Lower Certificate Authority of IoTConnectUp Private Certificate Authority Certificate Policy

Ver.1.03

September 12, 2022

FUJIFILM Business Innovation Corp.
Enterprise Document Solutions
Business Group

Revision history		
Revision	Date	Detail
1.00	2020/2/1	Created
1.01	2020/5/11	Added target user to “3.1.5 Uniqueness of names”
1.02	2022/1/7	Changed corporate name to FUJIFILM Business Innovation Corp.
1.03	2022/9/12	Changed OID

Table of contents

1. INTRODUCTION

1.1 Overview

The Lower Certificate Authority of IoTConnectUp Private Certificate Authority certificate policy (this CP) indicates the purpose of use, the scope of application, the user procedure, and defines the policy regarding certificates issued by lower certificate authority (each CA) of IoTConnectUp PCA (this CA) operated by the Enterprise Document Solutions Business Group (EDS) of FUJIFILM Business Innovation Corp. The procedures for maintaining the operation of each CA are stipulated in the SECOM Digital Certification Infrastructure Certification Practice Statement (CPS).

The lower certificate authority of IoTConnectUp PCA has been issued a CA certificate by IoTConnectUp PCA.
The validity period of the certificate issued by the lower certificate authority of IoTConnectUp PCA shall be within 3 years.

The certificate issued by each CA is used for server authentication and encryption of information in the communication path. In addition, the issue target is determined by the Terms of Service of the Lower Certificate Authority of IoTConnectUp Private Certificate Authority. A person who receives a certificate from each CA need to evaluate his / her purpose of use against this CP, Terms of Service, and CPS and accept them before receiving the certificate.

If the content of this CP conflicts with the content of the Terms of Service or CPS, the Terms of Service, this CP, and CPS shall be applied in that order. In addition, if there is a separate contract between EDS and an organization that has a contractual relationship, the document such as the contract takes precedence over the Terms of Service, this CP, and CPS.

This CP shall be revised as necessary to reflect the technical and operational developments and improvements related to each CA.

This CP complies with RFC3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, which the IETF advocates as a framework for operating certificate authorities.

1.2 Document name and identification

The official name of this CP is “Lower Certificate Authority of IoTConnectUp Private Certificate Authority certificate policy”.
This CP and target certificate authorities are identified by the OID shown in the “Table **1.2-1** OID (This CP)”.

On September 12, 2022, OID 1.3.6.1.4.1.297.1.5.1.30 was changed to 1.3.6.1.4.1.297.1.5.1.38.

Table 1.2-1 OID (This CP)

CP	OID
Lower Certificate Authority of IoTConnectUp Private Certificate Authority certificate policy	1.3.6.1.4.1.297.1.5.1.29
IoTConnectUp Private Endorsement CA	1.3.6.1.4.1.297.1.5.1.38
IoTConnectUp Private Endorsement TEST CA	1.3.6.1.4.1.297.1.5.1.38
IoTConnectUp Private Product CA	1.3.6.1.4.1.297.1.5.1.38
IoTConnectUp Private Internal Test CA	1.3.6.1.4.1.297.1.5.1.38

The OID of CPS related to this CP is shown in the"Table **1.2**-**2** OID (CPS)".

Table 1.2-2 OID (CPS)

CPS	OID
SECOM Digital Certification Infrastructure Certification Practice Statement	1.2.392.200091.100.401.1

1.3 PKI participants

1.3.1 Certification authorities

The CA issues certificates, revokes them, discloses CRLs (Certificate Revocation Lists), and maintains and manages repositories. The operating entity of the CA operated on the electronic authentication platform is EDS.

1.3.2 Registration authorities

RA is responsible for issuing certificates, confirming the existence of subscribers who apply for revocation, examining identity verification, issuing certificates, and registering for revocation.

1.3.3 Subscribers

A subscriber is an individual, corporation, or other organization that applies for a certificate to EDS. It also refers to individuals, corporations, and other organizations that conclude individual contracts such as sales consignment contracts with EDS, mediate application procedures, and manage servers and place certificates.

1.3.4 Relying parties

A relying party is an individual, legal entity or other organization that verifies the identity of the subscriber and the validity of the public key. It also refers to individuals, corporations, and other organizations that trust and use CPs and CPS for the purpose of performing encrypted communication with the Web server owned by the subscriber using such public key.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificate issued by each CA can be used for server authentication and data encryption in the communication path.

1.4.2 Prohibited certificate uses

The certificate issued by each CA shall not be used for anything other than server authentication and data encryption via the communication path.

1.5 Policy administration

1.5.1 Organization administering the document

EDS will maintain and manage this CP.

1.5.2 Contact person

The contact information for this CP is as follows.

FUJIFILM Business Innovation Corp.
Enterprise Document Solutions Business Group
220-0012 6-1 Minatomirai Nishi-ku Yokohama-shi, Kanagawa JAPN

1.5.3 Person determining cps suitability for the policy

EDS will determine the suitability of the contents of this CP.

1.5.4 CPS approval procedures

This CP will be created and modified and published in the repository with the approval of the EDS department.

1.6 Definitions and acronyms

Archive

Information acquired for the purpose of storing history for legal or other reasons.

Audit log

Operation history and access history of the certificate authority system recorded to check for access to the certificate authority system and the presence of unauthorized operations, etc.

Baseline Requirements

A document in which the CA / Browser Forum defines the basic requirements for issuing and managing certificates.

CA (Certification Authority)

A certificate authority that issues certificates, and refers to the entity that issues, renews, and revokes certificates, generates and protects CA private keys, and registers subscribers. In this CP, the issuing office (IA: Issuing)

Authority) is also included.

CAA (Certificate Authority Authorization)

A function that prevents unauthorized issuance of a certificate from an unintended certificate authority in the domain authority. This is done by describing the certificate authority information that can issue a certificate to the domain in the DNS record.

CA/Browser Forum

A non-profit organization organized by certificate authorities and Internet browser vendors to define and standardize certificate requirements.

CP (Certificate Policy)

A document that specifies matters related to a certificate, such as the type, use, and application procedure of the certificate issued by the CA.

CPS (Certification Practices Statement)

A document that stipulates the operation of CA, such as procedures and security standards for operating CA.

CRL (Certificate Revocation List)

A list of certificate information that has been revoked due to changes in the contents of the certificate, loss of the private key, etc. during the validity period of the certificate.

CT (Certificate Transparency)

A mechanism specified in RFC 6962 that registers and publishes certificate information in a log server in order to monitor and audit the issued certificate information.

Digital certificate

Electronic data that proves that the person listed holds a certain public key. The validity of the digital signature is guaranteed by the CA electronically signing.

Escrow

Depositing with a third party.

FIPS140-2

A security certification standard for cryptographic modules established by the National Institute of Standards and Technology (NIST) in the United States. It is defined from the lowest level 1 to the highest level 4.

Key pair

In public key cryptography, a key pair consisting of a private key and a public key.

OID (Object Identifier)

It is a framework for maintaining and managing the uniqueness of network interoperability and services, and is a number registered with an international registration organization that is unique among networks around the world.

OCSP (Online Certificate Status Protocol)

A protocol that provides certificate status information in real time.

PKI (Public Key Infrastructure)

A platform that uses cryptographic technology called public key cryptography to realize security technologies such as digital signatures, encryption, and authentication.

Private key

One of the key pairs used in public key cryptography, and the key held only by the person corresponding to the public key.

Public key

One of the key pairs used in public key cryptography, which corresponds to the private key and is open to the other party of the communication partner.

RA (Registration Authority)

In the business of CA, the entity that examines application information, registers information necessary for issuing certificates, requests certificate issuance from CA, etc.

Repository

A database that stores and publishes CA certificates and CRLs.

RFC3647 (Request for Comments 3647)

A document issued by the IETF (The Internet Engineering Task Force), an organization that stipulates technology standards related to the Internet, and a document that defines the CP / CPS framework.

RSA

One of the most popular public key cryptosystems.

SHA-1 (Secure Hash Algorithm 1)

One of the hash functions (summary functions) used for digital signatures. A hash function is an operational method that generates a fixed-length bit string from a given source text. The bit length is 160 bits. By comparing the hash values on the data transmitting side and the data receiving side, it is possible to detect whether the original text has been tampered with during communication.

SHA-256 (Secure Hash Algorithm 256)

One of the hash functions (summary functions) used for digital signatures. The bit length is 256 bits. By comparing the hash values on the data transmitting side and the data receiving side, it is possible to detect whether the original text has been tampered with during communication.

Timestamp

Data that records the date and time when the electronic file was created and the date and time when the system executed the process.

WebTrust for CA

Standards established by the American Institute of Certified Public Accountants (AICPA) and the Chartered Accountants Association of Canada (CICA) for internal control over the reliability of certificate authorities and the safety of electronic commerce, and the certification system for those standards.

WebTrust for Baseline Requirements

Auditing standards established by the American Institute of Certified Public Accountants (AICPA) and the Chartered Accountant Association of Canada (CICA) for examination and certificate provisions by certificate authorities when issuing SSL certificates.

WHOIS

A service that allows you to refer to information about IP addresses and domain name registrants on the Internet.

X.500

A series of computer network standards for distributed directory services on a network.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

EDS maintains the repository so that subscribers and relying parties can use CRL information 24 hours a day, 365 days a year. However, the repository may not be available temporarily due to maintenance.

2.2 Publication of certification information

EDS stores the following in a repository for online reference by subscribers and relying parties:

-CRL

-Certificate of this CA and each CA

-Latest this CA and CPS

- Other related information regarding the certificate issued by this CA or each CA

In addition, as other public information, a test site is prepared for vendors to perform verification.

2.3 Time and frequency of publication

This CP and CPS will be published in the repository for each change. The CRL contains revocation information processed in accordance with this CP and will be published in the repository each time it is issued. Also, certificates that have expired will be deleted from the CRL.

2.4 Access controls on repositories

Subscribers and relying parties can refer to the repository at any time. The protocols used to access the repository are HTTP (HyperText Transfer Protocol) and HTTPS (HTTP with SSL / TLS data encryption function added). The information in the repository is accessible through a common web interface.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The name of each CA, which is the issuer of the certificate, and the name of the subscriber, who is the issue target, are set according to the Distinguished Name (DN) format of X.500.

The certificate issued by this CA shall include the following information.

1. "Country name" (C) shall be JP.
2. "Organization name" (O) is the name of an organization consisting of a corporation, a company, or another corporation. For a sole proprietorship, the name of the business or the name of the individual shall be used.
3. The "organizational unit name" (OU) should be an optional entry field. The OU column is used to distinguish between different departments within an organization (eg, personnel, marketing, and development departments).
4. "Common Name" (CN) shall be the host name used by the Web server on which the certificate issued by this CA will be installed. For the device, use the identifier of the device on which the certificate is installed.

3.1.2 Need for names to be meaningful

The usefulness of the common name used for the certificate issued by each CA is the host name used in the DNS of the web server where the subscriber will install the certificate issued by each CA. For the device, use the identifier of the device on which the certificate is installed.

3.1.3 Anonymity or pseudonymity of subscribers

The organization name and common name of the certificate issued by each CA will not be registered anonymously or in a pseudonym.

3.1.4 Rules for interpreting various name forms

The rules for interpreting the various name formats follow the X.500 Series Distinguished Name Regulations.

3.1.5 Uniqueness of names

The Distinguished Name (DN) attribute described in the certificate issued by each CA shall be unique to the Web server, target user and device to be issued.

3.1.6 Recognition, authentication, and role of trademarks

EDS does not verify that you have intellectual property rights to the names listed in your certificate application. Subscribers must not apply to this CA for registered trademarks or related names of third parties. EDS will not arbitrate or resolve any dispute between a subscriber and a third party due to a registered trademark, etc. In addition, EDS has the

right to refuse a certificate application from a subscriber or revoke a issued certificate because of a dispute.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Proof that the subscriber owns the private key is performed by the following method.
Verify the signature of the Certificate Signing Request (hereinafter referred to as "CSR") and confirm that the CSR is signed with the private key corresponding to the public key.

3.2.2 Authentication of organization identity

EDS authenticates an organization by means of EDS-approved certificate issuance instructions, EDS-trusted third-party investigations or databases thereof, or any other method that EDS deems worthy of equivalent trust.

3.2.3 Authentication of individual identity

EDS authenticates individuals by means of EDS-approved certificate issuance instructions, EDS-trusted third-party investigations or databases thereof, or any other method that EDS deems worthy of equivalent trust.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

EDS confirms that the person making the application for the certificate has the legitimate authority to make the application by means of this CP "3.2.2 Authentication of organization identity" or "3.2.3 Authentication of individual identity" check. In addition, in the case of an application from a third party other than the subscriber, if the intention of the application cannot be confirmed directly to the subscriber, a power of attorney certifying that the third party is the agent of the subscriber is required.

* The subscriber in this section means an individual, corporation or other organization that uses the host name described in the common name of the certificate specified in "3.1.1 Types of names".

3.2.6 Criteria for interoperation

This CA has been issued a self-signed one-way mutual authentication certificate.

3.2.7 Domain authentication

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identity verification and authentication of the subscriber at the time of key renewal shall be the same as in "3.2 Initial identity validation".

3.3.2 Identification and authentication for re-key after revocation

It does not renew revoked certificates. The certificate application will be treated as a new one, and the identity verification and authentication of the subscriber will be the same as in "3.2 Initial identity verification".

3.4 Identification and authentication for revocation request

After accepting the revocation application from the homepage that only the subscriber can access, EDS confirms the identity of the subscriber and authenticates it.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A person who can apply for a certificate is EDS, an authorized person or a company based on other corporate customer organization-specific submission document standards, or an agent delegated by representatives of other corporations.

4.1.2 Enrollment process and responsibilities

When applying for the issuance of a certificate, the subscriber shall apply after accepting the contents of this CP, the Terms of Service, and the CPS. In addition, it must be ensured that the content of the application to each CA is accurate information.
To apply for a certificate, follow the "application procedure" posted on the website and submit the required documents to EDS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

After accepting the certificate application, EDS will perform confirmation based on this CP "3.2 Initial identity validation".

4.2.2 Approval or rejection of certificate applications

As a result of the examination, EDS will issue a certificate for the approved application, and notify the subscriber of the completion of the examination and the issuance of the certificate. If the application for the certificate is incomplete, the subscriber will be notified of the reason for the incompleteness and the resubmission of necessary documents.

4.2.3 Time to process certificate applications

EDS will promptly issue a certificate for the approved certificate application.

4.2.4 Check the CAA record

This CA confirms the CAA record at the time of reviewing the application information. The domain of this CA described in the CAA record shall be "iotconnectup.com".

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

EDS issues the certificate after the examination of the certificate application is completed and sets the certificate download settings on the homepage that only the subscriber can access. Alternatively, the certificate will be sent to the subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

EDS will notify the subscriber by e-mail that the certificate download settings have been completed on the homepage that only the subscriber can access. The subscriber can download the certificate after receiving the notification from this CA. Alternatively, the issuance notification is given by sending the certificate to the subscriber.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

It is assumed that the certificate is received when the subscriber downloads the certificate from the homepage accessible only to the subscriber. In addition, when the certificate is sent to the subscriber, it is assumed that the certificate has been received within one week after the certificate is sent, if there is no request from the subscriber such as an error in the description of the certificate.

4.4.2 Publication of the certificate by the CA

This CA does not disclose the certificate of the subscriber.

4.4.3 Notification of certificate issuance by the CA to other entities

EDS does not notify the certificate issuance to anyone other than the person registered at the time of certificate application.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber uses the private key and the certificate for server authentication and encryption of information in the communication path. The subscriber shall use the certificate and the corresponding private key only for the purposes approved by this CA. Do not use for any other purpose.

4.5.2 Relying party public key and certificate usage

The relying party shall use the certificate of this CA or each CA after understanding and accepting the contents of this CP and CPS. The relying party can use the certificate of this CA or each CA to verify the certificate of the subscriber.

4.6 Certificate renewal

Each CA recommends that the subscriber generate a new key pair when renewing the certificate.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of certificate issuance by the CA to subscribers

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

The certificate can be renewed when the validity period of the certificate expires. Revoked or expired certificates cannot be renewed.

You can apply for certificate renewal 90 days before the expiration date.

4.7.2 Who may request certification of a new public key

Same as “4.1.1 Who can submit a certificate application”.

4.7.3 Processing certificate re-keying requests

Same as “4.3.1 CA actions during certificate issuance”.

4.7.4 Notification of new certificate issuance to subscriber

Same as “4.3.2 Notification to subscriber by the CA of issuance of certificate”.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as “4.4.1 Conduct constituting certificate acceptance”.

4.7.6 Publication of the re-keyed certificate by the CA

Same as “4.4.2 Publication of the certificate by the CA”.

4.7.7 Notification of certificate issuance by the CA to other entities

Same as “4.4.3 Notification of certificate issuance by the CA to other entities”.

4.8 Certificate modification

If the information registered in the certificate needs to be changed, each CA will revoke the certificate and issue a new one.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Subscribers must promptly apply for certificate revocation to EDS in the event of the following reasons.

* When there is a change in the information on the certificate
* When the private key is compromised or is likely to be compromised due to theft, loss, leakage, unauthorized use, etc. of the private key
* If the contents of the certificate and the purpose of use are incorrect
* When you stop using the certificate

In addition, EDS can revoke the certificate of the subscriber at the discretion of EDS in the following cases.

* If you have not fulfilled the obligations under the Terms of Service, this CP, CPS, related contracts or laws.
* When it is determined that the private key of this CA or each CA has been compromised or may be compromised.
* When reasonable evidence is found that the private key of subscriber, this CA or each CA has been compromised and do not comply with the key size requirements of the algorithm type and criteria requirements, or that the certificate has been misused in other ways.
* When it is found out that the certificate has not been issued in accordance with this CP or CPS
* When it is found that the certificate has been refused or revoked by EDS due to breach of contract or other reasons.
* When other circumstances are found in which EDS determines that it needs to be revoked.

4.9.2 Who can request revocation

The person who can apply for the revocation of the certificate shall be EDS, an authorized person or a company based on other corporate customer organization-specific submission document standards, or an agent delegated by the representative of the other corporations.

4.9.3 Procedure for revocation request

The subscriber selects the relevant certificate information from the homepage that only the subscriber can access and applies for revocation.

4.9.4 Revocation request grace period

If the subscriber determines that the private key has been compromised or is likely to be compromised, he / she must promptly apply for revocation.

4.9.5 Time within which CA must process the revocation request

After receiving a valid revocation application, EDS will promptly process the certificate revocation and reflect the certificate information in the CRL.

4.9.6 Revocation checking requirement for relying parties

The URL of the CRL storage destination is described in the certificate issued by each CA.

CRLs can be accessed using a common web interface. Note that the CRL does not include expired certificate information.

The relying party must confirm the validity of the subscriber's certificate. The validity of the certificate is confirmed by the CRL posted on the repository site.

4.9.7 CRL/ARL issuance frequency

CRLs are renewed every 24 hours with or without revocation processing. If the certificate is revoked, the CRL will be renewed at that point.

4.9.8 Maximum latency for CRL/ARLs

The CRL issued by each CA will be immediately reflected in the repository.

4.9.9 On-line revocation/status checking availability

No stipulation.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re-key compromise

No stipulation.

4.9.13 Circumstances for suspension

Each CA does not suspend the certificate.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

Each CA manages the repository site so that the validity of the certificate can be confirmed 24 hours a day, 365 days a year. However, the repository site may not be available temporarily due to maintenance, etc.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

When terminating the use of this service, the subscriber must apply for the revocation of the certificate. If you do not apply for renewal of the certificate and the validity period of the certificate has expired, it will be terminated.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Each CA does not escrow the private key of the subscriber.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

This section is stipulated in CPS.

5.1.2 Physical access

This section is stipulated in CPS.

5.1.3 Power and air conditioning

This section is stipulated in CPS.

5.1.4 Water exposures

This section is stipulated in CPS.

5.1.5 Fire prevention and protection

This section is stipulated in CPS.

5.1.6 Media storage

This section is stipulated in CPS.

5.1.7 Waste disposal

This section is stipulated in CPS.

5.1.8 Off-site backup

This section is stipulated in CPS.

5.2 Procedural controls

5.2.1 Trusted roles

This section is stipulated in CPS.

5.2.2 Number of persons required per task

This section is stipulated in CPS.

5.2.3 Identification and authentication for each role

This section is stipulated in CPS.

5.2.4 Roles requiring separation of duties

This section is stipulated in CPS.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

This section is stipulated in CPS.

5.3.2 Background check procedures

This section is stipulated in CPS.

5.3.3 Training requirements

This section is stipulated in CPS.

5.3.4 Retraining frequency and requirements

This section is stipulated in CPS.

5.3.5 Job rotation frequency and sequence

This section is stipulated in CPS.

5.3.6 Sanctions for unauthorized actions

This section is stipulated in CPS.

5.3.7 Independent contractor requirements

This section is stipulated in CPS.

5.3.8 Documentation supplied to personnel

This section is stipulated in CPS.

5.4 Audit logging procedures

5.4.1 Types of events recorded

This section is stipulated in CPS.

5.4.2 Frequency of processing log

This section is stipulated in CPS.

5.4.3 Retention period for audit log

This section is stipulated in CPS.

5.4.4 Protection of audit log

This section is stipulated in CPS.

5.4.5 Audit log backup procedures

This section is stipulated in CPS.

5.4.6 Audit collection system

This section is stipulated in CPS.

5.4.7 Notification to event-causing subject

This section is stipulated in CPS.

5.4.8 Vulnerability assessments

This section is stipulated in CPS.

5.5 Records archival

5.5.1 Types of records archived

SECOM Trust Systems Co., Ltd. (SECOM) stores the following information as an archive in addition to the system logs related to this CA in CPS "5.4.1 Types of events recorded".

* Issued certificate and CRL
* Processing history related to CRL issuance
* CPS
* A document that regulates the business operation of a certificate authority created based on CPS
* Documents related to the consignment contract when outsourcing the certification work to another company
* Records and audit reports regarding the results of audits
* Application documents from subscribers

5.5.2 Retention period for archive

SECOM will store the archive for a minimum of 5 years.

5.5.3 Protection of archive

Archives should be kept in a facility restricted to access only by authorized persons.

5.5.4 Archive backup procedures

If there is a change in important data related to the system related to this CA, such as certificate issuance, revocation or CRL issuance, make a timely backup of the archive.

5.5.5 Requirements for time-stamping of records

EDS uses NTP (Network Time Protocol) to synchronize the time of the system related to this CA, and adds a time stamp to important information recorded in the system related to this CA.

5.5.6 Archive collection system

The archive collection system is included in the system functions related to this CA.

5.5.7 Procedures to obtain and verify archive information

The archive is obtained by an access authority from a secure vault, and the storage status of the medium is checked on a regular basis. If necessary, the archive will be duplicated on a new medium for the purpose of maintaining the integrity and confidentiality of the archive.

5.6 Key changeover

As a general rule, key pair renewal or certificate renewal of this CA shall be carried out before the validity period of this CA becomes shorter than the maximum validity period of the certificate issued to the subscriber.

If the validity period of this CA is shorter than the maximum validity period of the certificate issued to the subscriber, the validity period of the certificate issued to the subscriber will be changed so that it falls within the validity period of this CA.

The validity period of the private key of this CA is assumed to be 40 years.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

EDS will develop procedures for accidents and threats, including the following, so that the systems and operations related to this CA can be promptly restored in the event of an accident or compromise.

* Compromise of CA private key
* Damage or failure of hardware, software, data, etc.
* Disasters such as fires and earthquakes

5.7.2 Computing resources, software, and/or data are corrupted

If the hardware, software or data of the system related to this CA is damaged, EDS will promptly recover the system related to this CA by using the hardware, software or data stored for backup.

5.7.3 Entity private key compromise procedures

When EDS determines that the private key of this CA has been compromised or is likely to be compromised, or that the system operation related to this CA may be interrupted or stopped due to a disaster, etc., it will safely resume operations according to predetermined plans and procedures.

5.7.4 Business continuity capabilities after a disaster

EDS will take measures to restore the authentication infrastructure system as soon as possible, such as securing a substitute for the system related to this CA, securing backup data for recovery, and formulating recovery procedures so that recovery work can be carried out promptly in the event of an unforeseen situation.

5.8 CA or RA termination

If EDS terminates this CA, it will notify the subscriber and other related parties at least one month in advance based on the resolution of EDS. All certificates issued by this CA will expire prior to the termination of this CA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

In the authentication infrastructure system, a CA key pair is generated by a FIPS 140-2 level 3 compliant cryptographic device.

The key pair generation work is performed by operations by multiple authorized persons.

The subscriber's key pair is generated by the subscriber himself.

The Web server key pair generation method recommended by each CA is described on the EDS homepage.

6.1.2 Private key delivery to subscriber

The private key will not be issued by each CA.

6.1.3 Public key delivery to certificate issuer

The subscriber's public key can be issued to each CA online. The communication path at this time is encrypted by SSL / TLS.

6.1.4 CA public key delivery to relying parties

The relying party can obtain the public key of each CA by accessing the repository of each CA.

6.1.5 Key sizes

The key pair of each CA uses the RSA method and has a key length of 2048 bits.

For the key pair of the subscriber, the key length is 2048 bits by the RSA method.

Depending on the environment of the subscriber's Web server, etc., the certificate application will be accepted even if the key size is different by the RSA method.

6.1.6 Public key parameters generation and quality checking

The generation of the parameters of the public key of each CA and the verification of the strength of the parameters are performed using the functions implemented in the cryptographic device used for the key pair generation.

It does not specify the generation of public key parameters and quality inspection of the subscriber.

6.1.7 Key usage purposes

The uses of each CA and the key of the certificate issued by each CA are as follows.

Table 6.1-1 Key usage purposes

	Each CA	Certificate issued by each CA
digital Signature	—	yes
nonRepudiation	—	—
keyEncipherment	—	yes
dataEncipherment	—	—
keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Each CA's private key is generated, stored, and signed using a FIPS 140-2 Level 3 compliant encryption device.

The private key of the subscriber is not specified.

6.2.2 Private key multi-person control

Operations such as activation, deactivation, and backup of the private key of each CA are performed by multiple authorized persons in a secure environment.

Operations such as activation, deactivation, and backup of the subscriber's private key must be performed safely under the control of the subscriber.

6.2.3 Private key escrow

Each CA does not escrow the private key of each CA.

Each CA does not escrow the private key of the subscriber.

6.2.4 Private key backup

The backup of the private key of each CA is performed by multiple authorized persons in the secure room and is stored in the secure room in an encrypted state.

A backup of the subscriber's private key must be kept securely under the control of the subscriber.

6.2.5 Private key archival

Each CA does not archive the private key of each CA.

The private key of the subscriber is not specified.

6.2.6 Private key transfer into or from a cryptographic module

The transfer of the private key of each CA to or from the encryption device is performed in a secure room with the private key encrypted.

The private key of the subscriber is not specified.

6.2.7 Private key storage on cryptographic module

The private key of the CA operated on this electronic authentication platform is stored in the encryption device in an encrypted state.

The private key of the subscriber is not specified.

6.2.8 Method of activating private key

The activation of the private key of each CA is performed by multiple authorized persons in a secure room.

The private key of the subscriber is not specified.

6.2.9 Method of deactivating private key

The private key of each CA is deactivated by multiple authorized persons in a secure room.

The private key of the subscriber is not specified.

6.2.10 Method of destroying private key

The private key of each CA is destroyed by completely initializing or physically destroying it by multiple authorized persons. The same procedure is used for backup.

The private key of the subscriber is not specified.

6.2.11 Cryptographic Module Rating

The quality standards for cryptographic devices used in each CA are as described in this CP "6.2.1 Cryptographic module standards and controls".

The private key of the subscriber is not specified.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public key of each CA is as described in CPS "6.2.1 Cryptographic module standards and controls".

The private key of the subscriber is not specified.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of the private key and public key of each CA shall be 40 years or less.

The private key of the subscriber is not specified. The validity period of the subscriber's certificate issued by this CA is within 3 years.

6.4 Activation data

6.4.1 Activation data generation and installation

This section is stipulated in CPS.

6.4.2 Activation data protection

This section is stipulated in CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

This section is stipulated in CPS.

6.5.2 Computer security rating

This section is stipulated in CPS.

6.6 Life cycle technical controls

6.6.1 System development controls

This section is stipulated in CPS.

6.6.2 Security management controls

This section is stipulated in CPS.

6.6.3 Life cycle security controls

This section is stipulated in CPS.

6.7 Network security controls

This section is stipulated in CPS.

6.8 Time-stamping

This section is stipulated in CPS.

7. CERTIFICATE, CRL/ARL, AND OCSP PROFILES

7.1 Certificate profile

The certificate issued by each CA is RFC5280 compliant. The profile is shown in the following table.

Table 7.1-1 Lower Certificate Authority of IoTConnectUp Private Certificate Authority certificate profile

Field	Explanation
Version number	Version.3
Serial number	Unique number within the CA
Digital signature algorithm identifier	Identifier of the electronic signature algorithm used in this service
Issuer name	Information specified by each CA
Validity period	Certificate start and end dates
Username	User information
User's public key information	User's public key algorithm identifier and public key data
Extended field	Not specified

7.2 CRL/ARL profile

The CRL issued by each CA is RFC5280 compliant. The profile is shown in the following table.

Table 7.2-1 Lower Certificate Authority of IoTConnectUp Private Certificate Authority CRL/ARL profile

Field	Explanation
Version number	Version.2
Digital signature algorithm identifier	Identifier of the electronic signature algorithm used in each CA
Issuer name	CRL issuer information specified by each CA
Update date	CRL issuance date and time

Next update date	Next scheduled update date and time of CRL
Revocation list	The serial number of the revoked certificate and the date and time of revocation are listed.

7.3 OCSP profile

No stipulation.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This CA will conduct a timely audit to see if it is operating in accordance with each CP and CPS.

Matters concerning compliance audits conducted by this CA are stipulated in each CP and CPS.

8.1 Frequency or circumstances of assessment

EDS conducts a compliance audit at least once a year to determine whether the Service operates in compliance with the CP and CPS.

8.2 Identity/qualifications of assessor

Each CA's compliance audit is conducted by an auditor who is familiar with the CA's business.

8.3 Assessor’s relationship to assessed entity

The auditor selects an auditor who has no special interest in EDS.

8.4 Topics covered by assessment

The audit will be conducted on the operations related to the operation of each CA.

It may also be based on the WebTrust for CA Criteria for Certificate Authorities and the WebTrust for BR Criteria.

8.5 Actions taken as a result of deficiency

EDS will promptly take necessary corrective actions regarding the matters pointed out in the audit report.

8.6 Communication of results

The audit report will be reported to the Certification Service Improvement Committee. Audit reports are stored and managed so that only authorized ones can access them.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees for certificates issued by each CA will be specified separately.

9.2 Financial responsibility

EDS shall maintain a sufficient financial base to maintain the operation of each CA.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

This section is stipulated in CPS.

9.3.2 Information not within the scope of confidential information

This section is stipulated in CPS.

9.3.3 Responsibility to protect confidential information

This section is stipulated in CPS.

9.4 Privacy of personal information

This section is stipulated in CPS.

9.5 Intellectual property rights

The following works are property belonging to EDS.

* this CP

9.6 Representations and warranties

9.6.1 CA representations and warranties

EDS has the following obligations in carrying out the business of CA:

* Securely generate and manage CA private keys
* Accurate issuance, revocation and management of certificates based on applications from RA
* System operation and operation monitoring
* Issuing and publishing CRLs
* Maintaining the repository

9.6.2 RA representations and warranties

EDS has the following obligations in carrying out RA's business:

* Install and operate the registered terminal in a secure environment

* When issuing a certificate, perform an accurate examination such as confirmation of existence.

* Promptly and accurately give instructions such as certificate issuance and revocation.

9.6.3 Subscriber representations and warranties

The subscriber shall have the following obligations.

* Subscribers must provide accurate and complete information when applying for certificate issuance.

* If there is a change in the information, promptly notify EDS to that effect.

* Protect your private key from compromise.

* Use the certificate in accordance with the Terms of Service and this CP.

* If the subscriber determines that the private key corresponding to the public key described in the certificate has been compromised or is likely to be compromised, or if the registration information has been changed, the subscriber shall promptly apply for certificate revocation to EDS.

9.6.4 Relying party representations and warranties

The relying party shall have the following obligations:

* Check the validity of each CA's certificate.

* For the validity of the certificate used by the subscriber, check whether the certificate has expired and whether the certificate has been revoked from the CRL.

* It is the responsibility of the relying party to decide whether to trust the information of the subscriber.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

EDS is liable for any indirect, special, incidental or consequential damages arising in connection with the warranties set forth in this CP "9.6.1 CA representations and warranties" and "9.6.2 RA representations and warranties". And is not liable for any lost profits, data loss or other indirect or consequential damages.

9.8 Limitations of liability

Regarding the contents of this CP "9.6.1 CA representations and warranties" and "9.6.2 RA representations and warranties", EDS shall not be liable in the following cases:

* All damages caused by illegal acts, unauthorized use or negligence not caused by EDS

* Damage caused by the subscriber failing to fulfill his / her obligations

* Any damage caused by the subscriber's system

* Damage caused by defects, malfunctions, or other operations of the subscriber's environment (hardware, software)

* Damage caused by information published on certificates and CRLs for reasons not attributable to EDS

* Any damage caused by abnormal communication due to reasons that cannot be attributed to EDS.

* All damages such as transactional debts incurred in connection with the use of certificates

* Damage caused by improvements in hardware or software-based cryptographic algorithm decryption technology that exceed current expectations

* All damages caused by the suspension of operations of this CA due to natural disasters, earthquakes, eruptions, fires, tsunamis, floods, lightning strikes, wars, turmoil, terrorism and other force majeure.

9.9 Indemnities

EDS covers damages to the subscriber caused by the certificate up to the contract fee received. In addition, we do not take any responsibility other than that.

9.10 Term and termination

9.10.1 Term

This CP becomes effective with the approval of EDS.

This CP will not become invalid before the end specified in this CP "9.10.2 Termination".

9.10.2 Termination

This CP becomes invalid when EDS terminates each CA, except for the contents specified in "9.10.3 Effect of termination and survival".

9.10.3 Effect of termination and survival

Even if the subscriber terminates the use of the certificate, or even if the EDS terminates the service provision, the terms that should survive by its very nature will apply to the subscriber and each CA regardless of the reason for termination.

9.11 Individual notices and communications with participants

EDS will provide necessary notifications to subscribers and relying parties via homepage, e-mail or in writing.

9.12 Amendments

9.12.1 Procedure for amendment

This CP will be revised from time to time at the discretion of EDS and will come into effect with the approval of the Certification Service Improvement Committee.

9.12.2 Notification mechanism and period

If this CP is changed, the changed CP will be announced promptly to notify the concerned parties.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

If a dispute relating to a certificate issued by each CA is to be filed against EDS through legal proceedings including proceedings, arbitration, etc., EDS shall be notified in advance. The arbitration and courtrooms have exclusive jurisdiction over the dispute resolution body in Tokyo.

9.14 Governing law

The laws of Japan shall apply to disputes concerning the interpretation, validity and use of certificates of this CP and CPS.

9.15 Compliance with applicable law

Each CA shall comply with various domestic export regulations and handle cryptographic hardware and software.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

In providing this service, EDS comprehensively defines the obligations of the subscriber or relying party by this CP, Terms of Service, and CPS, and no other agreement, whether verbal or written, shall have effect.

9.16.2 Assignment

If EDS transfers the Services to a third party, it may transfer the obligations set forth in this CP, Terms of Service and CPS and other obligations.

9.16.3 Severability

Even if some provisions of this CP, Terms of Service, and CPS are invalid, the other provisions described in the document shall be valid.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.