仮訳
Provisional Translation

# Final Report
# of Study Group on e-Seal

**April 2024**

**Study Group on e-Seal**

Table of Contents

Introduction ..... 1

Chapter 1 What is an e-Seal? ..... 2

1.1 What is a Trust Service? ..... 2

1.2 What is an e-Seal? ..... 3

Chapter 2: History of Deliberations by the Japanese Government ..... 5

2.1 Discussions of the "Trust Service Review Working Group" ..... 5

2.2 Discussions in the "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations" ..... 5

2.3 Discussions in the "Sub-Working Group for Promoting DX with Secured Trust" ..... 6

2.4 Establishment of This Study Group ..... 6

Chapter 3 Establishment of a Certification System for e-Seal ..... 7

3.1 Positioning of e-Seal in Government Strategies ..... 7

3.2 Realization of Conformity Assessment for e-Seal ..... 8

3.3 Present Status of the Certification System ..... 8

3.4 Revision of "Guidelines on e-Seal" ..... 9

Chapter 4 Individual Discussion Points and Directions ..... 10

4.1 Classification of e-Seal ..... 10

4.2 Scope of Organizations to Which Electronic Certificates for e-Seal are Issued ..... 11

4.3 Method of Verifying the Existence and Application Intention of the e-Seal Generator . 14

4.4 Format and Matters to be Specified in Electronic Certificates for e-Seal ..... 16

4.5 Standards for Management of Private Keys of Certification Authorities ..... 17

4.6 Standards for Management of Private Keys of e-Seal Generators ..... 17

4.7 Process When Generating a Large Number of e-Seal ..... 18

4.8 Remote e-Seal ..... 18

4.9 Revocation Request of Electronic Certificates for e-Seal ..... 19

Chapter 5 Issues to be Considered in the Future ..... 19

5.1 Main Matters to be Discussed Before the Certification System Begins Operation ..... 19

5.2 Efforts to Promote e-Seal ..... 20

5.3 Possibility of Using e-Seal in International Data Distribution ..... 22

Conclusion ..... 24

## Introduction

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.

Against this context, in June 2021, the Ministry of Internal Affairs and Communications (MIC) established the "Guidelines on e-Seal," which prescribed certain technical and operational standards for e-Seal. Although certain companies have adopted e-Seal following these guidelines, the absence of a conformity assessment framework, such as a national certification system, has led to minimal public awareness regarding e-Seal.

A study group was convened in September 2023 under the auspices of the Minister for Internal Affairs and Communications to enhance the dissemination and utilization of e-Seal. The group's mandate included evaluating the necessity for a MIC-led certification system for e-Seal. In January 2024, the group published its preliminary findings in an "Interim Report" document. While preparing the "Interim Report," the study group engaged with a substantial number of stakeholders via a public consultation process (public comments). After considering the opinions, the group held further deliberations and prepared the "Final Report."

We sincerely hope that the discussions in this study group will highlight the crucial role of trust services, such as e-Seal, in society. By promoting the use of these services, we aim to support the construction of a social infrastructure that ensures secure and reliable electronic data distribution, thereby delivering significant benefits to all citizens.

# Chapter 1 What is an e-Seal?

## 1.1 What is a Trust Service?

The term "Trust Services" is defined in the "Trust Service Review Working Group of the Study Group on Platform Services Final Report," published by MIC, as the "mechanisms designed to verify the authenticity of individuals, organizations, and data on the Internet, and to prevent falsification and impersonation of the sender."[1]

In the context of Society 5.0 and the realization of Data Free Flow with Trust (DFFT), as advocated by Japan, trust services are expected to become fundamental and play an important role in the secure and efficient exchange of electronic data. These services are recognized as pivotal in numerous governmental policies, reflecting their critical role in fostering a reliable digital environment.

**Reference: Descriptions of "Trust services" in various government policies**

◆ **Cybersecurity Strategy (Cabinet decision on September 28, 2021)**

To effectively promote diverse economic and social activities in cyberspace, it is essential to guarantee the authenticity of data, which is foundational to its value, and to ensure the trustworthiness of the distribution infrastructure. This is crucial from a data governance perspective to achieve "Data Free Flow with Trust (DFFT)." (Omitted) Regarding mechanisms to prevent impersonation of the sender, data falsification, and other issues (hereinafter referred to as "Trust Services"), it is necessary to establish effective mechanisms for their utilization.

◆ **Priority Policy Program for Realizing Digital Society (Cabinet decision on June 9, 2023)**

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.

Through these policies, the government actively promotes a range of trust services. These include "Electronic signatures," "Timestamps," and "e-Seal" (Fig. 1). Specifically, the Digital Agency promotes the comprehensive framework for trust services and "electronic signatures." While, MIC advances individual trust services, including "timestamps" and "e-Seal."

[1] Source: Ministry of Internal Affairs and Communications, "Trust Service Review Working Group of the Study Group on Platform Services Final Report" February 7, 2020, p. 2.

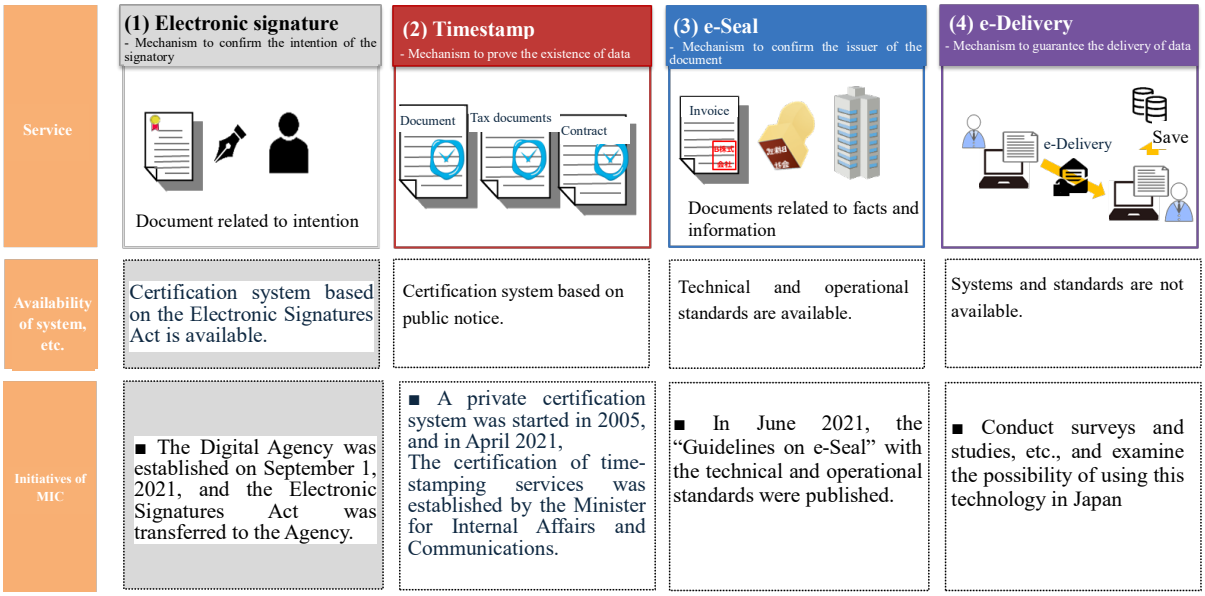



Fig. 1 Status of representative trust services in Japan

Looking at other countries, the eIDAS (Electronic Identification, Authentication and Trust Services) regulation of the EU defines trust services as follows[2,3]:

**Reference: Regulations regarding "Trust Services" in eIDAS**

Article 3(16) 'trust service' means an electronic service normally provided for remuneration which consists: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services;

## 1.2 What is an e-Seal?

The "Guidelines on e-Seal" formulated by MIC on June 25, 2021, shows the technological and operational parameters for e-Seal, which defined e-Seal as "An encryption tool designed to denote the organization or entity that issued the electronic documents, etc., with a mechanism to confirm that the relevant documents have not been falsified since the application of the encryption measure."

In this Study Group,

1) The eIDAS regulation designates e-Seal as "data," and to facilitate international

[2]"Electronic attestation of attributes," "the electronic archiving of electronic documents," "the management of remote electronic signature and seal creation devices," and "the recording of electronic data into an electronic ledger" are scheduled to be added to eIDAS2.0.

[3] The definition of Trust Services is described in Article 1. Definitions (l) of UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services in the United Nations Commission on International Trade Law (UNCITRAL).

interoperability, it is prudent to maintain the classification as "data,"

2) Considering the prevalent applications of e-Seal, they are commonly recognized as "data." Therefore, discussions were conducted on the necessity of revising the definition in the "Guidelines on e-Seal."[4]

**Reference 1: Regulations regarding "e-Seal" in eIDAS**

Article3 (25)'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

Furthermore, incorporating elements such as "origin" and "integrity" into the revised definition, as referenced in the eIDAS regulation, was determined to be appropriate.

Regarding the term "e-Seal," it was decided to maintain the term "e-Seal" since it has gained a certain level of recognition.

Based on the above, the definition of e-Seal is summarized as follows:

[Definition of an e-Seal]

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.

**Reference 2: Differences between e-Seal and electronic signatures[5]**

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., issuing them has the advantage of doing away with the requirement of reissuing electronic certificates for e-Seal due to personnel changes within the organization, and because there is no declaration of intent involved, e-Seal can be performed mechanically and automatically to a large number of electronic documents. It should be noted that the intention of the natural person who performed the e-seal is not expressed in the electronic documents, etc., bearing the e-seal.

---

[4] In accordance with the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000, hereafter referred to as the "Electronic Signatures Act"), where electronic signatures are defined as "measures," there were also suggestions that e-Seal also be likewise categorized as "measures."

[5] Excerpt from "1.2 Differences between e-Seal and Electronic Signatures" on p. 5 of the "Guidelines on e-Seal" (June 25, 2021).

## Chapter 2: History of Deliberations by the Japanese Government

### 2.1 Discussions of the "Trust Service Review Working Group"

From January 2019 to November 2019, under the aegis of MIC "Platform Services Study Group," the "Trust Service Review Working Group" was convened, which was tasked with organizing issues pertinent to trust services within Japan and deliberating on their optimal implementation (Fig. 2).

The working group delivered a comprehensive overview of the trends in the utilization of trust services within Japan, the results of international surveys on similar trends, and the economic impacts associated with the utilization and widespread adoption of trust services. In the context of e-Seal, the discussions underscored the importance of presenting technical and operational standards that trustworthy service providers must meet. Thereby ensuring users can utilize these services with absolute confidence. On the other hand, concerns were raised about the potential impact on future technological development and service deployment if e-Seal are positioned within a national certification system, especially since the service content and technologies required for e-Seal service provision have not yet been established in Japan.

In light of these discussions, the "Final Report"[6] of the working group recommended that "first, to facilitate the development and deployment of services that provide e-Seal, primarily via private voluntary initiatives with some governmental involvement, a private certification mechanism for credible service providers should be established. Additionally, attention must be paid to the technical and operational standards necessary for trustworthy service providers and the certification mechanism."

### 2.2 Discussions in the "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations"

Drawing on the guidelines provided in the "Final Report" of the "Trust Service Review Working Group Final Report," the "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations Report" convened from April 2020 to June 2021 to deliberate on their optimal implementation of e-Seal in Japan (Fig. 2).

In this study group, discussions were conducted from three distinct perspectives: (1) Consistency with other similar frameworks in Japan (interactions with electronic signatures as defined in the Electronic Signatures Act, etc.), (2) International harmonization (Conformity with frameworks and institutions in other jurisdictions, such as the EU, etc.), and (3)

[6] Source: Ministry of Internal Affairs and Communications, "Trust Service Review Working Group Final Report" (February 7, 2020), p. 31

Advancement of the dissemination and application of e-Seal (structuring e-Seal for enhanced clarity and accessibility from the perspective of e-Seal users, etc.).

In the "Report"[7] of this study group, a strategic vision for the future development of e-Seal in Japan is outlined, focusing on several key aspects: (1) Essential elements of e-Seal, (2) Scope of organizations to which electronic certificates for e-Seal are issued (3) Procedures for confirming the existence and application intention of organizations, (4) Information to be included on electronic certificates for e-Seal, (5) Equipment specifications (Cryptographic devices used by certification authorities, e-seal generation devices for users, etc.), and (6) Additional technical standards (such as remote authentication methods and CRLs—Certificate Revocation Lists).

In June 2021, the "Guidelines on e-Seal" were formulated following deliberations within the study group. These guidelines define specific standards for e-Seal technology and operations as the government prescribes.

## 2.3 Discussions in the "Sub-Working Group for Promoting DX with Secured Trust"

Following the creation of the Digital Agency in September 2021, the "Sub-Working Group for Promoting DX with Secured Trust" convened from November 2021 to June 2022 under the auspices of the "Data Strategy Promotion Working Group" to deliberate on specific strategies for advancing digital transformation while ensuring trust (Fig. 2).

The "Report"[8] of this sub-working group articulated, "In the future, an anticipated escalation in the demand for verification of issuers in online transactions and processes is expected. Consequently, Digital Agency should bolster the Ministry's endeavors to develop standards for evaluating the reliability of private e-Seal services and realize conformity assessment according to the 'Guidelines on e-Seal' announced by MIC in June 2021."

## 2.4 Establishment of This Study Group

Based on the "Report" of the "Sub-Working Group for Promoting DX with Secured Trust," MIC has resolved to undertake further studies focused on "developing standards for evaluating the reliability of private e-Seal services and realize conformity assessment."

To accurately evaluate the current landscape of e-Seal service provision, MIC initiated a

[7] Source: Ministry of Internal Affairs and Communications, "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations Report" (June 25, 2021), p. 7
[8] Source: Digital Agency, "Sub-working Group for Trust-Assured Digital Transformation Report" (July 29, 2022), p. 3

"Research Study on e-Seal" in FY 2022 and solicited public input on the condition of e-Seal services across Japan from April to May 2023[9].

Consequently, it has been determined that numerous enterprises in Japan provide services that conform to the criteria for e-Seal. Nonetheless, the absence of a unified national framework for e-Seal has been recognized as a major impediment to their broad acceptance.

In consideration of these factors, MIC has resolved to convene the "Study Group on e-Seal" commencing in September 2023, to deliberate on the framework for e-Seal (Fig. 2). This study group published an "Interim Report" in January 2024 as a preliminary deliverable.

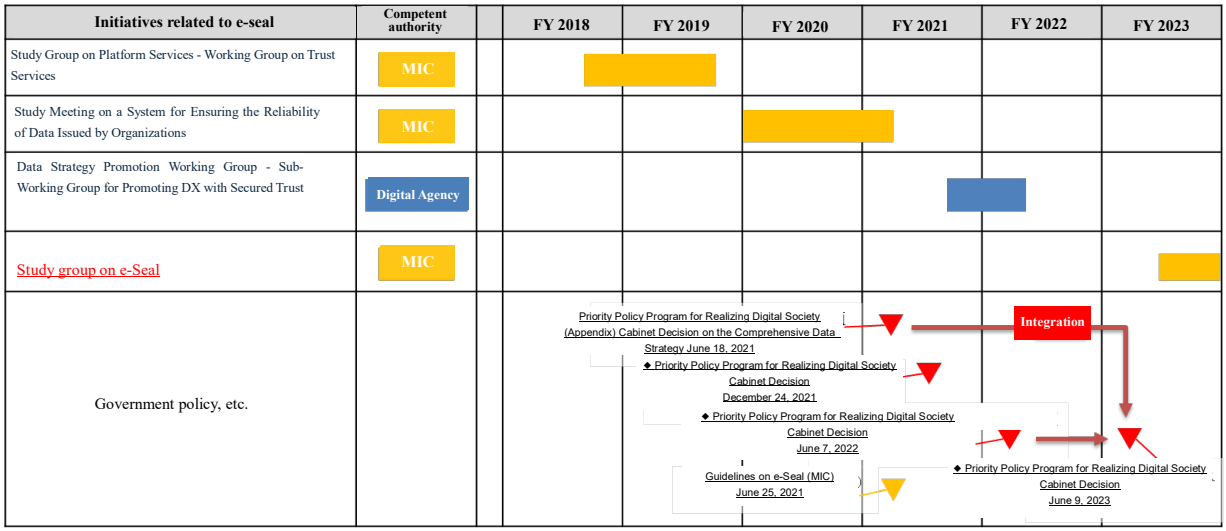



Fig. 2 History of deliberations by the Japanese government

# Chapter 3 Establishment of a Certification System for e-Seal

## 3.1 Positioning of e-Seal in Government Strategies

The "Priority Policy Program for Realizing Digital Society" (Cabinet decision on June 9, 2023. Hereinafter referred to as the "Priority Policy Program") states that "Efforts will also be made to develop standards for evaluating the reliability of private e-Seal services and realize conformity assessment," and the Priority Policy Program's progress schedule (Fig. 3) indicates that MIC should work on "Consideration of draft e-Sealtandards, etc."

**Reference: Description of "e-Seal" in government policies**

**◆ Priority Policy Program for Realizing Digital Society (Cabinet decision on June 9, 2023) (excerpt)**

In the future, an anticipated escalation in the demand for verification of issuers in online transactions

[9] Request for information regarding the status of e-Seal services in Japan https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00163.html

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.

◆ **Priority Policy Program for Realizing Digital Society: Progress schedule (excerpt)**

| Initiative name | Initiative details | FY 2022 | | | | FY 2023 | | | | FY 2024 | | | | FY 2025 | | | | FY 2026 | | | | Responsible government agency |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1Q | 2Q | 3Q | 4Q | 1Q | 2Q | 3Q | 4Q | 1Q | 2Q | 3Q | 4Q | 1Q | 2Q | 3Q | 4Q | 1Q | 2Q | 3Q | 4Q | |
| (1) Trust<br>- e-Seal, timestamp | Survey of needs for e-seals, etc., in Japan | | | | | | | | | | | | | | | | | | | | | MIC |
| | Understand the current situation of e-seal businesses | | | | | | | | | | | | | | | | | | | | | MIC |
| | Consideration of draft e-seal standards, etc. | | | | | | | | | | | | | | | | | | | | | MIC |

Fig. 3 Examination process for e-Seal

## 3.2 Realization of Conformity Assessment for e-Seal

Regarding the "development of the standards for evaluating the reliability of private e-Seal services" described in the Priority Policy Program, certain technical and operational standards have already been prescribed in the "Guidelines on e-Seal," formulated in June 2021. On the other hand, regarding the "Realization of conformity assessment," one of the policies listed in the Priority Policy Program, there is currently no framework for conformity assessment by the national government.

In response to this situation, the discussion in this study group concluded that it would be appropriate for the Minister for Internal Affairs and Communications to establish a certification system for e-Seal as a framework for conformity assessment by the national government.

## 3.3 Ideal Status of the Certification System

A precedent for establishing a certification system for trust services by the Minister for Internal Affairs and Communications is the certification system for timestamps, which was established through a notification by MIC (Fig. 4). Concerning this system, discussions were held on the establishment of a certification system for e-Seal, with "Certification Business for e-Seal[10]" serving as the subject [11,12]of certification.

Specifically, each point described in Chapter 4, "Individual Discussion Points and Direction," was discussed based on what has been organized to a certain extent in the "Guidelines on e-Seal." The "Guidelines on e-Seal" will be revised based on the direction indicated by the "Study Group on e-Seal."

[10] Refers to the operations of certifying organizations that generate e-Seal. The same shall apply hereinafter.
[11]A certification system for "Electronic signatures," which shares many technical similarities with "e-Seal," has also been established with respect to "Certification Business Conducted by the Certification Authority.".
[12] The study group concluded that it would be appropriate to set the validity period of certification to two years, and to allow a "Designated survey institution" to perform part of the work concerning assessment of certification.

**MIC notification for the timestamp certification system**

- Certification (Article 3)
- Update of certification (Article 4)
- Certification of changes (Article 5)
- Operation rules (Article 6)
- Handling of personal information (Article 7)
- Reporting, etc., on the status of implementation (Article 8)
- Cancellation of certification (Article 9)
- Approval (Article 10)
- Reporting obligations, etc. (Article 11)
- Designated survey institutions, etc. (Article 12 - Article 24)

**Stipulation of bylaws**

**Implementation guidelines for certification of time certification business (Excerpts)**

| Public notice | Implementation guidelines |
|---|---|
| - **Article 3(1), paragraph 1**<br>Digital signature method (omitted) shall be used. | - **Article 4 (Timestamp)**<br>- Standards for timestamp<br>- **Article 5 (Electronic Certificate)**<br>- Items to be included in the electronic certificate<br>- Requirements for reliable certification businesses, etc. |
| - **Article 3(1), paragraph 2**<br>The institution reporting the Japan Standard Time (omitted) shall use the Coordinated Universal Time (UTC (NICT)) as its time source and implement measures to control and certify the quality of time so that the time difference from that time source is within 1 second. | - **Article 6 (Time Source)**<br>- Time source requirements<br>- **Article 7 (Time Quality Control and Certification)**<br>- Time quality control and certification method |
| - **Article 3(1), paragraph 3**<br>A timestamp containing information that can uniquely identify whether it is a certified business and has the means to detect any tampering with the timestamp must be reliably generated using encryption technology and devices that are sufficiently secure while the timestamp is valid. | • **Article 8 (Identification of Certified Business)**<br>- Information to be included in the timestamp<br>• **Article 9 (Encryption Technology Involved in Generating Timestamps)**<br>- Requirements of encryption technology related to generation<br>• **Article 10 (Private Key Protection Device)**<br>- Requirements of private key protection device<br>• **Article 11 (Generation Process of Timestamps)**<br>- Requirements of generation process methods<br>• **Article 12 (Management of Private Keys)**<br>- Requirements of management method for private keys<br>• **Article 13 (Validity Period of Timestamp)** |

Fig. 4: Ministry of Internal Affairs and Communications notification for timestamp certification system

## 3.4 Revision of "Guidelines on e-Seal"

As described in Section 2.2, the "Guidelines on e-Seal" were established in June 2021 based on the discussions of the "Study Group on a System for Ensuring the Reliability of Data Issued by Organizations," and serve as guidelines to indicate the ideal form of e-Seal in Japan and to provide technical and operational standards to ensure the trustworthiness of e-Seal. In response to the direction given by the "Study Group on e-Seal," the "Guidelines on e-Seal" will be revised as shown in Fig. 5.

| Draft plan | | Major revisions |
|---|---|---|
| Purpose of these guidelines, etc. | | - Description of application of these guidelines and previous guidelines |
| Chapter 1 | What is an e-seal? | |
| 1.1 | Definition of e-Seal | - Revision of the e-seal definition |
| 1.2 | Differences Between e-Seal and Electronic Signatures | |
| 1.3 | Assurance Level of e-Seal | - e-Seal classification (warranty level) described in Chapter 2 moved to Chapter 1<br>- Regarding the **e-seal assurance level**, the redefined assurance level 1 and assurance level 2 are described. |
| 1.4 | Use Cases of e-Seal | New description of **possible use cases for each redefined assurance level** |
| 1.5 | Mechanism for Ensuring Trust Using E-Seal | |
| 1.6 | e-Seal Generation Methods<br>(Local e-Seal Method/Remote e-Seal Method) | - Explanation and update of the figures and tables based on the first set of materials |
| Chapter 2 | Present Status of Certification Business for e-Seal in Japan | |
| 2.1 | Scope of Organizations, etc., to Which Electronic Certificates for e-Seal are Issued | - Describes the scope of issuance of electronic certificates for e-Seal certified by the Minister for Internal Affairs and Communications<br>- Describes the **organization identifier** to be stored in the electronic certificates for e-Seal |
| 2.2 | Method of Verifying the Existence and Application Intention of the e-Seal Generator | - Regarding the methods to confirm the **actual existence of the e-seal generators, etc.**, describe guidelines to confirm the physical and operational existence of the e-seal generators and the legal existence of the e-seal generators. |
| 2.3 | Format and Matters to be Specified in Electronic Certificates for e-Seal | - Describes the format of electronic certificates for e-Seal<br>- Describes the direction to develop a **common certificate policy OID system** |
| 2.4 | Standards for Management of Private Keys of Certification Authorities | - Regarding the management of private keys by the certification authorities, the **technical standards for HSMs** are described in the direction shown in the implementation guidelines, etc. |
| 2.5 | Standards for Management of Private Keys of e-Seal Generators | |
| 2.6 | Process When Generating a Large Number of e-Seal | |
| 2.7 | Use Authentication with the Remote e-Seal Method | |
| 2.8 | Revocation Request of Electronic Certificates for e-Seal | - Describes when **the certification authority can make revocation requests** in addition to requests from the e-seal generator. |
| Conclusion | | |

* Main revisions are indicated in red

Fig. 5 Main revisions of "Guidelines on e-Seal"

# Chapter 4 Individual Discussion Points and Directions

## 4.1 Classification of e-Seal

(1) Discussion points

The "Guidelines on e-Seal" prescribe three levels [13] of measures to ensure the trustworthiness of data issuer confirmation. The point of discussion is whether to follow the concept of these levels.

Note that the Electronic Signatures Act focuses on "Certification Business" and defines "Certification Business," "Specific Certification Business," [14] and "Certified Certification Business."

(2) Directionality

The "Assurance level of e-Seal" [15] is divided into two 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 certified by the Minister for Internal Affairs and Communications (e.g., for data exchanged between companies on a routine basis), and (2) Assurance level that is guaranteed by certification business for e-Seal certified by the Minister for Internal Affairs and Communications, promising a high degree of confidence concerning the source and integrity of the electronic data bearing the e-seal (e.g., qualification certificate for professional services that are considered exclusive monopoly services).

Fig. 6 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.

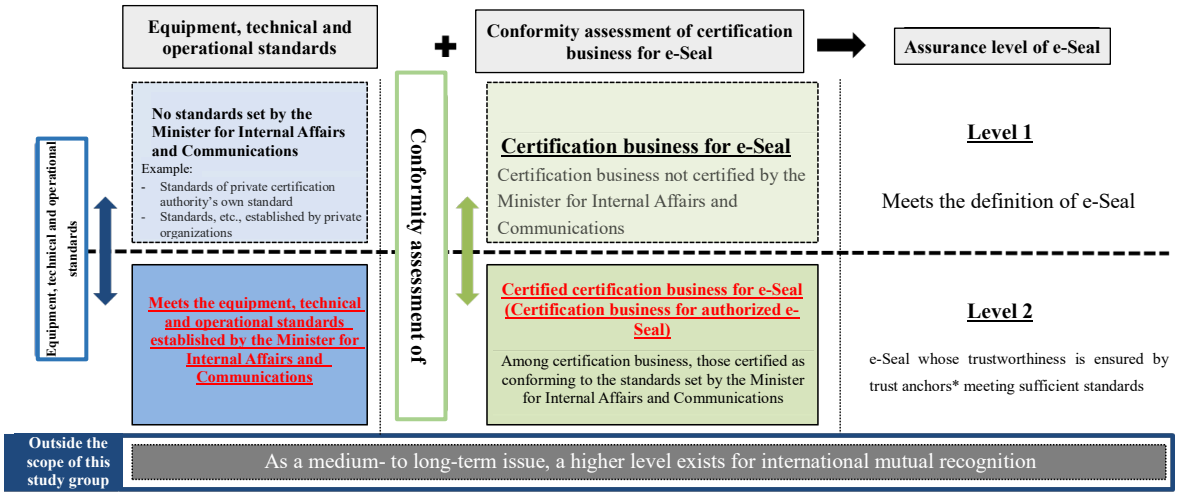
In addition, the members stated the importance of discussing level classifications from the

[13] The "Guidelines on e-Seal" provide a level classification for e-Seal: Level 1: e-Seal that satisfy the definition of an e-seal; Level 2: e-Seal that meet certain technical standards; and Level 3: e-Seal that meet Level 2 with reliability that is guaranteed by a trust anchor that meets proper standards.

[14] The Electronic Signatures Act defines "Certification Business" as the business of certifying, at the request of the user who has issued the electronic signature or another person using the business, that the matters used to confirm the user as the person who has issued the electronic signature are pertinent to the relevant user. "Specific Certification Business" is defined as certification business performed for electronic signatures that conform to the standards prescribed by the ordinance of the competent ministry as services that can only be performed by the principal in accordance with the method used. "Certified Certification Business" refers to services offered by a person who intends to engage in specific certification business, is recognized as conforming to the standards prescribed by the ordinance of the competent ministry, and may be certified by the competent minister.

[15] As a future issue, it is necessary to consider requirements for "Qualified e-seal generation devices" at a higher level, with a view to Common Criteria Recognition with other countries. However, the current level classification is focused on "Certification business for e-Seal."

viewpoint of introduction cost for organizations that generate e-Seal and that attention should be given to ensuring that user companies easily understand the organization of these level classifications. Based on this point, promoting public awareness of the system can be considered appropriate.




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

Fig. 6 Assurance level of e-Seal

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

The "Guidelines on e-Seal" stipulate that the scope of organizations to which electronic certificates for e-Seal[16] are issued should include "Corporates, individuals (assumed to be mainly sole proprietors), associations/foundations without legal capacity to hold rights, and other voluntary organizations, etc.," discussions were held on whether to maintain this arrangement.

### 4.2.1 Identifiers for Uniquely Identifying Organizations (Organization Identifiers)

(1) Discussion points

Organizations to which electronic certificates for e-Seal are issued need an identifier that uniquely identifies the organization. The point of discussion will be how to set the identifier.

(2) Directionality

The study group proposed using a combination of internationally used prefixes[17,18] and the existing number system issued by public institutions as identifiers for electronic certificates for

[16] An example of an electronic certificate for e-Seal is shown in "(Reference) Example of items to be included in electronic certificates for e-Seal (ITU-T X.509) (Image)."

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

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

e-Seal concerning certification. Based on this, for corporates etc., the prefix "NTRJP" is combined with the existing "Corporate Number" to configure the organization identifier[19]. While electronic certificates for e-Seal concerning certification must include at least one organization identifier using the number system issued by a public institution, it is possible to include an additional organization identifier using the Legal Entity Identifier (LEI)[20] or the private enterprise code described below. (Fig. 7)

**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 digital certificates is defined in ISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificates.

Fig. 7 Organization identifiers used for electronic certificates for e-Seal of the certification business for authorized e-Seal with assurance level 2

In addition, non-certified electronic certificates for e-Seal are not required to use organization identifiers using the number system issued by a public institution. They may only use the number system provided by private enterprises. Furthermore, as with electronic certificates for e-Seal concerning certification, multiple numbering systems may be used. The prefix used in organization identifiers based on the private enterprise number system should be determined independently by Japan. In consideration of international interoperability, the "Guidelines on e-Seal" and other documents recommended using "●●:JP" (where "●●" is the identifier prefix). (Fig. 8)

[19] The prefix "GOVJP" can be used by government agencies or local governments to assign e-Seal concerning certification.
[20] The format for storing LEIs in electronic certificates for e-Seal is defined in ISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificates.

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 ublicly-S/MIME Certificates Version 1.0.0.
*4: The method of storing LEIs in the extended area of digital 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 certification business for e-Seal with assurance level 1

4.2.2 Handling of "Sole Proprietors"

(1) Discussion points

Regarding the handling of "Sole proprietors," the point of discussion is whether it is possible to utilize the "Sole proprietor number system" and the Qualified Invoicing Business Registration Number described in the Priority Policy Program as identifiers for "sole proprietors."

(2) Directionality

The "Sole proprietor number system" described in the Priority Policy Program is currently under consideration by the Digital Agency concerning using the sole proprietor management number assigned in the GbizID.

In the case of sole proprietors, the information regarding the Qualified Invoicing Business Registration Number available on the public website is limited to the "date of registration," "registration number," and "name," meaning there is no reliable way of distinguishing between sole proprietors with the same first and last names.

Furthermore, the issue of how to identify tax-exempt sole proprietors remains even if the Qualified Invoicing Business Registration Number is used as an identifier.

Therefore, there will be no immediate conclusion on the identifier to identify sole proprietors during this fiscal year, and will not include sole proprietors under the issuance of electronic

certificates for certification business for authorized e-Seal of assurance level 2. The status of the Digital Agency's study of the "Sole proprietor number system" will be under close watch and an issue for further consideration.

To be covered by the certification system, sole proprietors must have an official number system that can be used as an identifier. However, outside the certification system's framework, sole proprietors can be eligible to be issued electronic certificates for e-Seal since private codes may be used if the certification system does not cover them.

4.2.3 Handling of "Business Office or Sales Office, etc." of Corporates, etc.

(1) Discussion points

The "Guidelines on e-Seal" state that "Although there is a certain level of need for business offices, sales offices, branch offices, departments, persons in charge (individuals without the declaration of intent), and equipment within an organization to be eligible for issuance of electronic certificates for e-Seal, it is difficult for the certification authority to confirm their existence accurately, etc. Therefore, they can be listed in the extended area, an optional field in electronic certificates for e-Seal." Discussions were held on whether to maintain this arrangement.

(2) Directionality

Although business offices, sales offices, etc., can be entities utilizing e-Seal, it is difficult for the certification authority to confirm their existence accurately. Therefore, the "Guidelines on e-Seal" arrangement should be maintained. Business offices, sales offices, etc., will be listed in the extended area, an optional field in electronic certificates for e-Seal.

## 4.3 Method of Verifying the Existence and Application Intention of the e-Seal Generator

(1) Discussion points

The "Guidelines on e-Seal" state that "It is assumed that a Certificate of Registration or third-party institution database, etc., is used" to confirm the existence of the e-seal generator, and that "It is assumed that electronic signature-Sealignature, etc. are used" to confirm the applicant's intention to apply. Discussions were held on whether to maintain this arrangement.

(2) Directionality

Extended Validation (EV) certificates are similar to electronic certificates for e-Seal in that they confirm the organization and issue certificates. Following the CA/Browser Forum guidelines, etc.[21], confirming the existence of the organization in the certificate requires three

[21] Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.8.0,

points: (1) confirmation of legal existence, (2) confirmation of physical existence, and (3) confirmation of operational existence. We believe it is appropriate to organize electronic certificates for e-Seal similarly.

Based on this, the following is an example of a method to confirm the existence of the e-seal generator and their intention to apply, referring to the CA/Browser Forum guidelines, etc.[22] (Fig. 9 ~ Fig. 12)

| 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. 9 Image explaining the method of verifying the existence of the e-seal generator and the information to be stored in an electronic certificate by 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><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. 10 Image explaining the method of verifying the application intent of the e-seal generator of the certification business for authorized e-Seal of assurance level 2

| Classification of e-seal generator | Confirm the existence of e-seal generator |
|---|---|
| **- 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. 11 Image explaining the method of verifying the existence of the e-seal generator and the information to be stored in an electronic certificate by the certification business for e-seal with assurance level 1

CA/Browser Forum, 30 November, 2022

[22]Because the use of the corporate base registry may be considered in confirming the existence of a legal entity. The status of the corporate base registry should also be monitored closely.

| Classification of e-seal generator | 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 | 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. 12 Image explaining the method of verifying the application intent of the e-seal generator by the certification businesses for assurance Level 1 e-Seal

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

(1) Discussion points

The "Guidelines on e-Seal" stipulate that the format for electronic certificates for e-Seal will use "ITU-T X.509," and the details to be mentioned in electronic certificates for e-Seal will include the "Official name of the organization to which the certificate is issued, an identifier that can uniquely identify the organization, validity period, public key, signature algorithm, issuer of the electronic certificate for e-seal, information that can identify the e-seal level, and other attribute information (sales offices, business office, equipment, etc.)." Discussions were held on whether to maintain this arrangement.

It is essential that electronic certificates for "electronic signatures" and electronic certificates for "e-Seal" are distinguishable in a machine-readable format. This may be achieved by using a common certificate policy OID (Object IDentifier) system. In this case, the point of discussion was how to develop a common certificate policy OID system since distinguishable information includes the distinction between electronic signatures and e-Seal, whether the e-seal certification business is certified, and the distinction between local and remote e-Seal.

(2) Directionality

While maintaining the arrangement in the "Guidelines on e-Seal," in principle, the study group concluded that it would be appropriate to develop a common certificate policy OID system from the viewpoint of international interoperability and to make electronic certificates for "electronic signatures" and "e-Seal" machine-readable. Specific details of the common certificate policy OID system will be considered in time for the certification system to begin operation.

Regarding the common certificate policy OID system, the members discussed the importance of a single private key to enable issuing multiple certificates to reduce the operation costs of certification authorities.

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

(1) Discussion points

The "Guidelines on e-Seal" states that "the provisions of the Electronic Signatures Act (equivalent to FIPS 140-1 Level 3) shall apply" to the management of private keys by certification authorities, and "It is assumed that the technical standards for HSMs will be modernized (equivalent to FIPS140-2 level 3), and the level to be kept in mind is equivalent to FIPS140-2 level 3 or ISO/IEC 15408 EAL4+ (protection profile requires separate consideration)."

If technical standards such as the Federal Information Processing Standards (FIPS) are included in the "Guidelines on e-Seal," there will be a need to revise the guidelines following technological advances. Discussions were held on how to establish equipment, technical and operational standards.

(2) Directionality

It is appropriate to maintain the concept prescribed in the "Guidelines on e-Seal," which essentially applies the provisions of the Electronic Signatures Act to the management of private keys by certification authorities. Furthermore, it is preferable to refer to the timestamp certification system, etc., when discussing the details of the implementation guidelines.

Given the technological advances, the technical, equipment, and operational standards, including the FIPS standards that must satisfy the technical standards for HSMs, will change. Therefore, it would be appropriate to establish them separately from the "Guidelines on e-Seal" so that they can be reviewed flexibly in consideration of international trends, etc., and to stipulate the "Guidelines on e-Seal" concerning these standards.

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

(1) Discussion points

The "Guidelines on e-Seal" states that the management of private keys by e-seal generators "shall be left to the organization, etc., to which the e-seal is issued." Discussions were held on whether to maintain this arrangement.

(2) Directionality

Regarding the management of private keys by e-seal generators, it is appropriate to maintain the provisions of the "Guidelines on e-Seal" and have the certification authority explain to e-seal generators the importance of private key management and that the responsibility for managing the private keys of e-seal generators lies with the e-seal generators.

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

(1) Discussion points

Discussions were held on whether to allow e-Seal for certification by the Minister for Internal Affairs and Communications to be granted to multiple documents simultaneously.

(2) Directionality

It is anticipated that there will be a need to mechanically and automatically grant e-Seal to multiple electronic documents simultaneously. Hence, based on the direction indicated in the "Guidelines on e-Seal," e-Seal for certification by the Minister for Internal Affairs and Communications may be granted to multiple documents simultaneously.

## 4.8 Remote e-Seal

(1) Discussion points

The "Analysis of cases where e-Seal are expected to be utilized (2nd)," conducted as part of the study group's stakeholder survey, indicated the need for remote e-Seal, which allow users to use e-Seal easily. Discussions were held on how to position remote e-Seal in the certification system.

(2) Directionality

Although there are some differences between remote signatures and remote e-Seal, such as the latter's ability to assign a large number of e-Seal to multiple electronic documents on a system, the two have many technical similarities, making it necessary to proceed with the study of remote e-Seal based on the study of remote signatures.

Discussions on remote signatures, including issues related to remote signature generators, are underway at the Digital Agency. Close attention should be paid to these discussions when studying the e-seal certification system.

Therefore, regulations for "remote e-seal generators" will continue to be the subject of further study, and discussions at this study group focused on issues concerning "certification authorities" while also considering the study of remote signatures[23].

[23] The Ministry of Internal Affairs and Communications (MIC), the Ministry of Justice (MOJ), and the Ministry of Economy, Trade and Industry (METI), which were the competent ministries for the Electronic Signatures Act at the time, announced the position of remote signatures under the Electronic Signatures Act at the Working Group for Growth Strategy (10th) of the Council for Promotion of Regulatory Reform on May 12, 2020. "Remote e-Seal" will be organized in the same manner, and those that meet the definition of "e-Seal" will be considered as "e-Seal" under the certification system.
https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200512/200512seicho04.pdf

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

(1) Discussion points

The "Guidelines on e-Seal" state that only persons who can request the issuance of electronic certificates for e-Seal can request revocation. Discussions were held on whether the certification authority can revoke electronic certificates for e-Seal in certain cases.

(2) Directionality

Certified certification businesses based on the Electronic Signatures Act include cases in which the certification authority can revoke an electronic certificate, such as "when a factual discrepancy is discovered in the details recorded in the electronic certificate[24]" or "when there is a possibility that the user signature code has been compromised.[25]" Even in the case of e-Seal, the certification authority can invalidate electronic certificates for e-Seal.

# Chapter 5 Issues to be Considered in the Future

## 5.1 Main Matters to be Discussed Before the Certification System Begins Operation

Based on the discussions of this study group, the "Guidelines on e-Seal" (formulated by MIC in June 2021) will be revised, and a certification system for e-Seal will be established through a notification from MIC. Implementation guidelines for establishing this system will be considered from the next fiscal year onwards, and the following points, in particular, will be considered based on the discussions of the study group.

(1) Establishment of technical, equipment, and operational standards

Under the certification system for e-Seal by the Minister for Internal Affairs and Communications, it would be appropriate for MIC to establish technical, equipment, and operational standards for e-Seal in advance, and when an application for certification by the Minister for Internal Affairs and Communications is submitted, to evaluate whether the certification business pertaining to the application conforms to these standards. Therefore, when formulating implementation guidelines, MIC will also consider technical, equipment, and operational standards for e-Seal [26].

(2) Optimization of conformity assessment using the certification system of the Electronic

[24] See Article 6, Item (10) of the ordinance to enforce the Act on Electronic Signatures and Certification Business.

[25] See Article 8, Item (3) of the Guidelines Pertaining to Accreditation in Specific Certification Business under the Act on Electronic Signatures and Certification Business.

[26] As mentioned in "4.5 Standards for Management of Private Keys of Certification Authorities," while the "Guidelines on e-Seal" do not include technical standards for HSMs, it can be used to refer to the technical, equipment, and operational standards for e-Seal.

Signatures Act

In establishing a certification system for e-Seal by the Minister for Internal Affairs and Communications, it should be known that the costs paid by certification authorities to obtain certification may be passed on to the price of the services. Therefore, MIC will continue to consider ways to reduce this cost. Specifically, MIC will consider integrating the certification system under the Electronic Signatures Act when formulating the implementation guidelines.

(3) Organizing the minimum details that should be included in CP/CPS

The discussions of the study group confirmed the necessity of specifically organizing the minimum details to be included in the CP/CPS, which are the operating regulations of the certification authority, including the method of verifying the existence and application intention of the organization, etc., at the certification authority, and the procedure for revocation request and verifying the status of revocation of electronic certificates for e-Seal from the competent certification authority. From this point of view, it is necessary to consider the minimum items that should be included in the CP/CPS, in conjunction with the formulation of implementation guidelines.

(4) Development of Common Certificate Policy OID System

The discussions of the study group included the need to consider using a common certificate policy OID to allow the issuance of electronic certificates for "electronic signatures" and "e-Seal" from the private key of a single certification authority, from the perspective of reducing operation costs at certification authorities. Including this, it would be appropriate for the Digital Agency and MIC to cooperate in considering the development of a common certificate policy OID system in conjunction with the formulation of implementation guidelines.

In addition to considering the matters mentioned above, from next fiscal year onwards, MIC will monitor the status of e-seal promotion regularly to identify any disparities from the assumptions made by this study group, issues in system operation, user needs, etc., and promote initiatives to spread the system.

## 5.2 Efforts to Promote e-Seal

To promote e-Seal in society, those assigning e-Seal must choose e-Seal for use based on their business judgment. For this reason, it is important to educate[27] the public and raise awareness that (1) Costs such as labor costs that are reduced due to increased digitalization through the use of e-Seal exceed the costs required to use e-Seal, and (2) In addition to the quantitative effects described above, the use of e-Seal encourages safe and secure data

[27] Compared to electronic signatures, which indicate the intention of the signatory, e-Seal, which are expected to be issued in large numbers, are expected to work in economies of scale. It is important to take these differences into consideration and effectively raise awareness of e-Seal.

distribution.

In doing so, it is important to broaden understanding of the relationship between the level of trustworthiness that is ensured by assigning an e-seal and the cost required to achieve it, based on the concept of "Assurance Level of e-Seal."

In addition, to spread the effectiveness of e-Seal throughout society, it is necessary to improve literacy regarding e-Seal and other trust services since the ability of recipients of e-Seal to be able to verify them properly is a prerequisite[28].

From this perspective, the study group analyzed the quantitative and qualitative effects of using e-Seal after citing cases of e-Seal being used for construction-related documents[29] and support work reports for office equipment.

In analyzing cases where e-Seal are used in construction-related documents, an estimate was made, under certain assumptions, of the benefits of using e-Seal (e.g., reduction in labor costs for document verification) and the costs associated with introducing e-Seal (e.g., service contracts), from the perspective of both the party assigning the e-Seal and the party verifying the e-Seal.

According to this estimate, the quantitative effect of reducing labor costs involved in verifying the issuer of a document, printing it, mailing it, etc., can reduce the total cost incurred in the conventional process by approximately two-thirds. The study group also concluded that the use of e-Seal can encourage safe and secure data distribution.

In the case of support work reports for office equipment (Fig. 13), the study group conducted trial calculations based on an actual case at Otsuka Shokai, confirming the quantitative effect of reducing the cost of copier paper, etc., in reducing the total cost incurred in the conventional process by approximately 40%, and improved reliability of electronic data and the associated increase in customer satisfaction through the use of e-Seal, which ensures safe and secure data distribution.

[28] Technical aspects concerning the verification of e-Seal are compiled in the "Digital Signature Verification Guidelines" (NPO Japan Network Security Association Electronic Signature Working Group). The efforts of these private organizations should also be referred to.
https://www.jnsa.org/result/e-signature/2021/

[29] The case study analysis of the study group considered the use of e-Seal with assurance level 2 with respect to various construction-related documents submitted for public works.

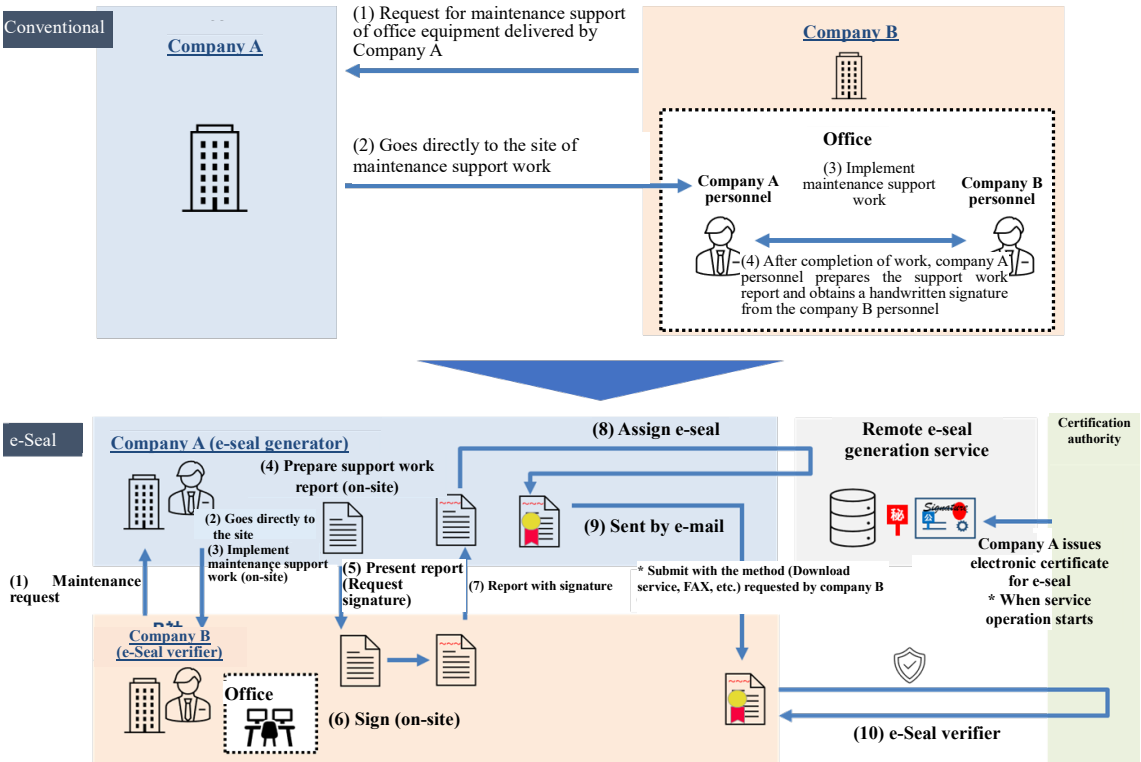



Fig. 13 Image showing the use of e-seal (Support work report)

e-Seal are expected to be used in situations other than those mentioned above, and cases that may require using e-Seal of assurance level 2 will emerge in the future, further promoting e-Seal.

Thus, the Digital Agency and MIC must continue promoting the effectiveness of trust services such as e-Seal in promoting DX and safe and secure data distribution in collaboration with related ministries and agencies.

## 5.3 Possibility of Using e-Seal in International Data Distribution

The study group discussed cases where e-Seal had been used for carbon footprint and surveyed "The system for screening, certification, and registration of user companies on the international data collaborative platform Catena-X/Cofinity-X and e-Seal" from the perspective of collecting materials to consider the possibility of utilizing trust services in the medium to long term.

Regarding carbon footprint, Europe is considering the "European Battery Regulation" regarding storage batteries, which is expected to make the carbon footprint of storage batteries mandatory from 2024 onwards. In the future, Japanese companies that deliver storage batteries and related components to Europe may also be required to comply with the regulations[30].

[30] Ministry of Internal Affairs and Communications, Document 2-3 Analysis of cases where e-Seal are

In this case, analysis, since the supply chain for each product, including storage batteries, is comprised of suppliers from various countries, with Japan sometimes acting as a supplier (party assigning the e-Seal) and sometimes as a manufacturer (party verifying the e-Seal), the necessity of considering the use of e-Seal from the perspective of both the party that assigns the e-Seal and the party that verifies the e-Seal was pointed out.

The survey on "The system for screening, certification, and registration of user companies on the international data collaborative platform Catena-X/Cofinity-X and e-Seal" revealed a case in which a Japanese company was forced to log in to the European data collaborative platform using the ID of a European corporate because there is no legal system or trust platform in Japan equivalent to the EU's eIDAS regulation or Gaia-X DCH.

The survey noted that while the creation of the certification system for e-Seal by the Minister for Internal Affairs and Communications was a major step forward, there is a need to continue studying the development of a trust platform that allows interoperability and interconnectivity between Europe and Japan.

In addition to the above discussion, the study group identified the need to strategically consider system design, including establishing a comprehensive trust platform in Japan and a method of publicizing certification while referencing the situation in Europe and the United States. The use of trust services in international data distribution is consistent with the concept of DFFT, etc., advocated by Japan, including services other than the international data collaborative platform mentioned above. Therefore, the Digital Agency and MIC must strategically consider using trust services, taking into account international standards and specifications.

expected to be utilized (1) (Carbon footprint), study group on e-Seal (2nd), p. 2

## Conclusion

"Facilitation of Cross-Border Data Flows and Data Free Flow with Trust" was one of the six agendas discussed at the G7 Digital and Tech Ministers' Meeting in Takasaki, Gunma, held on April 29 and 30, 2023, and its importance has been strongly recognized.

Since electronic data has become an indispensable part of people's lives, promoting data distribution while ensuring safety and security is essential for digitalization to progress.

While "Trust services," such as "e-Seal," are gradually gaining traction in Japan, it is still far from being fully utilized. The establishment of the "Certification System for e-Seal by the Minister for Internal Affairs and Communications," which is the outcome of the discussions in this study group, can be considered a major step toward creating a foundation for the safe and secure distribution of electronic data in Japan.

In the future, discussions about establishing a certification system will take shape based on this report. The Digital Agency and MIC are expected to continue to work closely together to examine the current state of trust services in Japan from a broader perspective.

## (Reference) Example of items to be included in electronic certificates for e-Seal (ITU-T X.509) (Image)

An example of how to describe an electronic certificate for e-seal (ITU-T X.509) is shown in Fig. 14. Example of displaying the certificate path of an electronic certificate for e-seal is shown in Fig. 15[31].

(Supplement: Understanding Fig.14)

The relationship between the matters described in the text of this draft report and the description in Fig. 14 is as follows.

(1) The "organization identifier" (issuer of the electronic certificate for e-seal) discussed in 4.2.1 is listed in the "Issuer name" column of the basic area.

(2) The "organization identifier" (e-seal generator) discussed in 4.2.1 is listed in the "Subject name" column of the basic area.

(3) The "business office, sales office, etc." discussed in 4.2.3 is listed in the "Subject alias" column of the extended area.

(4) The "Common Certificate Policy OID" discussed in 4.4 is listed in the "Certificate policy" column of the extended area.

| | 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) (1) |
| | 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) (2) |
| | 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 (Image)

[31] The electronic certificates for e-seal is also electronically signed by a certification authority, making it possible to verify the issuer of the electronic certificate for e-seal and detect falsification of information.

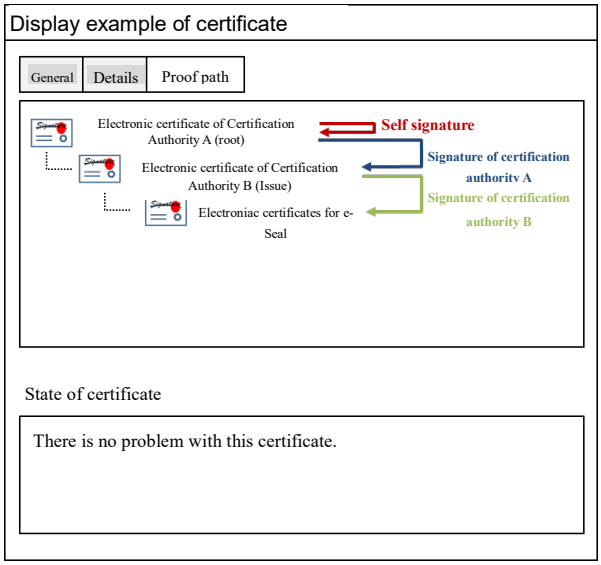



Fig. 15 Example of displaying the certificate path of an electronic certificate for e-seal