require the signatory’s declaration of intent as a natural person. On the other hand, an e-Seal only serves

---

[2] Act on Electronic Signatures and Certification Business (Act No. 102 of 2000)

Article 2(1)The term "electronic signature" as used in this Act means a measure taken with respect to information that can be recorded in an electronic or magnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers; hereinafter the same applies in this Act), and which falls under both of the following requirements:

(i) a measure to indicate that the relevant information was created by the person who has taken that measure; and

(ii)a measure to confirm whether the relevant information has been altered.

as a proof of issuer and is expected to be used, for example, in electronic documents issued by organizations, etc., that do not require the declaration of intent as a natural person, such as invoices, receipts, quotations, and various other certificates.

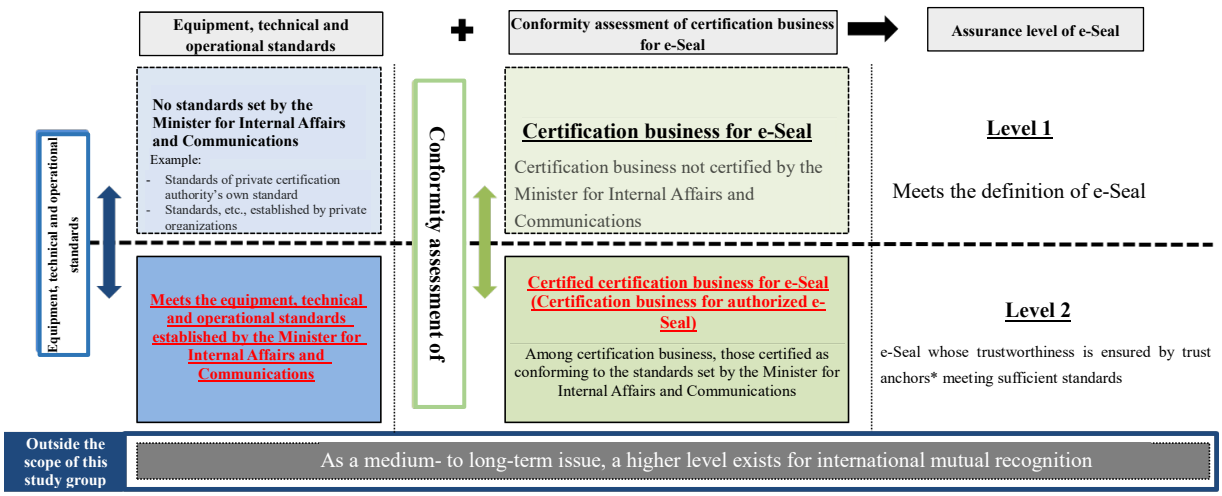
Therefore, unlike electronic signatures, which are strongly associated with the natural person who is the user due to their role as a declaration of intent, e-Seal, which are associated with the organization, etc., that issue them, have the advantage of doing away with the requirement of reissuing electronic certificates for e-Seal when personnel changes occur within the organization. Because no declaration of intent is involved, e-Seal can be assigned mechanically and automatically to a large number of electronic documents. It should be noted, however, that the intention of the natural person who assigned the e-Seal is not expressed in the electronic documents bearing the e-Seal.

As mentioned above, it is important for users to fully understand the difference between an e-Seal and an electronic signature and to use them appropriately for the intended purposes.

## 1.3 Assurance level of e-Seal

The assurance level of e-Seal is divided into 2 levels, depending on their use: (1) Assurance level expected for e-Seal issued in large numbers at lower cost and with simpler procedures, although not guaranteed by certification business for e-Seal (hereinafter referred to as "Certification business for authorized e-Seal) certified by the Minister for Internal Affairs and Communications, and (2) Assurance level that is guaranteed by certification business for authorized e-Seal, providing a high degree of confidence concerning the source and non-alteration of the electronic data bearing the e-Seal.

Fig. 1 focuses on how the certification system of the Minister for Internal Affairs and Communications is organized and does not preclude other voluntary efforts by private organizations to ensure the trustworthiness of certification business for e-Seal by certification authorities.




* Reference point for electronic certification procedures conducted over the Internet, etc. In this Guidelines, a certification authority is assumed to be the reference point for trustworthiness.

**Fig. 1 Assurance level of e-Seal**

## 1.4 Use cases of e-Seal

Using e-Seal makes it possible to verify the issuing organization, etc., easily and to check whether electronic documents have been falsified, previously performed manually on paper. Documents can now be exchanged between businesses electronically and securely, and they can also be processed mechanically and automatically, which is expected to improve operational efficiency and productivity. e-Seal are also expected to eliminate the cost of paper storage and the risk of paper loss incurred until now.

Areas where e-Seal are expected to be used include interactions between businesses, information published by organizations, certificates issued by organizations, communication between the public and private sectors, and audits. Different e-Seal with different assurance levels may be used in each area, depending on the degree of reliability required by the electronic documents, which will bear the e-Seal. For example, the relationship between the assurance level of e-Seal shown in the previous section and each use case is shown in Fig. 2.

However, this is just an example, and organizations, etc., that assign e-Seal should consider using e-Seal of different assurance levels depending on the magnitude of damage in the event of damage to the electronic data, the reliability required and importance of the electronic data, the situation in which an e-Seal is to be used, and user requirements. In addition, this may change in the future with revisions to various laws, regulations, and systems.

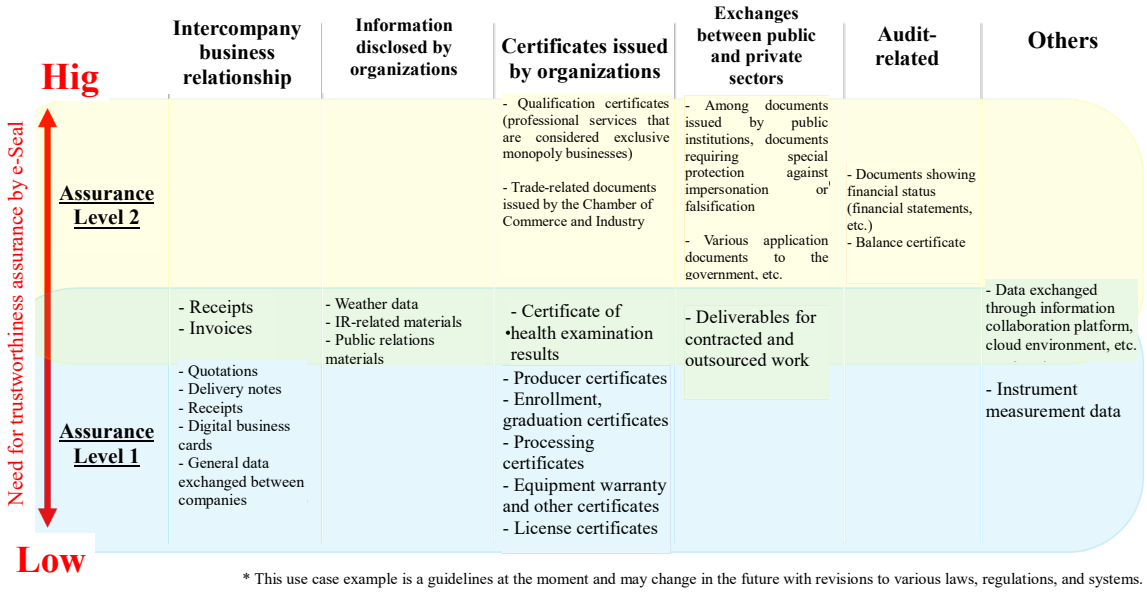



**Fig. 2 Image of the relationship between the assurance level of e-Seal and each use case**

Some specific examples of use cases where e-Seal are expected to be used are given below. Of course, applications of e-Seal are not limited to these.

### 1.4.1 Expected Use Cases for e-Seal with Assurance Level 2

(1) Certificates issued by organizations (e.g., qualification certificates for professional services that are considered exclusive monopoly services)

Since qualification certificates for professional services that are considered exclusive monopoly services must have a high degree of reliability in terms of ensuring trust, it is preferable to utilize e-Seal with "Assurance Level 2," which are guaranteed by certification business for authorized e-Seal and provide a high degree of confidence concerning the source and non-alteration of the electronic data bearing the e-Seal.

In such cases, as shown in Fig. 3, electronic qualification certificates bearing an e-Seal can be automatically verified to have not been falsified and are expected to promote digitalization, such as completing the application and issuing such qualification certificates digitally.

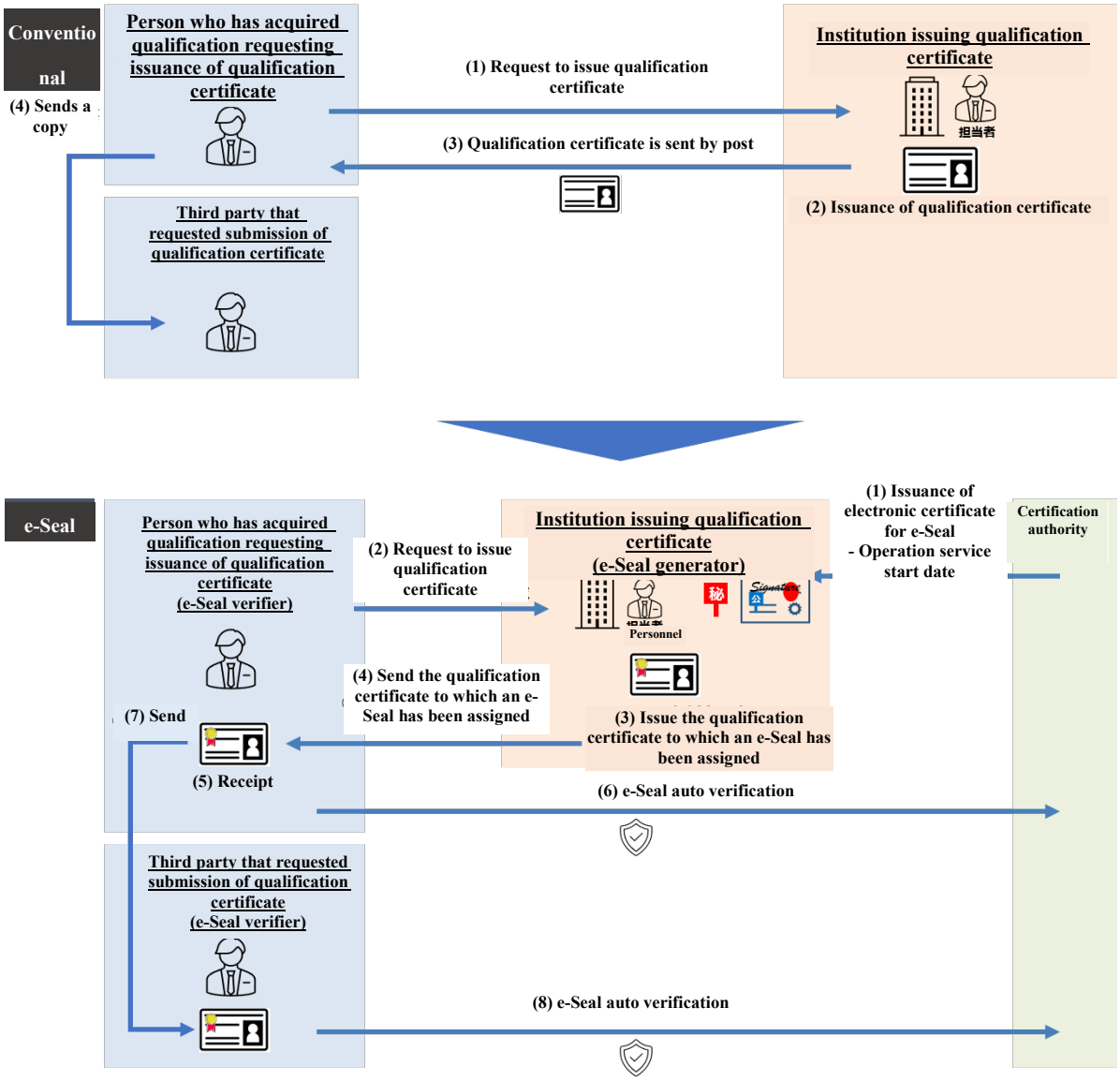



**Fig. 3 Image showing the use of e-Seal (Qualification certificate)**

(2) Communication between the public and private sectors (Among documents issued by public institutions, documents requiring special protection against impersonation or falsification)

In the communication between the public and private sectors, documents issued by public institutions, especially those that need to be protected against impersonation or falsification, must have a high degree of reliability concerning ensuring trust.

In such cases, it is preferable to utilize e-Seal with "Assurance level 2," which are guaranteed by certification business for authorized e-Seal and provide a high degree of confidence concerning the source and non-alteration of the electronic data bearing the e-Seal.

(3) Audits (financial statements and other materials that serve as audit evidence)

The financial statements and other materials that serve as evidence in financial audits are important materials for the stakeholders of a company to judge its business situation, and to determine whether a company is suitable as a partner for investment or trade.

Therefore, digitalizing such materials must have a high reliability to ensure trust. In such cases, it is preferable to utilize e-Seal with "Assurance level 2," which is guaranteed by certification business for authorized e-Seal and provides a high degree of confidence concerning the source and non-alteration of the electronic data bearing the e-Seal.

### 1.4.2 Expected Use Cases for e-Seal with Assurance Level 1

(1) Certificates issued by organizations (e.g., electronic warranties for electrical appliances)

As described in Section 1.4.1, qualification certificates for professional services considered exclusive monopoly services require a high degree of reliability to ensure trust. However, for the various certificates issued by an organization on a routine basis, using e-Seal with assurance level 1, which are expected to be issued in large numbers at lower cost and with simpler procedures, is considered sufficient.

An example of this is electronic warranties for electrical appliances. While some electronics retail stores already provide electronic warranties, using e-Seal is expected to improve user satisfaction from the perspective of preventing counterfeiting warranties, such as falsifying the purchase date of electrical appliances.

(2) Interactions between businesses (e.g., data exchanged between companies on a routine basis)

Data, etc., exchanged between companies on a routine basis may often use e-Seal with assurance level 1, which are expected to be issued in large numbers at lower cost and with simpler procedures.

Examples of actual use of e-Seal in Japan include the use of e-Seal for construction-related documents[3] and support work reports shown in Fig. 4. In Fig. 4, support work reports, which were previously created and shared on paper, are now digitized and assigned an e-Seal. In addition to quantitative effects, such as reducing the cost of discarding paper materials and lowering paper storage costs, qualitative effects, such as improved customer satisfaction and data reliability, have also been confirmed. Although this case study focused on support work reports, quantitative and qualitative effects can also be expected for data exchanges between companies on a routine basis.

[3] The case study analysis of the "Study group on e-Seal" considered the use of e-Seal with Assurance Level 2 with respect to various construction-related documents submitted for public works.

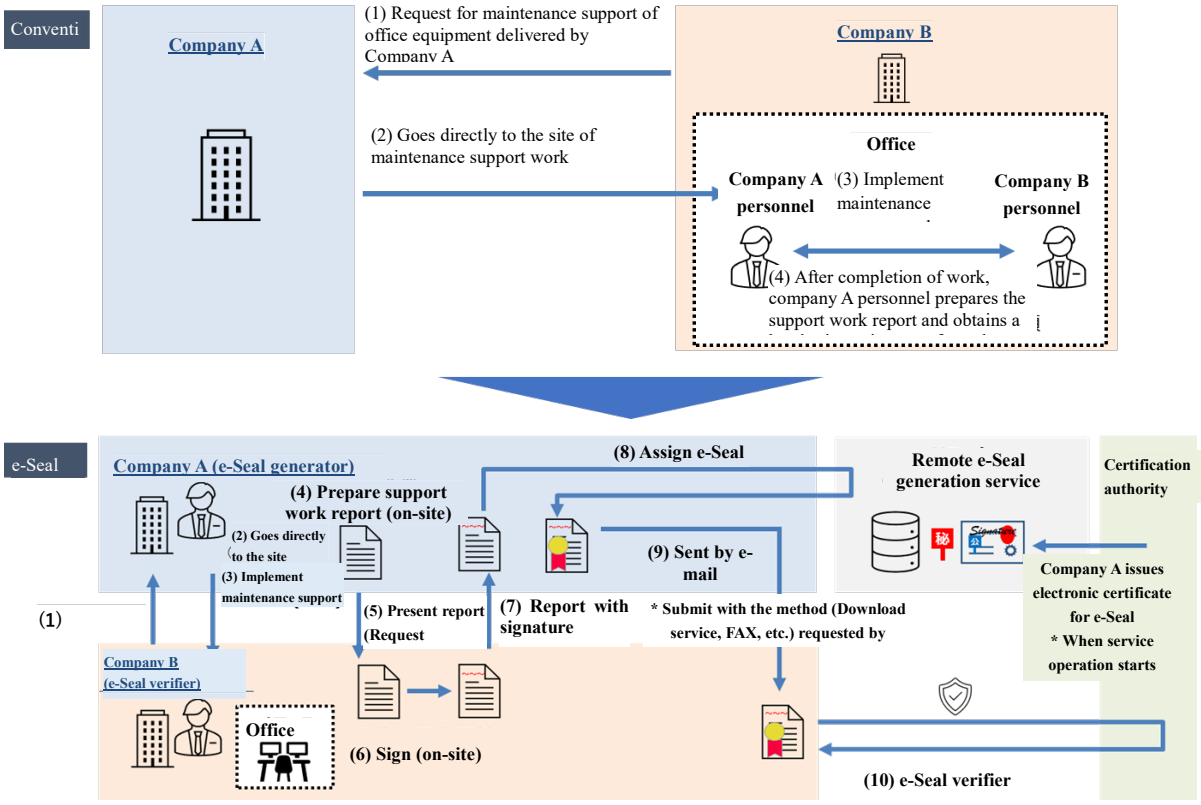



**Fig. 4 Image showing the use of e-Seal (Support work report)**

(3) Information disclosed by organizations (PR materials, etc.)

Considering the possibility of falsifying PR materials posted on a company's website when such materials are distributed to a third party, e-Seal may be considered to ensure trust.

In such cases, PR material routinely disclosed by companies does not necessarily need to be guaranteed by certification business for authorized e-Seal. In many cases, using e-Seal with assurance level 1, which are expected to be issued in large numbers at lower cost and with simpler procedures, is considered sufficient.

## 1.5 Mechanism for Ensuring Trust Using e-Seal

Fig. 5 shows an example of a mechanism for ensuring trust using e-Seal. This example uses public key infrastructure (PKI). When a certification authority that issues electronic certificates for e-Seal generates a key pair, it sends media containing the electronic certificate for the e-Seal and private key issued by the certification authority (hereinafter referred to as "Storage media") to the e-Seal generator, which uses the storage media to issue an e-Seal to the electronic data. The e-Seal generator sends the electronic data bearing the e-Seal to the recipient (e-Seal verifier), who verifies that the electronic certificate for the e-Seal has not been revoked and that the electronic data has not been falsified, thereby ensuring trust of the electronic data.

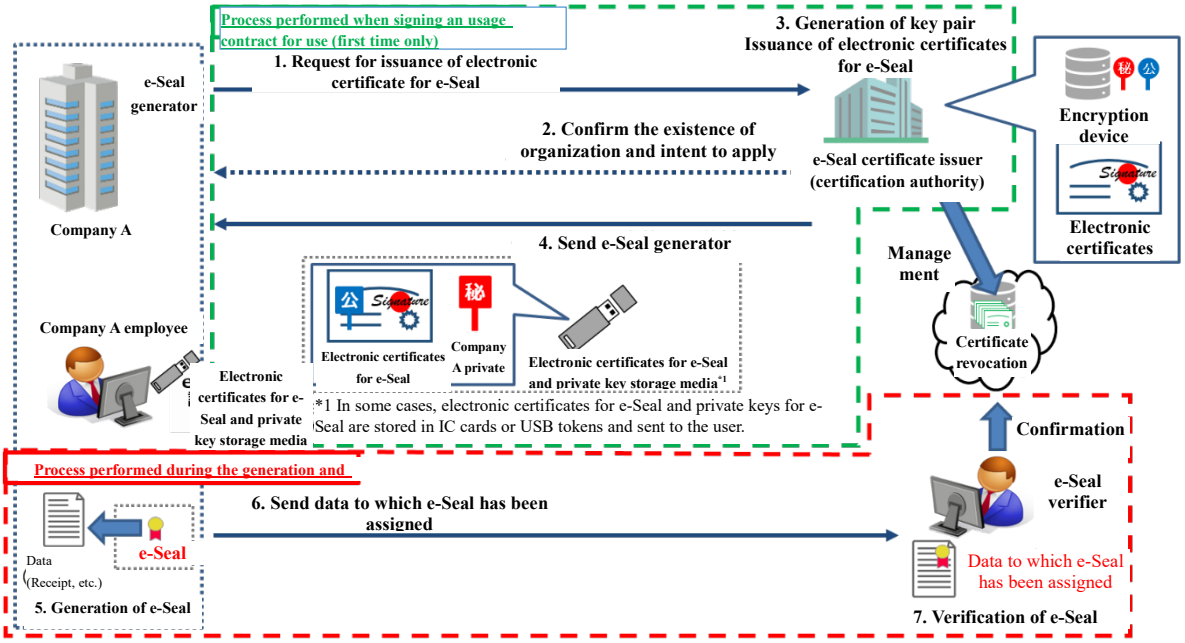



**Fig. 5 Example of the e-Seal mechanism using PKI**

While this guidelines illustrates a method using PKI, various methods may emerge as technology progresses, and they should not be excluded from the viewpoint of technology neutrality.

## 1.6 e-Seal Generation Methods (Local e-Seal Method/Remote e-Seal Method)

There are two main e-Seal generation methods, depending on the environment in which the e-Seal generator's private key is stored: the local e-Seal generation method, in which the private key is stored and issued locally (hereinafter referred to as "Local e-Seal method"), and the remote e-Seal generation method, in which the private key is stored and issued remotely (hereinafter referred to as "Remote e-Seal method"). A brief introduction to each method is given below.

### 1.6.1 Local e-Seal Method

In the local e-Seal method, the private key is stored in an environment under the management of the e-Seal generator, and the e-Seal is generated in this environment. This method is further divided into several more patterns depending on where the key pair (private and public keys) is generated. For example, assume a pattern in which the certification authority generates the e-Seal generator's key pair and the relevant public key, then sends the electronic certificate for e-Seal issued for the private and public keys to the e-Seal generator (Fig. 6) or a pattern in which the e-Seal generator generates its key pair, following which the certification authority sends the electronic certificate for the e-Seal issued for the relevant public key to the e-Seal generator.

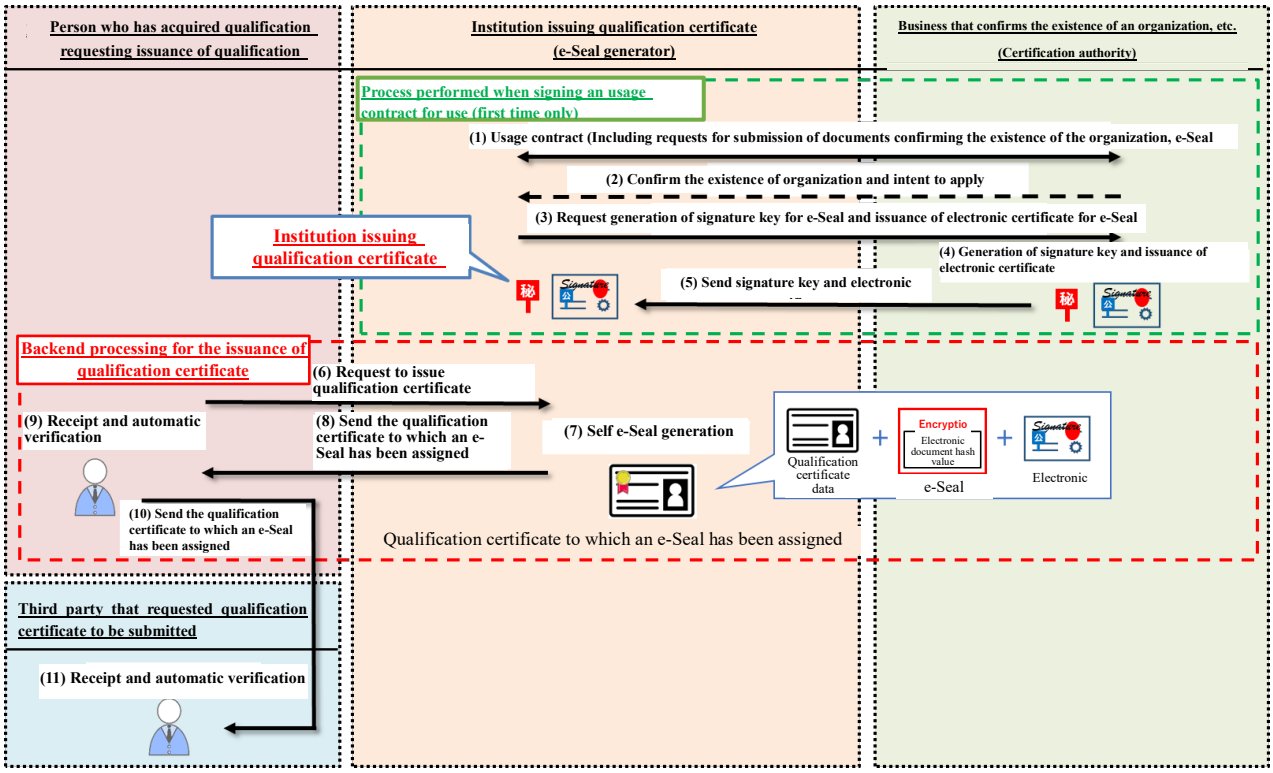



**Fig. 6 Example of local e-Seal method (Example of assigning an e-Seal for qualification certificate data)**

### 1.6.2 Remote e-Seal Method

In the remote e-Seal method, the e-Seal generator delegates the management of the private key to a remote environment, such as the cloud, and the e-Seal is generated by accessing the remote environment. For example, assume that an e-Seal generator delegates the management of the private key to a cloud managed by a business operator providing remote e-Seal services (hereinafter referred to as "Remote e-Sealervice provider"), then accesses the cloud to generate the e-Seal in a remote environment.

An example of the remote e-Seal method is shown in Fig. 7. In the remote e-Seal method, a remote e-Sealervice provider manages the e-Seal generator's private key in the cloud and generates the e-Seal based on the e-Seal generator's instructions. Note that, as shown in this case study, a business operator providing an application that utilizes e-Seal (hereinafter referred to as "Application provider") may provide a service that mechanically and automatically issues an e-Seal to electronic data by linking its services with a certification authority or a remote e-Sealervice provider.

Since the remote e-Seal method has many commonalities with remote signatures[4], the

[4] A method with which signatories access their private key in a remote environment, such as the cloud, to assign electronic signature.

"Remote Signature Guidelines[5]" for electronic signatures may be used as a reference for the general security measures and specific methods required for the remote e-Seal method.

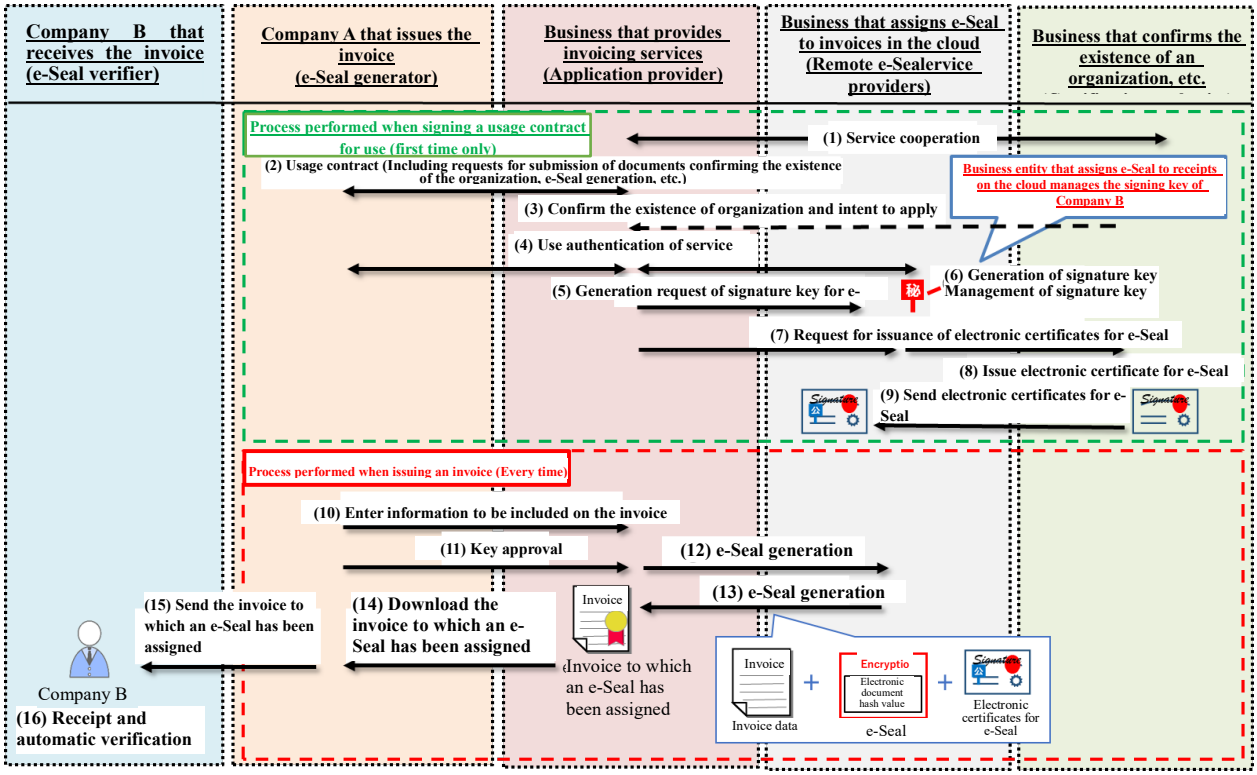



**Fig. 7 Example of remote e-Seal method (Example of assigning an e-Seal for invoice data)**

[5] Guidelines that provide technical standards for remote signatures, created by the Japan Trust Technology Association (JT2A).
https://www.jnsa.org/result/jt2a/data/RemoteSignatureGguide_All-r1.pdf

# Chapter 2 Ideal Status of Certification Business for e-Seal in Japan

Considering the definitions and characteristics of e-Seal, the items addressed in this Guidelines are as follows. However, note that this Guidelines are not an exhaustive list of items required for e-Seal but only focus on the specific items required for certification business for authorized e-Seal, concerning the Electronic Signatures Act, the certification system for timestamps, etc., and based on the premise that PKI is used.

- Scope of Organizations to Which Electronic Certificates for e-Seal are Issued
- Method of Confirming the Existence and Application Intention of the e-Seal Generator
- Format and Matters to be Specified in Electronic Certificates for e-Seal
- Standards for Management of Private Keys of Certification Authorities
- Standards for Management of Private Keys of e-Seal Generators
- Process When Generating a Large Number of e-Seal
- Use Authentication with the Remote e-Seal Method
- Revocation Request of Electronic Certificates for e-Seal

## 2.1 Scope of Organizations to Which Electronic Certificates for e-Seal are Issued

To identify organizations, etc., to which electronic certificates for e-Seal are issued, i.e., e-Seal generators, identifiers that uniquely identify such organizations are necessary. However, the scope of organizations to which electronic certificates for e-Seal are issued depends on the extent of organizations to which organization identifiers are issued.

Identifiers used for electronic certificates for e-Seal of the certification business for authorized e-Seal with assurance level 2 are a combination of an internationally used prefix[6, 7] and an existing number issued by a public institution. For corporates, etc., the prefix "NTRJP" is combined with the existing "Corporate Number" to configure the organization identifier[8, 9]. Furthermore, for electronic certificates for e-Seal of the certification business for authorized e-Seal, although it is a requirement to include an organization identifier that uses the Corporate Number, an additional organization identifier that uses a private company code may be included, as described below.

---

[6] CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates Version 1.0.1, August 11, 2023

[7] ETSI, ETSI TS 119 412-1 V1.3.11, 2019-08

[8] When government agencies or local governments use an e-Seal for certification, a combination of the prefix "GOVJP" and the "Corporate Number" may be used.

[9] The Qualified Invoicing Business Registration Number described in the Priority Policy Program were considered as a candidate for the "Sole proprietor number system"; however, the issue was set aside for further consideration since there is no reliable method to distinguish sole proprietors with the same name based on the information posted on public websites.

Regarding electronic certificates for e-Seal of the certification business for e-Seal with assurance level 1, only the numbers provided by private companies may be used. Furthermore, as with electronic certificates for e-Seal concerning the certification business for authorized e-Seal, multiple numbering systems may be used. In such cases, regarding international interoperability, using "●●:JP" (where "●●" is the identifier prefix)[10] is recommended[11].

Although there are certain requirements for business offices, sales offices, branch offices, or departments within an organization or for persons in charge of an organization (individuals with no declared intent) to which/whom electronic certificates for e-Seal are issued, both assurance level 1 and assurance level 2 of electronic certificates for e-Seal can be listed in the extended area, which is an optional field of electronic certificates for e-Seal, since it is difficult for a certification authority to confirm their existence accurately. The method of their verification and description is described in Section 2.3[12].

Based on the above, the organization identifiers to be stored in electronic certificates for e-Seal of the certification business for authorized e-Seal with assurance level 2 are arranged according to Fig. 8. It is recommended to use one of the organization identifiers shown in Fig. 9 for electronic certificates for e-Seal of the certification business for authorized e-Seal with assurance level 1.

**Legend◎: All items are numbered (complete coverage) ○: Basically, numbering is possible △: Some items are numbered -: Out of scope**

| Organization identifiers used for electronic certificates for e-Seal in the certification business for qualified e-Seal with assurance level 2 | | Mandatory | Can be used by adding to the corporate number | | | |
|---|---|---|---|---|---|---|
| | | Corporate number | TDB company code | Standard company code | TSR company code*1 | LEI |
| | | Number system managed by public institutions | Numbering system managed by the private sector | | | |
| Identifier prefix | | NTRJP※2 | TD:JP | JI:JP | TS:JP | LEIXG※3※4 |
| Organization identifier example | | NTRJP-1234567890123 | TD:JP-123456789 | JI:JP-123456 | TS:JP-123456789 | LEIXG-12345678901234567890 |
| Note: | | | | | | |
| Target for numbering with the existing numbering system | Corporate | ◎ | ○ | ○ | ○ | ○ |
| | Associations and foundations without legal capacity to hold rights | ○ | ○ | ○ | ○ | — |
| | Other voluntary organizations | — | ○ | ○ | ○ | — |
| | Sole proprietorship | — | ○ | ○ | ○ | ○ |
| | Other individuals | — | — | — | — | — |

*1: The "D-U-N-S Number" is linked to the TSR company code.
*2: The prefix "GOVJP" can be used for government agencies or local governments.
3: Based on Appendix A of CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates Version 1.0.0.
*4: The method of storing LEIs in the extended area of electronic certificates is defined in ISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificates.

**Fig. 8 Organization identifiers used for electronic certificates for e-Seal of the**

[10] The method of storing LEIs in the extended area of electronic certificates is defined in ISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificates.
[11] Using "LEI: XG" is recommended for the Legal Entity Identifier (LEI).
[12] There are requirements for electronic devices to which electronic certificates for e-Seal are issued, but there has not been sufficient consideration of the technical and institutional aspects of electronic devices as the entities that create e-Seal.

**certification business for authorized e-Seal with assurance level 2**

Legend◎: All items are numbered (complete coverage) ○: Basically, numbering is possible △: Some items are numbered -: Out of scope

| Organization identifiers used for electronic certificates for e-Seal in the certification business for authorized e-Seal with assurance level 2 | | Using one of the organization identifiers is recommended | | | | |
|---|---|---|---|---|---|---|
| | | Corporate number | TDB company code | Standard company code | TSR company code※1 | LEI |
| | | Number system managed by public institutions | Numbering system managed by the private sector | | | |
| Identifier prefix | | NTRJP※2 | TD:JP | JI:JP | TS:JP | LEIXG※3※4 |
| Organization identifier example | | NTRJP-1234567890123 | TD:JP-123456789 | JI:JP-123456 | TS:JP-123456789 | LEIXG-12345678901234567890 |
| Note: | | | | | | |
| Target for numbering with the existing numbering system | Corporate | ◎ | ○ | ○ | ○ | ○ |
| | Associations and foundations without legal capacity to hold rights | ○ | ○ | ○ | ○ | — |
| | Other voluntary organizations | — | ○ | ○ | ○ | — |
| | Sole Proprietors | — | ○ | ○ | ○ | ○ |
| | Other individuals | — | — | — | — | — |

*1: The "D-U-N-S Number" is linked to the TSR company code.
*2: The prefix "GOVJP" can be used for government agencies or local governments.
3: Based on Appendix A of CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates Version 1.0.0.
*4: The method of storing LEIs in the extended area of electronic certificates is defined in ISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificates.

**Fig. 9 Organization identifiers used for electronic certificates for e-Seal of the certification business for e-Seal with assurance level 1**

## 2.2 Method of Confirming the Existence and Application Intention of the e-Seal Generator

Since the trustworthiness of e-Seal is ensured by confirming the existence and intent of applying organizations, etc., to which electronic certificates for e-Seal are issued (in other words, e-Seal generators), the confirmation method is important. In the case of electronic certificates for e-Seal of the certification business for authorized e-Seal, confirmation by a strict method is necessary. In the case of the certification business for authorized e-Seal with assurance level 1, confirmation may be done by a simpler, low-cost method.

The existence of an e-Seal generator is supposed to be verified in terms of (1) legal existence, (2) physical existence, and (3) operational existence. As a specific confirmation method, legal existence is supposed to be confirmed using the certificate of registration, etc. While physical and operational existence is supposed to be confirmed using a third-party institution database, etc.

As a specific method to confirm the intent of an e-Seal generator to apply, confirmation based on electronic signature-Seal, or signature etc., is performed. However, it is necessary to be able to confirm that the said applicant (an individual who signs electronically, affixes their seal, or signs, etc.) is definitely the representative of the said organization or a person authorized by the representative (only when it can be confirmed that the applicant is authorized by a letter of

attorney, etc.).

Based on the above, the image of the method of confirming the existence of an organization, etc., for the certification business for authorized e-Seal with assurance level 2 is shown in Fig. 10. The image of the method of confirming the intent to apply is shown in Fig. 11, referring to the CA/Browser Forum Guidelines[13], etc.

| Classification of organizations, etc. | Confirmation of existence of the organizations, etc. | | |
|---|---|---|---|
| | Confirmation of legal existence | Confirmation of physical existence | Confirmation of operations |
| - Corporate<br>- Associations and foundations without legal capacity to hold rights | Confirm using any of the following methods.<br>1. Confirm the validity of the electronic signature of the corporate representative(★) (Limited to those certified under Article 12(1), Paragraph 1 and Paragraph 3 of the Commercial Registration Act.)<br>2. Confirm the validity of the electronic signature using the electronic certificate that stores the attributes of the organization, etc. (★) (Certified Certification Business based on Article 4 of the Electronic Signatures Act)<br>3. Confirm the Certificate of Registration (Or check a third-party institution database*1) | Confirm using any of the following methods.<br>1. Confirm the address in the application with the address shown on the Certificate of Registration<br>2. Confirm the address in the application with the address registered in a third-party institution database*1(★) | Confirm using any of the following methods.<br>1. Check the date of incorporation on the Certificate of Registration and confirm that at least 3 years have passed since the company was established<br>2. Confirm registration in the database* of a third-party institution (★)<br>3. Confirm the holding status of bank account at financial institutions that are licensed, permitted, registered, etc. |
| Offices, sales offices, branches, divisions, etc., personnel, equipment | The Certification Authority shall respect the results of the declaration made by the representative of the organization, etc., and include the result of the declaration in the usage application in the extended area of the electronic certificate for e-Seal, assuming that the organization to which the electronic certificate is issued bears the primary responsibility. | | |

**Fig. 10 Image of the method of confirming the existence of an organization, etc., of the certification business for authorized e-Seal with assurance level 2**

| Classification of organizations, etc. | Confirm the intent of the organization, etc. (Representative) | Confirm the enrollment of the organization's representative |
|---|---|---|
| - Corporate<br>- Associations and foundations without legal capacity to hold rights | Application for use with electronic signature using commercial registration electronic certificate (★) | |
| | Seal on the application form (only if a registered seal certificate of the representative-Seal is attached) | |
| | Application for use with the electronic certificate for signature of representative's My Number Card, or electronic signature based on electronic signature for Certified Certification Business (★) (1)<br>Signature or seal of the representative on the application form (2) | [A: If confirmation of intent is (1)]<br>Confirm that the representative's address in the third-party institution database*1 matches the representative's address on the electronic certificate (★)<br>[B: If the confirmation of intention is (2) or cannot be confirmed by A]<br>Confirm whether the representative has submitted the application through the telephone number, etc., registered in the third-party institution database*1 |

**Fig. 11 Image of the method of confirming the intent to apply for the certification business for authorized e-Seal with assurance level 2**

In addition to Fig. 10, the confirmation method shown in Fig. 12 can be considered to confirm the existence of an organization, etc., for the certification business for e-Seal with assurance level 1. In addition to Fig. 11, the confirmation method shown in Fig. 13 can be considered for confirming the intention to apply for the certification business for authorized e-Seal.

| Classification of organizations, etc. | Confirmation of existence of the organizations, etc. | | |
|---|---|---|---|
| | Confirmation of legal existence | Confirmation of physical existence | Confirmation of operations |
| - Corporate<br>- Associations and foundations without legal capacity to hold rights<br>- Other voluntary organizations | Confirm the contents of the application with the registered contents in the database*1 (★) managed by a third-party institution | | |
| Sole proprietorship | Confirm various types of identification (Driver's license, etc.) | | |
| Offices, sales offices, branches, divisions, etc., personnel, equipment | The Certification Authority shall respect the results of the declaration made by the representative of the organization, etc., and include the result of the declaration in the usage application in the extended area of the electronic certificate for e-Seal, assuming that the organization to which the electronic certificate is issued bears the primary responsibility. | | |

**Fig. 12 Image of the method to confirm the existence of an organization, etc., for the certification business for e-Seal with assurance level 1**

[13] Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.8.0, CA/Browser Forum, 30 November, 2022

| Classification of organizations, etc. | Confirm the intent of the organization, etc. (Representative) | Confirm the enrollment of the organization's representative |
|---|---|---|
| - Corporate<br>- Associations and foundations without legal capacity to hold rights | Application for use with the electronic certificate for signature of representative's (or applicant's[*2]) My Number Card, or electronic signature based on electronic signature for Certified Certification Business (※) (1)<br><br>Signature or seal of the representative (or applicant[*2]) on the application form(2) | [C: If confirmation of intent is (1)]<br>Confirm that the representative's (or applicant's[*2]) address in the database[*1] managed by a third-party institution matches the representative's (or applicant's[*2]) address on the electronic certificate (★)<br>[D: If the confirmation of intention is (2) or cannot be confirmed by C]<br>Confirm whether the representative (or applicant[*2]) has submitted the application through the telephone number, etc., registered in the database[*1] managed by the third-party institution |
| Sole proprietorship | | |

**Fig. 13 Image of the method to confirm the intent to apply for the certification business for authorized e-Seal with assurance level 1**

The certification authority will respect the result of the declaration of a representative of the organization, etc., will enter the result of the declaration in the extended area of the electronic certificates for e-Seal based on the assumption that the organization, etc., to which the certificate is issued bears primary responsibility, in light of such facts, that the business offices, sales offices, branch offices, or departments pertaining to the e-Seal generator, or personnel of the organization (individuals with no declared intent) are not themselves the subject of issuance of electronic certificates for e-Seal, that the cost to verify their existence by the certification authority is expected to be enormous, and that the information thereof is described in the real space according to the rules of each organization, such as in documents (for example, the names of offices and business offices included in documents, etc.).

## 2.3 Format and Matters to be Specified in Electronic Certificates for e-Seal

To maintain consistency with similar systems in Japan and overseas, the format of electronic certificates for e-Seal with assurance level 2 will be ITU-T X.509. The details to be mentioned in electronic certificates for e-Seal include the official name of the organization to which the certificate is issued (in other words, the e-Seal generator), an identifier that uniquely identifies the said organization, etc., the validity period, public key, signature algorithm, issuer (certification authority) of the electronic certificates for e-Seal, and other attribute information (business office, sales office, devices, etc.), an example of which is shown in Fig. 14.

In addition, in electronic certificates for e-Seal, a detail that can distinguish between electronic certificates for “electronic signatures” and electronic certificates for “e-Seal” in a machine-readable form is included. In the EU, an OID (Object Identifier) is specified for each type of trust service and included in the certificate policy, one of the items included in electronic certificates. This helps to distinguish between electronic certificates of electronic signatures and e-Seal, etc. From the perspective of international interoperability, an OID will be included as part of a common certificate policy.

| | Field Name | Value (Sample) |
|---|---|---|
| Basic area | Version | V3 |
| | Serial number | 01ab45678cdfe |
| | Signature algorithm | SHA256withRSA/SHA512withRSA, etc. |
| | Name of issuer | Information identifying the issuer (organization identifier is stored in Organization Identifier) |
| | Expiration start time | December 8, 2023 12:30:45 UTC |
| | Expiration end time | December 8, 2025 12:30:45 UTC |
| | Subject name | Official name of the organization that is subject of issuance, information identifying the organization, etc. (organization identifier is stored in Organization Identifier) |
| | Public key information | RSA (2048bit), etc. |
| Extended area | Purpose of key usage | digitalSignature, nonrepudiation |
| | Basic restrictions | cAflag = FALSE |
| | Issuer key identifier | kid=1234abcd･･･ |
| | Subject key identifier | 4567cdef･･･ |
| | Certificate policy | [1] CA-specific certificate policy [2] Common certificate policy |
| | Subject alias | “Offices, sales offices, branches, divisions, etc., personnel, equipment” or “Japanese trade name of organization”, etc. |
| | CRL distribution point | http://example.co.jp/ica.crl |
| | Institution information access | [1] URL of CA certificate [2] URL of OCSP |
| | LEI (Legal Entity Identifier) | 123456789012345ABCDE |

**Fig. 14 Example of items to be included in electronic certificates for e-Seal**

## 2.4 Standards for Management of Private Keys of Certification Authorities

The private key of a certification authority is used to sign electronic certificates and certificate revocation lists issued by the certification authority. It has a different purpose than the private key used to create e-Seal[14]. Therefore, for example, if stolen and misused by a malicious third party, the trustworthiness of electronic certificates for e-Seal issued by the certification authority will be severely damaged, affecting all organizations, etc., to whom electronic certificates for e-Seal have been issued by the certification authority. Therefore, private keys of certification authorities must be strictly managed by an HSM[15], etc. In addition, security measures and measures against unauthorized access to the room where the relevant HSM is located are necessary.

Concerning the standards for the HSM and the management of certification authorities, it is assumed that electronic certificates for e-Seal of the certification business for authorized e-Seal must fulfill sufficient standards in terms of security requirements, etc., and are required to meet the same standards as the management of private keys of certification authorities in the certified certification business[16] for digital signatures, which is one of the trust services. Therefore, the

[14] In the unlikely event that the private key of a certification authority is leaked, a malicious third party could impersonate the certification authority and issue forged electronic certificates and revocation lists.
[15] Abbreviation of Hardware Security Module. A cryptographic processor with key management functionality, the physical security of which is ensured by a tamper-proof mechanism.
[16] Specific certification business (a certification business performed for highly secure digital signatures) in the Electronic Signatures Act, certified by the cabinet minister, which conforms to the standards of rigor for the implementation of the business (e.g., confirmation of user authenticity).

provisions of the Electronic Signatures Act will apply. However, concerning the technical standards for the HSM, it is assumed that the current version will be used as per the standard specified separately.

## 2.5 Standards for Management of Private Keys of e-Seal Generators

Regarding the management of an e-Seal generator's private key in the local e-Seal method, once the private key is safely and securely transferred from the certification authority to the e-Seal generator, it becomes a matter of management by the e-Seal generator.

In this regard, even in the case of electronic signatures, which are used for a declaration of intent and for which presumptive provisions are legally stipulated, there are no provisions regarding the medium on which the private key, etc., of an e-Seal generator, is stored or how the private key of an e-Seal generator is managed, leaving the management of the private key of the e-Seal generator to the e-Seal generator.

Therefore, for the time being, the certification business for authorized e-Seal does not have any requirement of the provision regarding the media (hereinafter referred to as "e-Seal generation device" to store the private key, etc., of an e-Seal generator, and as "certified e-Seal generation device", for e-Seal generation devices authenticated, in particular, by a third-party institution) for accreditation, and the management of the e-Seal generator's private key will be left to the organization, etc., to which the key is issued (in other words, the e-Seal generator).

However, the following 2 points require special attention.

(1) Matters to be explained by the certification authority to the e-Seal generator

Although the management of the private key of an e-Seal generator is left to the party concerned, the party needs to understand the importance[17] of such management. Therefore, as a matter to be explained by the certification authority to the person to whom an electronic certificate for e-Seal is issued (in other words, the e-Seal generator), it is necessary to stipulate that the private key must be strictly managed (e.g., duplication is not preferred) as a matter about private key management. Also, it should be noted that since duplication of the private key on the part of the e-Seal generator is not preferred, duplication of the e-Seal generator's private key on the part of the certification authority is also not preferred. It should also be noted that when the certification authority creates the e-Seal generator's private key, the method of managing the private key should be agreed upon in advance between the certification authority

[17] In the case of an e-Seal with assurance level 2, the-Seal is naturally expected to be recognized and processed as a e-Seal with trustworthiness by the recipient of electronic documents, etc., assigned the relevant e-Seal, thus requiring careful handling of the management of the e-Seal generator's private key necessary for the e-Seal.

and the e-Seal generator, including the deletion of the private key by the certification authority after the private key is sent to the e-Seal generator by the certification authority. An example of the management of an e-Seal generator's private key is shown in Fig. 15.

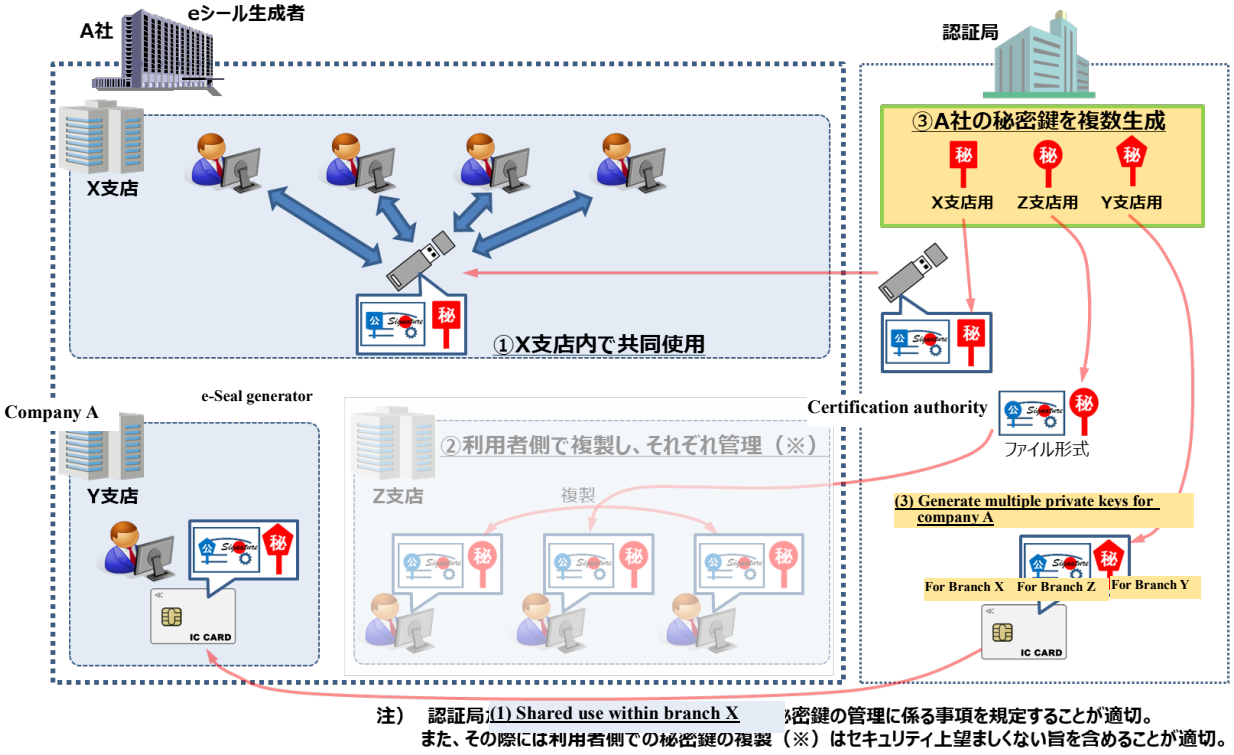



**Fig. 15 Example of private key management of an e-Seal generator**

(2) Duplicated by the users and managed respectively(*) File format

Branch Y Branch Z Duplication

(2) Use of e-Seal generation device

Although the provision related to e-Seal generation devices is not a requirement for accreditation in the certification business for e-Seal, authenticated e-Seal generation devices may be use Branch X t is envisaged that there will be situations in the future where authenticated e-Seal generation devices will be required from the perspective of international consistency. It is preferable to ha an authenticated e-Seal generation device has been used to assign the e-Seal.

Note: It is appropriate to stipulate matters related to private key management as explanations from the certification authority to users.
In addition, also include that duplication (*) of private keys by the users is not preferred for security reasons.

If security issues arise in the future, including the Electronic Signatures Act, it will be necessary to consider whether certification of generation devices is required again, and should the certification of generation devices be required, it should be noted that the current accreditation criteria of the Electronic Signatures Act would be strengthened (what was previously allowed would no longer be allowed).

## 2.6 Process When Generating a Large Number of e-Seal

In the case of e-Seal, it is expected that there will be a need to assign e-Seal mechanically and automatically in batches to multiple target electronic documents (e.g., receipts, etc.),

regardless of local and remote e-Seal methods, to improve operational efficiency.

In Japan, it is common practice to approve and seal multiple target documents at once in real-space procedures, and because an e-Seal does not involve a declaration of intent and serves only as a proof of the issuer in the first place, in the certification business for authorized e-Seal, it is allowed to create e-Seal in batches for multiple target electronic documents, etc.

However, when creating e-Seal in batches, since it is required to create e-Seal only for the electronic documents specified by the e-Seal generator, especially in the remote e-Seal method, the remote e-Sealervice provider must ensure that no other electronic documents are mixed with the electronic documents for which the e-Seal generator has granted the e-Seal.

## 2.7 Use Authentication with the Remote e-Seal Method[18]

### 2.7.1 User Authentication when Creating e-Seal with the Remote e-Seal Method

In the local e-Seal method, it is generally assumed that the private key managed by the e-Seal generator is authorized[19] using a PIN code, etc., to create an e-Seal. On the other hand, in the remote e-Seal method, the e-Seal generator does not manage the private key and entrusts the management to a remote e-Sealervice provider, requiring consideration of use authentication when creating a remote e-Seal with assurance level 2.

Based on the key authorization in the local e-Seal method, it is necessary for the remote e-Seal method first to authenticate the e-Seal generator authority who has access to the cloud environment of the remote e-Sealervice provider, where the private key of the e-Seal generator is stored (hereinafter referred to as “Use authentication”), and then authorize the key to create the e-Seal.

In other words, when using the remote e-Seal method to perform the certification business for authorized e-Seal, separately performing use authentication and key authorization is a minimum requirement. In addition, presumptive provisions[20] are legally stipulated for electronic signatures with a declaration of intent, and the “Remote Signing Guidelines” for remote signatures require key authorization to be performed separately from the use

---

[18] The issues related to remote e-Sealervice providers need to be addressed based on the trend of discussions, including issues related to remote signature service providers, at the Digital Agency, which are consolidated as a matter for continued consideration.

[19] Refers to the activation and enabling the use of private key by the e-Seal generator to assign an e-Seal.

[20] Act on Electronic Signatures and Certification Business (Act No. 102 of 2000)

Article 3 Any electromagnetic record that is made to express information (except for those prepared by public officials in the course of duties) is presumed to be established authentically if the electronic signature (limited to that which can be performed by the principal through appropriate management of codes and objects necessary to perform this) is performed by the principal with respect to information recorded in the relevant electromagnetic record.

authentication and multi-factor authentication to be performed for key authorization. However, in the key authorization for the remote e-Seal method, single-factor authentication may be performed, considering that e-Seal serve only as proof of the issuer without a declaration of intent.

### 2.7.2 Management of Authentication Factors Used in Key Authorization

In the remote e-Seal method where the remote e-Sealervice provider manages the e-Seal generator's private key, if the remote e-Sealervice provider also manages authentication factors such as PIN code used in key authorization and can potentially perform e-Seal without informing the e-Seal generator, it may be impossible to determine the e-Seal generator. In particular, if there is a possibility that authentication factors are not properly managed in the remote e-Seal method with assurance level 2, e-Seal with assurance level 2 having impaired reliability may exist and circulate, which could affect the system stability.

In the case of electronic contract services using electronic signatures, there is room to consider that both parties agree on using the remote signature service because the parties to the document agree on the method to use. However, in the case of securing the trust of electronic data using e-Seal, there is a high probability that the recipient of electronic documents (e.g., the recipient of receipts) cannot be consulted in advance regarding the use of remote e-Seal services. Thus, it cannot be considered that there is a mutual agreement.

Considering the above, the management of authentication factors is performed by the e-Seal generator. In addition, to prevent the existence and circulation of e-Seal for which the e-Seal generator does not manage the authentication factors, certain standards (e.g., no management of authentication factors by service providers is allowed) are required for remote e-Sealervice providers who provide the certification business for authorized e-Seal using the remote e-Seal method.

## 2.8 Revocation Request of Electronic Certificates for e-Seal

When the private key of an e-Seal generator is compromised[21], or when organizations, etc., to which electronic certificates for e-Seal are issued (in other words, e-Seal generators) are reorganized, the electronic certificates for e-Seal must be revoked at an appropriate time. Specifically, since a compromised private key of an e-Seal generator may be misused by a third party for impersonation, etc., the electronic certificates for e-Seal associated with the private key must be revoked as soon as possible.

[21] A situation in which the level of security has significantly reduced, such as when private key information has been or is likely to be leaked to a third party, or when the PIN code, etc. used for key authorization of a private key has been lost.

In the case of electronic signatures, the signatory's private key and the person who can handle the key are on a one-to-one basis, and in the case of e-Seal, it is assumed that a single private key of the e-Seal generator is used by multiple personnel within the organization. Therefore, it is necessary to consider who can request revocation of the private key since a revocation request requires a declaration of intent in the same manner as an application to issue electronic certificates for e-Seal. In principle, those who can request revocation will be limited to those who can request issuance of electronic certificates for e-Seal (in the case of a corporate, the representative or a person authorized by the representative).

The Ordinance for Enforcement of the Act on Electronic Signatures and Certification Business (Ordinance No. 2 of the Ministry of Internal Affairs and Communications, the Ministry of Justice, and the Ministry of Economy, Trade and Industry, 2001) stipulates cases in which a certification authority may request a revocation, such as "when something different from the fact is found in the matters recorded in the electronic certificate[22]" or "when there is a possibility that the user signature code has been compromised[23]", and it is preferable to define CP/CPS, etc., for e-Seal as well, by referring to the ordinance.

[22] Stipulated in Article 6, Item (10) of the Ordinance for Enforcement of the Act on Electronic signatures and Certification Business.
[23] Stipulated in Article 8, Item (3) of the Guidelines Pertaining to Accreditation in Specific Certification Business under the Act on Electronic Signatures and Certification Business. "Compromised" is defined as "Theft, leakage, etc., that results in a state that allows use by another person.".

## Conclusion

In a society driven by data, where data is the source of value and has significant value, the key is ensuring data reliability and constructing a robust trust infrastructure to support safe and secure data distribution.

In a society where perceptions of work styles, including remote work, are diversifying among companies and individuals due to the spread of the novel coronavirus, there has been a significant increase in the need to complete all procedures electronically in a smooth manner, regardless of whether they are for government or private sector use.

In this context, the current systems, such as electronic signatures that indicate intent and timestamps that authenticate time, cannot address these needs, and there is a growing expectation for an easier and simpler mechanism to guarantee the origin and integrity of various other information.

Furthermore, in addition to these trends, the business environment in which Japanese companies operate is also changing constantly. As international business activities continue to grow exponentially, there is an increasing demand for a system that facilitates seamless data exchange with overseas trading partners.

Given this situation, MIC convened the “Study Group on a System for Ensuring the Reliability of Data Issued by Organizations” from April 2020 to June 2021 and formulated the previous Guidelines outlining the status of e-Seal in Japan. Subsequently, from the perspective of promoting the further spread and utilization of e-Seal, a “Study group on e-Seal” has been held from September 2023. The study group concluded that it would be appropriate for the Minister for Internal Affairs and Communications to establish a certification system for e-Seal and decided to revise the previous Guidelines following the establishment of this certification system.

We expect that policy to assist business operators who will manage the certification authority providing certification business for e-Seal, enhancing their operations, and contributing to ensuring the reliability of data distribution.