Japanese Government Public Key Infrastructure (GPKI)

Application Certification Authority Certificate Policy and Certification Practice Statement

Issued　July 6th, 2007

Amended　May 25th, 2009

Approved by the Inter-ministerial Council of Government Information Systems

1. Introduction

This document is a translated text of "Japanese Government Public Key Infrastructure (GPKI) Application Certification Authority Certificate Policy and Certification Practice Statement (May 25th, 2009 Approved by the Inter-ministerial Council of Government Information Systems)" into English. Please refer to the original document for any sentence that is not clear.

This CP/CPS defines the operation policy related to certification services of the Application Certification Authority (hereinafter referred to as "Application CA") that issues server certificates and code signing certificates to implement encrypted communications between business servers of organizations including offices and ministries and signature on software.

This Application CA CP/CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices Framework.

1.1 Overview

The Application CA issues server certificates and code signing certificates to organizations including offices and ministries.

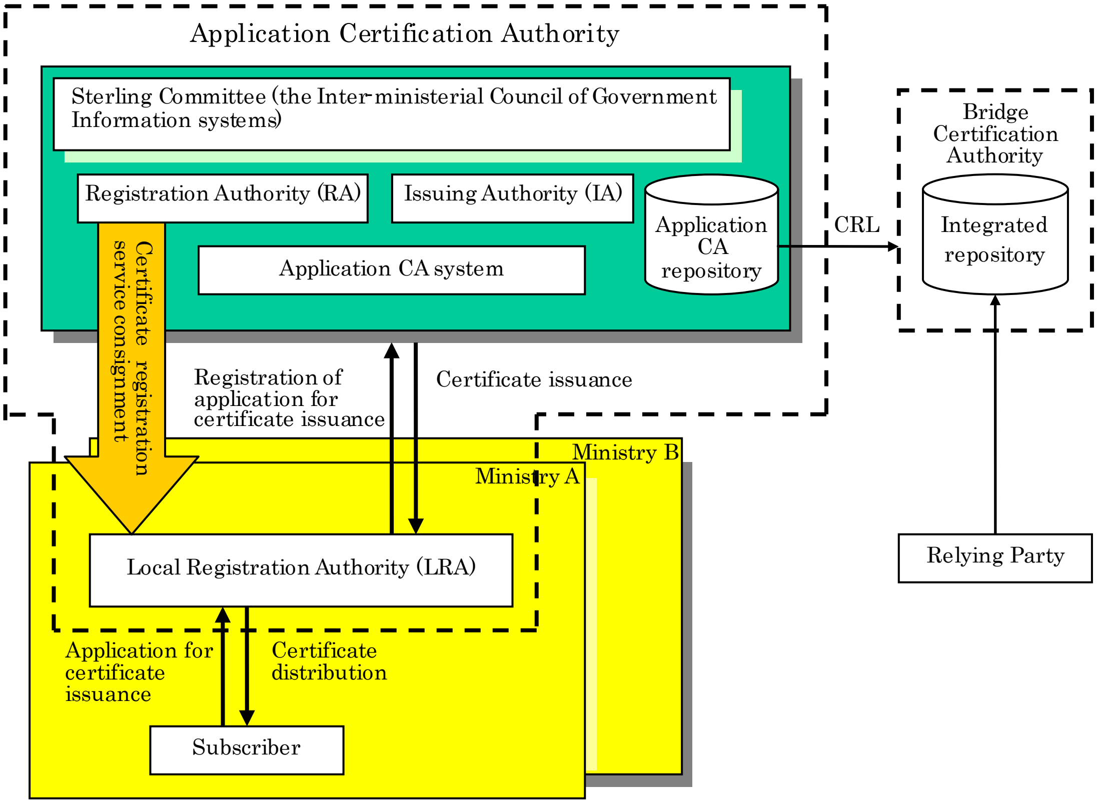
The Application CA does not assume the CP (Certificate Policy) and the CPS (Certification Practices Statement) to be independent but defines this CP/CPS as the operation policy related to the certification services of the Application CA.

1.2 Document name and identification

The certificate policy of the Application CA covers the certificate policy for the server certificate and the certificate policy for the code signing certificate of the Application CA. The identifiers of the policies are as follows:

- Server certificate policy: 0.2.440.100145.8.4.1.11.10
- Code signing certificate policy: 0.2.440.100145.8.4.1.1.20

1.3 PKI participants



Application Certification Authority
Sterling Committee (the Inter-ministerial Council of Government Information systems)
Registration Authority (RA)
Issuing Authority (IA)
Application CA repository
Application CA system
Certificate registration service consignment
CRL
Bridge Certification Authority
Integrated repository
Registration of application for certificate issuance
Certificate issuance
Ministry B
Ministry A
Local Registration Authority (LRA)
Relying Party
Application for certificate issuance
Certificate distribution
Subscriber

Fig. 1-1 Organization Diagram

1.3.1 Certification authorities

The Inter-Ministerial Council of Government Information Systems makes the decision concerning operations of the Application CA.

The role of the Governing Council in relation to Application CA operations shall be as follows:

- Decision concerning the CP/CPS of the Application CA
- Decision concerning action to CA private key compromise state
- Decision concerning action to emergencies such as occurrence of disasters
- Decision concerning establishment and abolishment of the Local Registration Authority (LRA)
- Decision concerning other important matters pertaining to operation of the Application CA

1.3.2 Issuing Authority (IA) and Registration Authority (RA)

Application CA director, IA key administrator, Reception personnel, reviewer perform operation services related to administration of the CA private key and establishment and abolishment of the LRA.

The general manager of the Information System Administration of the Government Information Systems Planning Division, Administrative Management Bureau, Ministry of Internal Affairs and Communications is Application CA director.

Application CA administrator, assistant Application CA administrator, senior IA operators, general IA operators, and audit log inspector perform operation services such as system operation, system maintenance and administration, and issuance, re-key, and revocation of certificates. The tasks of these personnel are defined in "5.2 Procedural Controls".

1.3.3 Local Registration Authority (LRA)

This organization is approved by the sterling committee and established for each office and ministry in principle. This organization accepts and review applications, form subscriber, related to issuance, re-key and revocation of certificates.

In this organization, LRA administrators, LRA operators, LRA reception personnel, and LRA reviewer are staffed. The tasks of these personnel are defined in "5.2 Procedural Controls".

1.3.4 Subscriber

The subscriber administers certificates issued from the Application CA, and uses the certificates in accordance with this CP/CPS.

1.3.5 Relying parties

The relying party who verifies a certificate checks the validity of the certificate of self-signed certificates, server certificates, and code signing certificates using the Certificate Revocation List (CRL) issued by the Application CA.

1.3.6 Other participants involved

No stipulation

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Server certificates are used for existence certification of servers used by offices and ministries and for encrypted communications. Server certificates shall remain valid for three years from the date on which they take effect.

Code signing certificates are used for signatures in software distributed to citizens and enterprises from offices and ministries. Code signing certificates shall remain valid for three years from the date on which they take effect.

1.4.2 Prohibited certificate uses

Certificates issued from the Application CA shall not be used other than purposes described in "1.4.1 Appropriate certificate uses".

1.5 Policy Administration

1.5.1 Organization administering the document

The Government Information Systems Planning Division, Administrative Management Bureau, Ministry of Internal Affairs and Communications perform services related to change, update, and so on of this CP/CPS.

1.5.2 Contact person

The Contact Officer about this CP/CPS shall be an official of the Government Information Systems Planning Division, Administrative Management Bureau, Ministry of Internal Affairs and Communications is Application CA director.

Then URL of the contact side is as follows:

URL: http://www.gpki.go.jp/

1.5.3 Person determining CPS suitability for the policy

The Inter-ministerial Council of Government Information Systems decides the suitability of the CP/CPS of the Application CA.

1.5.4 CPS approval procedures

The Application CA's CP/CPS for the Application CA shall be validated by a decision of the Inter-ministerial Council of Government Information Systems.

1.6 Definitions and acronyms

- CA (Certification Authority)

An agency that issues, re-keys or revokes certificates, generates and protects private keys for CAs, etc., and registers subscribers. If referred to simply as a "CA", certificate issuance and registration operations are included.

- CP/CPS (Certificate Policy/Certification Practices Statement)

CP: A document stipulating the operating policy to be applied when a CA issues certificates

CPS: A document stipulating matters relating to CA operations, certificate policies, key generation and management, and liabilities, etc. It shall externally demonstrate the reliability and security of the CA. While the Certificate Policy indicates which policy shall be applied, the Certification Practices Statement indicates how the specific policy shall be applied.

- CRL (Certificate Revocation List)

A list of server certificates and code signing certificates that have been revoked prematurely for such reasons as the CA private key compromise. The signatures of the CAs that issued the revoked certificates are attached to this list.

- FIPS 140-1 (2) (Federal Information Processing Standard)

Federal Information Processing Standards compiled by NIST (the National Institute of Standards and Technology) of the United States, which stipulate security requirements pertaining to encryption technology. These cover general requirements relating to encryption technology for cryptographic modules used in computers and communication systems. There are four security levels, from lowest to highest.

Level 1: The lowest security level defined in the FIPS. Applied to cryptographic modules used in ordinary PCs.

Level 2: At this level, cryptographic modules are equipped to retain evidence of intrusion in the event of unauthorized access.

Level 3: At this level, cryptographic modules are equipped to retain evidence of intrusion in the event of unauthorized access. Compared with Level 2, a more stringent tracing capability is provided. Special hardware is used to delete data in the event of an intrusion.

Level 4: The highest security level defined in the FIPS. It also provides for the detection of environmental changes, such as temperature and current fluctuations.

- GPKI (Government Public Key Infrastructure)

Organization or infrastructure that confirms mutually that electronic documents, created by computerized processes, such as applications and notifications between citizens and governmental organization, and electronic documents, created by computerized processes, between governmental organizations or within the same organization were created by the proper nominal persons and that the contents were not modified. Specifically, it is a certification system of national governments using signatures by the public key cryptosystem, consisting of the Bridge CA (hereinafter referred to as "BCA") and governmental organization side CA.

- HSM (Hardware Security Module)

Hardware devices used to store private keys.

- IA (Issuing Authority)

An agency that carries out those aspects of CA operations that relate to certificate issuance. A "general IA operator" is a person whose main task is the issuance of certificates. Within the Application CA, these people are classified on the basis of the authority into "senior IA operators" and "general IA operators".

- IETF (Internet Engineering Task Force)

The main mission of this technical task force is to develop and standardize protocol technology for the Internet. A specification created by this group is called a "Request for Comments".

- ISO (International Standardization Organization)

The mission of this organization is to set international standards in all technical fields except electrical engineering.

- ITU (International Telecommunication Union)

A specialist agency of the United Nations dedicated to the improvement and rational utilization of telecommunications.

- ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)

A division of the ITU dedicated to telecommunication standardization.

- LRA (Local Registration Authority)

A Registration Authority with responsibility for a local community. This organization is established in the unit of office and ministry. This organization accepts and reviews applications for issuance, re-key and revocation of certificates from subscribers.

- OID (Object Identification)

Identifiers registered with registration agencies (ISO, ITU) with values that are unique in the world. Registered object identifiers are used for such items as the PKI algorithms used, and the subject types (country names and other attributes) stored in certificates.

- PKCS (Public Key Cryptography Standards) #10

PKCS are technical standards used to implement the public key encryption technology developed by RSA Data Security of the United States. PKCS #10 specifies the certification request syntax standard for CSRs to CAs.

- PKI (Public Key Infrastructure)

The infrastructure required to use public key certificates that warrant the validity of public keys.

- PKIX (Public-Key Infrastructure (X.509))

An IETF task force that works on security issues. Its objective is to establish certificate and CRL profiles and CP and CPS frameworks.

- RA (Registration Authority)

An agency that handles CA operations pertaining to registration. The main tasks are identity checking for parties to which certificates are issued, the registration of information required for the issuance of certificates, and CSR to CAs.

- RFC3647 (Request For Comments3647)

RFC is the generic term for standard documents related to the Internet. RFC3647, one of the documents, provides frameworks and guidelines for creating a CPs or CPSs.

- RSA

One of the encryption algorithms used in public key cryptography. Proper security levels are ensured this way because it is almost impossible to apply prime factor analysis to an integer produced by multiplying two sufficiently large, different prime numbers.

- SSL (Secure Socket Layer)

Protocol that performs cryptography and certification of communications between server and client to send and receive data safely

- X.500 Identifier (DN: Distinguished Name)

X.500 is a directory standard developed by the ITU to provide a wide spectrum of services, ranging from name and address surveys to attribute-based searches. X.500 identifiers are used in X.509 issuer names and subject names.

- X.509s

A certificate and CRL format established by the ITU-T. X.509v3 (Version 3) has extended fields to hold optional information. Within GPKI, X.509v3 is used for certificates and X.509v2 for CRLs.

- archive

To retain certificate issuance histories, revocation histories and other information on a long-term basis.

- access control

Control functions that prevent unauthorized access to computers and other information resources. These functions allow the identity of the person seeking access to be checked so that the person can perform only those operations (reading, writing, etc.) which have previously been authorized.

- application CA repository

This is used to store certificates and CRL issued by the Application CA. (See "Repository".)

- algorithm

A procedure or method for computation or problem solving.

- cryptography module

Product including hardware, firmware, and software that install cryptography functions such as encryption, decryption, digital signature, certification technology, and random number generation

- tampering

Changing the content of data.

- key size (key length)

One of the factors that determines the degree of encryption. The key size is expressed as a length in bits. The strength of the encryption increases in proportion to key length.

- key pair

A public key and private key pair used in public key cryptography. Since one key cannot be deduced from the other, it is possible to disclose one (the public key) while keeping the other (the private key) confidential.

- activation

Turning on a system or equipment, etc., for use.

- activation data

The data (passwords, etc.) required to activate a system or equipment, etc.

- control key

A key required for HSM operations. It is used to control HSM functions.

- compromise state

A situation in which reliability may have been lost. In the case of a CA, the CA private key compromise undermines the reliability of all certificates issued by that CA.

- public key

One of the pair of keys used in public key cryptography. It is the public key corresponding to a private key.

- public key cryptosystem

A cryptography method that employs two different keys to decrypt messages. RSA cryptography is typical of this approach.

- public key parameter

A value used by both the certificate owner and the relying party when using elliptic curve encryption or other methods. In the case of elliptic curve encryption, it means the curve's parameters on which calculations are based.

- computer security

Countermeasures used to protect computers and other assets relating to information processing activities from external threats to ensure the confidentiality, integrity, and usability of information.

- Self-signed certificate

A certificate signed using the CA private key corresponding to the public key of the same CA. It guarantees the validity of the CA's own public key.

- revocation information

Information published by a CA to indicate that certificates issued by that CA have been revoked prematurely for such reasons as re-key due to changes in the information contained in the certificate, or the CA private key compromise.

- revocation list

See "CRL".

- subject name

A name that identifies the subscriber who owns the certificate and the private key corresponding to the public key stored in the certificate.

- certificate (public key certificate)

An electronic document certifying that a public key is owned by the person named in the certificate. The CA checks the content and applies its signature, thereby guaranteeing the validity of the public key.

- relying party

A party (including software) who verifies the validity of a certificate.

- certificate signing request (CSR)

The data file used as the basis for the issuance of a certificate. The CSR includes the public key of the party requesting the issuance of the certificate, and the certificate is issued by applying the signature of the issuer to that public key. GPKI conforms with PKCS#10.

- subscriber

The user or device to whom or to which a certificate is issued. (Web server, administrator of the server, etc.)

- signature (digital signature)

A mechanism that guarantees the integrity of a message using private keys under the public key cryptography method. The hash value of the message is encrypted and attached to the message using the private key of the sender. The recipient uses the public key of the signatory to check the identity of the sender and detect any alteration in the message. .

- security audit

An audit of important security issues.

- operation key

A key required for HSM operations.

- time stamp

A value that indicates the time when an event recorded in the log, etc., took place. It is based on time data controlled by a reliable time management device.

- Elliptic Curve Cryptography

An encryption method that uses addition and subtraction operations defined by an elliptic curve. It is necessary to maintain the strength of the encryption by changing the parameters.

- integrated repository

A published repository containing the certificates and CRL required to check the validity of certificates, which are part of the information in the BCA repository and Application CA repositories. (See “Repository”.)

- issuer name

A name that identifies the CA that issued a certificate and applied its signature.

- hash function

A function that prevents the calculation of the same output values from two different input values. It is also impossible to calculate back to the input value from the output value.

- hash value

The output value of the hash function corresponding to a particular value. (See "Hash Function".) .

- deactivation

To render a system or equipment, etc., unusable.

- private key

One of the pair of keys used in public key cryptography. This key, which corresponds to the public key, is used only by the party concerned.

- private key escrow

Entrusting the private key used in signatures, which only the legitimate owner can hold, to a third party.

- finger print

The hash value corresponding to any message. Under GPKI, this indicates the hash value of the public key. It is called a "fingerprint" because of the ability of the hash function to assign a unique value. (See "Hash Function".)

- profile

A definition of the data included in certificates and CRL. Certificate and CRL profiles are defined in RFC3280.

- restore

To restore data from a backup.

- repository

A published database containing certificates and CRL. Under GPKI, a directory server is used.

- log

A file recording operations and processes carried out on a computer

2. Publication and repository responsibilities

2.1 Repository

Information pertaining to the Application CA is published in the integrated repository and on web site.

2.2 Publication of certification information

(1) The publication in the integrated repository

The Application CA registers the following information held in the Application CA repository in the integrated repository and publishes them:

- Self-signed certificate of the Application CA
- CRL

(2) The publication in web site

The Application CA publishes the following information on web site:

- Self-signed certificate of the Application CA and its finger print
- CRL
- Information about the CA private key compromises
- The CP/CPS and their revision history

2.3 Time or frequency of publication

Published information shall be updated at the following intervals.

- Whenever a Self-signed certificate and CRL are issued or re-keyed
- Whenever this CP/CPS is amended

2.4 Access controls on repositories

Access control is not performed for information registered in the integrated repository from the Application CA repository and published on web site.

3. Identification and authentication

3.1 Naming

3.1.1 Types of Names

The issuer name and subject name of a certificates issued by the Application CA shall be determined according to the format of the X.500 Distinguished Name (DN).

3.1.2 Need for names to be meaningful

(1) Server certificate

A name used in a Server certificate is a server name. An absolute domain name (FQDN: Fully Qualified Domain Name) is set.

(2) Code signing certificate

A name used in a code-signing certificate is the name of an organization distributing an application.

3.1.3 Anonymity or pseudonymity of subscribers

As described in "3.1.2 Need for names to be meaningful".

3.1.4 Rules for interpreting various name forms

The rules for interpreting various types of names shall be determined to the X.500 series distinguished name rules.

3.1.5 Uniqueness of names

Name uniqueness in certificates shall be performed by the Application CA.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

As for the application procedure of a Server certificate and code-signing certificate, the IA and RA shall verify the signatures of the CSRs and confirm that it is signed using the private key that correspond to the public key included in the CSRs.

3.2.2 Authentication of organization identity

As for the application procedure of a Server certificate and code-signing certificate, the LRA shall confirm the authenticity of the organization to which the subscriber belongs by collating the information (organization and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on.

3.2.3 Authentication of individual identity

As for the application procedure of a Server certificate and code-signing certificate, the LRA shall confirm the authenticity of the subscriber by collating the information (name, contact address and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on.

And the LRA shall confirm the intention to subscribe by telephone or face to face.

3.2.4 Non-verified subscriber information

No stipulation

3.2.5 Validation of authority

The correctness of authority is confirmed according to the procedures defined in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

3.2.6 Criteria for interoperation

No stipulation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identification and authentication for routine re-key of a certificate are performed according to the procedure defined in "3.2 Initial identity validation".

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication for re-key after revocation of a certificate are performed according to the procedure defined in "3.2 Initial identity validation".

3.4 Identification and authentication for revocation request

Identification and authentication for revocation of a certificate are performed according to the procedures defined in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity".

4. Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

(1) Server certificate

The Server certificate application shall be submitted to the LRA by an authorized representative of the same organization as that of the subscriber.

The LRA shall perform application of the Server certificate to the IA and RA.

(2) Code signing certificate

The code signing certificate application shall be submitted to the LRA by an authorized representative of the same organization as that of the subscriber.

The LRA shall perform application of the code signing certificate to the IA and RA.

4.1.2 Enrollment process and responsibilities

(1) Server certificate

The subscriber shall apply accurate information on their certificate applications to the LRA.

The LRA shall confirm that the domain holder of the common name (CN) described in the Server certificate application is the organizations of offices and ministries to which the LRA belongs by using the database provided by the third-party body and so on, and apply accurate information to the IA and RA.

(2) Code signing certificate

The subscriber shall apply accurate information on their certificate applications to the LRA.

The LRA shall confirm that the organization name of the common name (CN) described in the code-signing application exists and it is the organization name of offices and ministries to which the LRA belongs by using the public documents published by offices and ministries, and apply accurate information to the IA and RA.

4.2 Certificate application processing

(1) Server certificate

The subscriber shall apply to the LRA in accordance with the prescribed procedures.

The LRA shall perform review according to the procedures defined in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity", and registers to the IA and RA.

The IA and RA shall check that the application contents are appropriate by operating of the procedures defined by "3.2.1 Method to prove possession of private key", and shall check that the review in LRA is completed.

(2) Code signing certificate

The subscriber shall apply to the LRA in accordance with the prescribed procedures.

The LRA shall perform review according to the procedures defined in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity", and registers to the IA and RA.

The IA and RA shall check that the application contents are appropriate by operating of the procedures defined by "3.2.1 Method to prove possession of private key", and shall check that the review in LRA is completed.

4.3 Certificate issuance

(1) Server certificate

The IA and RA sign to the registered public key with the CA private key, issue a Server certificate.

The IA and RA distribute the issued Server certificate to the LRA by using a safe means of communication.

The LRA distributes the Server certificate to the subscriber or certificate applicant in accordance with the prescribed procedures. The issuance is notified by distribution of the Server certificate.

(2) Code signing certificate

The IA and RA sign to the registered public key with the CA private key, issue a code signing certificate.

The IA and RA distribute the issued code signing certificate to the LRA by using a safe means of communication.

The LRA distributes the code signing certificate to the subscriber or certificate applicant in accordance with the prescribed procedures. The issuance is notified by distribution of the code signing certificate.

4.4 Certificate acceptance

(1) Server certificate

The subscriber shall check promptly the contents of the certificate. When detecting a problem, the subscriber shall notify the LRA of the problem.

The LRA assumes acceptance of the Server certificate to be completed if the subscriber notify the LRA of no problem.

(2) Code signing certificate

The subscriber shall check promptly the contents of the certificate. When detecting a problem, the subscriber shall notify the LRA of the problem.

The LRA assumes acceptance of the code signing certificate to be completed if the subscriber notify the LRA of no problem.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

When using private keys and certificates, the subscriber is obliged to:

- Use the Server certificate and code signing certificate in accordance with this CP/CPS.
- Administer the Server certificate, code signing certificate, and these private keys corresponding to the certificates safely.
- Inform the LRA of the compromise state of the private keys as soon as the state occurs.

4.5.2 Relying party public key and certificate usage

When trusting and using public keys and certificates, the relying party of the Server certificate and code signing certificate is obliged to:

- Check the use purpose of the Server certificate and code signing certificate.
- Check that the Server certificate and code signing certificate are not tampered.
- Verify the validation of the Server certificate and code signing certificate.

4.6 Certificate Renewal

(1) Server certificate

No stipulation

(2) Code signing certificate

No stipulation

4.7 Certificate re-key

(1) Server certificate

When the cases that the expiration date of the Server certificate, if Re-Keying the Server certificate, corresponding private key shall be generated newly according to the procedures stipulated in "4.2 Certificate application processing" and "4.3 Code signing certificate ".

(2) Code signing certificate

When the cases that the expiration date of the code signing certificate, if Re-Keying the code signing certificate, corresponding private key shall be generated newly according to the procedures stipulated in "4.2 Certificate application processing" and "4.3 Code signing certificate".

4.8 Certificate modification

(1) Server certificate

When the cases that certificate information is modified, the certificate shall be issued according to the procedures stipulated in "4.2 Certificate application processing" and "4.3 Code signing certificate". When a certificate is revoked due to modification, the procedure in "4.9.3 Procedure for revocation request" is performed.

(2) Code signing certificate

When the cases that the certificate information is modified, the certificate shall be issued according to the procedures stipulated in "4.2 Certificate application processing" and "4.3 Code signing certificate". When a certificate is revoked due to modification, the procedure in "4.9.3 Procedure for revocation request" is performed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

(1) Server certificate

The IA and RA revoke a Server certificate when the following certificate revocation reasons occur:

- In case of loss or compromise of private key.
- In case of reissuing of certificate.
- In case of modification of contents described in the certificate.
- The CA private key is lost or compromise.
- Use of the certificate is stopped.
- The Inter-ministerial Council of Government Information Systems decides that the certificate is revoked because of any reason such as a case in which the subscriber or LRA violates the obligations defined by this CP/CPS.
- Application CA director decides the revocation according to a request from the LRA.
- Application CA administrator decides the revocation because of events such as erroneous issuance of the certificate due to any reason chargeable to the Application CA.

(2) Code signing certificate

The IA and RA revoke a code signing certificate when the following certificate revocation reasons occur:

- In case of loss or compromise of private key.
- In case of reissuing of certificate.
- In case of modification of contents described in the certificate.
- The CA private key is lost or enters a compromise state.
- Use of the certificate is stopped.
- The Inter-ministerial Council of Government Information Systems decides that the certificate is revoked because of any reason such as a case in which the subscriber or LRA violate the obligations defined by this CP/CPS.
- Application CA director decides the revocation according to a request from the LRA.
- Application CA administrator decides the revocation because of events such as erroneous issuance of the certificate due to any reason chargeable to the Application CA.

4.9.2 Who can request revocation

(1) Server certificate

An applicant of revocation of a Server certificate to the LRA shall be the user of the certificate or a person belonging to the same organization as that of the subscriber.

LRA shall perform application for Server certificate revocation to the IA and RA.

(2) Code signing certificate

An applicant of revocation of code signing certificate to the LRA shall be the user of the certificate or a person belonging to the same organization as that of the subscriber.

The LRA shall perform an application for code signing certificate revocation to the IA and RA.

4.9.3 Procedure for revocation request

(1) Server certificate

The certificate applicant shall perform an application for Server certificate revocation to the LRA in accordance with the prescribed procedures.

The LRA shall confirm that the common name (CN) described in the application is the same common name (CN) of the application for issuing certificate and registers the Server certificate revocation application to the IA and RA.

The IA and RA shall perform revocation processing of the Server certificate according to the revocation application from the LRA and register the CRL in the integrated repository and web site.

The LRA shall check the completion of Server certificate revocation and informs the subscriber or the applicant of it.

(2) Code signing certificate

The certificate applicant shall perform an application for revocation of code signing certificate to the LRA in accordance with the prescribed procedures.

The LRA shall confirm that the common name (CN) described in the application is the same common name (CN) of the application for issuing certificate and registers the code signing certificate revocation application to the IA and RA.

The IA and RA shall perform revocation processing of the code signing certificate according to the revocation application from the LRA and register the CRL in the integrated repository and web site.

The LRA shall check the completion of code signing certificate revocation and informs the subscriber or the applicant of it.

4.9.4 Revocation request grace period

In case of event needing revocation, subscriber shall perform the revocation application immediately.

4.9.5 Time within which CA must process the revocation request

The IA and RA shall perform revocation immediately after the revocation application procedure terminates.

When an already-issued certificate is revoked, its revocation processing is not cancelled. When the certificate is issued again to the subscriber of the revoked certificate, the issue procedure is performed newly.

4.9.6 Revocation checking requirement for relying parties

The relying party shall check the validity of a certificate using the CRL. The IA and RA publish the CRL in the integrated repository and web site so that the validity can be checked.

4.9.7 CRL issuance frequency

The CRL of 48-hour validity period is issued at intervals of 24 hours. However, if an event such as occurrence of a CA private key compromise state, the CRL is issued immediately.

4.9.8 Maximum latency for CRLs

The IA and RA reflect the issued CRL on the Application CA repository, integrated repository and web site quickly.

4.9.9 On-line revocation/ status checking availability

The BCA maintains and administers the integrated repository and web site.

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 related to key compromise

When the private key of a subscriber enters a compromise state, the user shall inform the LRA of the state immediately. The LRA shall perform the revocation application procedure quickly. The IA and RA shall perform revocation processing quickly according to the revocation application from the LRA.

4.9.13 Circumstances for suspension

The IA and RA do not terminate the certificates temporarily.

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

No stipulation

4.11 End of subscription

No stipulation

4.12 Key escrow and recovery

The CA private key is not escrowed.

5. Administration of Facilities and Operations

5.1 Physical controls

5.1.1 Site location and construction

The IA and RA facilities shall be located at a site where it will not be affected by flooding, earthquakes, fire and other disasters. Structural countermeasures shall also be used to protect the building from earthquakes, fire and illegal intrusion. The equipment used shall be installed in safe locations that provide protection from disasters and illegal intrusion.

5.1.2 Physical access

Rooms within the IA and RA facilities shall be subject to strict entry/exit control at multiple security levels, depending on the importance of the authentication operations carried out in those rooms. Authentication shall be provided using IC cards or biometric identification systems that allow the identification of authorized operators.

Authorization to entry/exit rooms shall be granted by the Application CA director as stipulated in “5.2 Procedural controls”.

Security guards shall be stationed in the IA and RA facilities, and it shall also be monitored 24 hours a day, 365 days a year by surveillance systems.

5.1.3 Power and air conditioning

The IA and RA shall secure adequate power supply capacity for its equipment, etc., and implement countermeasures against power interruptions, power failure and fluctuations in voltage or frequency. If commercial power becomes unavailable, the facility shall switch to generator power within a specified time.

Air conditioning equipment shall be installed to maintain an appropriate operating environment for equipment and working environment for personnel.

5.1.4 Water exposures

Rooms in the building in which the IA and RA facilities is located shall be equipped with water leakage detectors, and steps shall be taken to make floors or ceilings water-proof.

5.1.5 Protect against earthquake-damaged

The building in which the IA and RA facilities is located shall have an earthquake-resistant structure, and steps shall be taken to prevent equipment and machinery from toppling or falling.

5.1.6 Fire prevention and protection

The building in which the IA and RA facilities is located shall have a fire-resistant structure. Rooms shall be protected with firewalls, and fire extinguishers shall be provided.

5.1.7 Media storage

The IA and RA shall store memory devices that include archive and backup data in a lockable storage facility located in a room to which there is appropriate entry/exit control. Media shall be taken into or out of storage in accordance with the prescribed procedures.

5.1.8 Waste disposal

The IA and RA shall dispose documents and memory devices that contain confidential information of in accordance with the prescribed procedures.

5.1.9 Offsite backup

When the IA and RA store media of important data at an off-site location separate from the IA and RA facilities, the IA and RA shall assure security of a transport route, also device a security countermeasure, commensurate to that of the IA and RA facilities, to the facility in which the media are retained.

5.2 Procedural control

5.2.1 Trusted roles

(1) Application CA director

Application CA director is responsible for operation of the Application CA and performs:

- Establishment of Application CA management policies
- Coordination of authentication operations
- Coordination of actions in emergencies, such as the CA private key compromise or disasters
- Coordination of other aspects of Application CA management

(2) IA key administrator

The IA key administrator is responsible for services using the CA private key and shall perform the following task:

Multiple IA key administrators perform the operations.

- Retention and management of keys used to control HSM functions (hereinafter referred to as "control keys")
- Retention and management of backup memory devices for the CA private key
- Attendance at HSM key operations for the generation of the CA private key and issuance of self-signed certificates
- Attendance at HSM key operations for the re-key of the CA private key
- CA private key backups and HSM key operations for restoration from backups, as well as setting up of backup media for the CA private key

(3) Reception personnel

Reception personnel accept applications related to participation and withdrawal from the LRA, adjusts communication with applicants, and administers application documents.

(4) Reviewer

Reviewer shall perform reviews of applications related to participation and withdrawal from the LRA.

(5) Application CA administrator

Application CA administrator is responsible for operations of the Application CA and shall perform the following task:

- Provision of work instructions to senior IA operators and general IA operators, and confirmation of results
- Instruction concerning initial actions in response to emergencies, such as CA private key compromise and disasters

- Operations control of the Application CA
- Control of a key required for HSM operations (hereafter referred to as "operation key")

(6) Assistant application CA administrator

The assistant application CA administrator is acting Application CA administrator, and shall perform the following task in place of Application CA administrator:

- Provision of work instructions to senior IA operators and general IA operators, and confirmation of results
- Operations control of the Application CA
- Control of the operation key required for HSM operations

(7) Senior IA operator

Senior IA operators perform the following task related to the Application CA system. The operations shall be performed by multiple senior IA operators.

- Generating CA private key, and operation of the operation key required for HSM operations at issuance of a self-signed certificate
- Operation of the operation key required for HSM operations at re-key of a CA private key
- Activation and deactivation of a CA private key
- Application CA system start and stop
- Application CA repository start and stop
- Administration of the Application CA system reconfiguration
- Administration of system reconfiguration relating to database backups, restoration and archive operations for the Application CA system

(8) General IA operator

General IA operators perform the following task related to certificates issued from the Application CA system. The operations shall be performed by multiple general IA operators.

- Registration and modification of the certificate policy
- Revocation of server and code signing certificates
- Processing of issues, re-keys and revocations for operator certificates
- Administration of Application CA repository settings

(9) Audit log inspector

The audit log inspector performs the following task related to the log recording important events related to security for the Application CA system and Application CA repository (hereafter referred to as "audit log"):

- Audit log inspect
- Deletion of unnecessary audit log

(10) LRA administrator

The LRA administrator is responsible for LRA management and shall perform the following task:

- Designation of LRA personnel and cancellation of designation
- Work planning and work instruction to LRA personnel
- Final approval of review result of requesting issuance, re-key and revocation of server and code signing certificates
- Control of review request for issuance, re-key and revocation of server and code signing certificates
- Controls of application documents
- Operation of internal review of the LRA
- Reporting of internal review result to Application CA director

(11) LRA operator

According to instructions of LRA administrator, LRA operators register requests for issuance, re-key and revocation of server and code signing certificates in the IA and RA.

(12) LRA Reception personnel

LRA Reception personnel accept applications for issuance, re-key, and revocation of server and code signing certificates, and perform associated paperwork and liaison services.

(13) LRA Reviewer

LRA Reviewer review applications for issuance, re-key and revocation of server and code signing certificates.

5.2.2 Number of persons required per task

In the IA and RA, two or more persons shall perform important services such as CA private key generating and issuance of self-signed certificates.

5.2.3 Identification and authentication for each role

Identification and authentication shall be carried out to ensure that only authorized operators operate the systems.

5.2.4 Role requiring separation of duties

Important services are instructed to Application CA administrator from Application CA director.

Application CA administrator instructs task to each personnel. When the important services are performed, authorities of personnel are separated for mutual checks and balances. An LRA administrator instructs LRA services to each LRA personnel.

5.3 Personnel controls

Matters pertaining to Application CA personnel, including review of qualifications, education and transfers, shall be governed by the National Public Service Law and other laws relating to personnel affairs. All personnel shall receive education and training so that they can acquire the knowledge and skills required for Application CA administration. When services are consigned partly, appropriate contracts, related to consigned services, including responsibility for maintaining confidentiality shall be placed with the consignee.

5.4 Audit logging procedures

Audit log inspector collate audit log with service execution records and perform security audit for checking abnormal events such as invalid operation.

5.4.1 Types of events recorded

Important events relating to the security in the Application CA system and the Application CA repository are recorded in the audit logs including the access log and operations log.

The following information shall be included in the audit log. The following information shall be included in the audit log.

- Type of event
- Date and time of event
- Processing result
- Information to identify source of event (operator name, system name, etc.)

5.4.2 Frequency of processing log

Audit log reviewers collate audit log with job execution records or the like every week.

5.4.3 Retention period for audit log

The audit log shall be retained for three years.

5.4.4 Protection of audit log

Access to audit log shall be controlled and action to enable tampering to be detected shall be taken.

Audit log is backed up every week in external storage media and retained in a lockable archive in a room of which entering and leaving are administered appropriately.

Audit log is browsed and deleted by audit log reviewers.

5.4.5 Audit log backup procedures

The audit log shall be backed up every day and is collected in external storage media every week.

5.4.6 Audit collection system

The audit log collection function shall be one of in the Application CA system functions. The function collects important events related to security as audit log from when the system starts.

5.4.7 Notification to event-causing subject

Audit log shall be is checked without notification to persons causing events

5.4.8 Vulnerability assessments

Operational and system-related vulnerability shall be assessed by means of audit log inspections.

5.5 Records archival

5.5.1 Types of records archived

Archive data types are:

- Certificate issuing history
- CRL issuing history

- Start and stop log
- Operation log

5.5.2 Retention period for archive

Archive data is retained for 10 years after the validity period of the certificate expires.

5.5.3 Protection of archive

Access to archive data shall be controlled and action to enable tampering to be detected shall be taken.

5.5.4 Archive backup procedures

Archive data shall be backed up every day and copied external memory devices every month.

5.5.5 Requirements for time-stamping of records

A time stamp is assigned to archive data in the unit of record.

5.5.6 Archive collection system

No stipulation

5.5.7 Procedures to obtain and verify archive information

The external memory devices on which the archive is stored shall be checked for readability on an annual basis.

5.6 Key changeover

CA key pairs shall be re-keyed over every seven years.

The distribution method of the new CA public key is the same as that in "6.1.4 CA public key delivery to relying parties".

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The IA and RA will plan procedures to restore services immediately, against with an accident or a compromise as follows.

- Crash of hardware resources, software, and/or data
- CA private key is compromised.

- Disasters such as fire and earthquake

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

If hardware resources, software and/or data is crashed, restoration is performed quickly by using backup hardware resources, software and/or data. Software and/or data necessary for restoration are collected periodically or whenever circumstances required it.

5.7.3 Entity private key compromise procedures

If a CA private key is compromised, certification services are stopped in accordance with predetermined procedures and the following procedures are performed:

- Publication of information related to the compromise state
- Revocation of Server and Code Signing certificates
- Discarding and re-generating of the CA private key
- Reissuing of Server and Code Signing certificates

If a subscriber's private key is compromise, the certificate is revoked in accordance with the procedure defined in "4.9 Certificate revocation and suspension ".

5.7.4 Business continuity capabilities after a disaster

If the IA and RA facilities are damaged by disasters, operation is performed in a backup site by using backup data. The backup site is set in a location separated from the main site by appropriate distance. The service policy at a disaster is defined as follows:

- CRL publication by the integrated repository and Web site is given the highest priority. The publication is restarted within 48 hours after the publication is stopped.
- Urgent issuance and revocation of certificates are restarted within 96 hours after the services stopped.
- Ordinary services are restarted after complete restoration of the IA and RA facilities and security at the main site is confirmed.

5.8 CA or RA termination

If the Inter-ministerial Council of Government Information Systems decides to terminate the certification services of the Application CA, the IA and RA shall notify the LRA, subscribers, and relying party about the storage organization and the disclosure method and the Application CA's backup and archive data, no later than 90 days before the termination of operations. Then the IA and RA perform prescribed service termination procedures.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

(1) CA keys

CA key pairs shall be generated by multiple senior IA operators by using the HSM certificated to FIPS140-2 level 3, with attendance of multiple IA key administrators.

(2) Server certificate key

Server certificate key pairs shall be generated by a subscriber.

(3) Code signing certificate key

Code signing certificate key pairs shall be generated by a subscriber.

6.1.2 Private key delivery to subscriber

The IA and RA do not deliver a private key to the subscriber.

6.1.3 Public key delivery to certificate issuer

A subscriber sends the public key of the user to the LRA by a secure method, and the LRA sends the key to the IA and RA by a secure method.

6.1.4 CA public key delivery to relying parties

The IA and RA shall publish self-signed certificates in the integrated repository and on web site and publish the finger prints on web site. The self-signed certificates and finger prints shall be published on web site by a secure method.

6.1.5 Key sizes

(1) CA key

RSA 2048-bit key shall be used.

(2) Server certificate key

RSA 1024-bit key shall be used.

(3) Code signing certificate key

RSA 1024-bit key shall be used.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes

The keys shall be used only for the following use purposes:

(1) CA key

CA private key shall be used for signatures.

(2) Server certificate key

Server certificate key shall be used for existence certification of the server and the encrypted communications.

(3) Code signing certificate key

Code signing certificate key shall be used for a signature of software such as programs.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

(1) CA key

CA private key shall be protected using the HSM certified to FIPS140-2 level 3.

(2) Server certificate key

No stipulation

(3) Code signing certificate key

No stipulation

6.2.2 Private key (n out of m) multi-person control

Operations related to CA private key administration shall be performed by multiple IA key administrators and multiple senior IA operators.

6.2.3 Private key escrow

CA private keys shall not be escrowed.

6.2.4 Private key backup

CA private key backups shall be carried out by multiple IA key administrators and multiple senior IA operators.

CA private key backed up from an HSM shall be retained securely by multiple IA key administrators.

6.2.5 Private key archival

CA private keys shall not be archived.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation

6.2.7 Private key storage on cryptographic module

(1) CA key

Multiple IA key administrators and multiple senior IA operators shall generate and store the CA private key within an HSM.

(2) Server certificate key

No stipulation

(3) Code signing certificate key

No stipulation

6.2.8 Method of activating private key

(1) CA key

CA private keys shall be activated by multiple senior IA operators, using the operation key and password.

(2) Server certificate key

No stipulation

(3) Code signing certificate key

No stipulation

6.2.9 Method of deactivating private key

(1) CA key

CA private keys shall be deactivated by multiple senior IA operators, using the password.

(2) Server certificate key

No stipulation

(3) Code signing certificate key

No stipulation

6.2.10 Method of destroying private key

(1) CA key

CA private keys in the HSM shall be erased by multiple IA key administrators and multiple senior IA operators, using the HSM function. Also, the medium shall be treated by the same method when the backup media of the CA private key shall be destroyed.

(2) Server certificate key

No stipulation

(3) Code signing certificate key

No stipulation

6.2.11 Cryptographic module Rating

This shall be as stipulated in "6.1.1 Key pair generation" and "6.2.1 Cryptographic module standards and controls ".

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys shall be included in certificate archives. They shall be retained for the period stipulated in "5.5.2 Retention period for archive ".

6.3.2 Certificate operational periods and key pair usage periods

(1) CA key

The public and private keys of the Application CA shall be valid for 10 years from the date they were validated. They shall be re-keyed within seven years.

If encryption security levels are judged to be low, keys shall be updated at that time.

(2) Server certificate key

The public and private keys of the server certificate shall be valid for three years from the date they were validated.

If encryption security levels are judged to be low, keys shall be updated at that time.

(3) Code signing certificate key

The public and private keys of the code signing certificate shall be valid for three years from the date they were validated.

If encryption security levels are judged to be low, keys shall be updated at that time.

6.4 Activation data

6.4.1 Activation data generation and installation

(1) CA key

The operation key and password required to activate the HSM in which the CA private key is stored shall be generated and registered by multiple IA key administrators and multiple senior IA operators.

(2) Server certificate key

The activation data of the private key of a server certificate shall be generated and registered by the subscriber.

(3) Code signing certificate key

The activation data of the private key of a code signing certificate shall be generated and registered by the subscriber.

6.4.2 Activation data protection

(1) CA key

The operation key and password required to activate the HSM in which the CA private key is stored shall be retained safely by the IA and RA.

(2) Server certificate key

The activation data of the private key of a server certificate shall be retained safely by the subscriber.

(3) Code signing certificate key

The activation data of the private key of a code signing certificate shall be retained safely by the subscriber.

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Application CA system shall be equipped with various functions, including the access control, operator identification and authentication, encryption for database security, audit log and archive data collection, and CA key and system recovery.

6.5.2 Computer security rating

No stipulation

6.6 Life cycle technical controls

6.6.1 System development controls

The development, adjustment, and modification of the Application CA system shall be carried out by a reliable organization in a reliable environment in accordance with the prescribed procedures. The developed, adjusted or modified system is verified in a test environment and approved by Application CA director. Then the system shall be introduced. The system specifications and verification reports shall be documented and retained.

6.6.2 Security management controls

The Application CA system maintenance and management shall include periodic security checks of the operating system and software. The verification results shall be documented and retained. The computer virus countermeasure and the malicious program countermeasure shall be performed appropriately.

6.6.3 Life cycle security controls

The IA and RA shall check development, operation, and maintenance of the Application CA system evaluated timely through audit. They shall improve if necessary.

6.7 Network security controls

The information that is published in information stored in the Application CA repository shall be copied in the BCA integrated repository through a firewall. As communications with the LRA, only the encrypted communications through a leased line are used. Proper security control measures shall be implemented to prevent unauthorized access or retrieval.

6.8 Time-stamping

The IA and RA shall carry out time synchronization of the system by using a reliable time source and assign time-stamp to important information recorded in the system in the unit of record.

7. Certificate and CRL profiles

7.1 Self-signed certificate profile

Table 7-1 Application CA self-signed certificate profile

Area name	Critical flag	Value	Description
Version (version number)		2	v3 integer
serial Number (serial number)		Example: 1	Certificate serial number, integer
signature algorithm ID (signature algorithm)			Application CA signature algorithm
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer name (issuer name)		ou=Application CA, o=Japanese Government, c=JP	Application CA distinguished name (DN) in English PrintableString
validity period (certificate validity period)			Validity period of certificate
notBefore (issue date)		Example: 010401000000Z	Starting date of certificate validity periodYYMMDDHHMMSSZ
notAfter (termination date)		Example: 110401000000Z	Termination date of certificate validity period YYMMDDHHMMSSZ
subject name (subject name)		ou=Application CA, o=Japanese Government, c=JP	Application CA distinguished name (DN) in English PrintableString

subject public key info (subject public key information)			Public key algorithm
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.1	Application CA public key algorithm identifier, RSA Encryption
parameter (parameter)		NULL	No value for RSA
public key (public key)		BIT STRING	Application CA public key, bit string
extensions (certificate extension area)			
subjectKeyIdentifier (subject key identifier)	FALSE	OCTET STRING	Subject key identifier
keyUsage (key usage)	TRUE		A key usage purpose is specified.
keyCertSign		1	[5]
cRLSign		1	[6]
subjectAltName (subject alternative name)	FALSE	ou=アプリケーション CA, 0=日本国政府, c=JP	Application CA distinguished name (DN) in Japanese UTF8String
basicConstraints (basic constraints)	TRUE		Distinction between CA certificates and end entity certificate
cA		cA=TRUE	Required (MUST)
issuer's signature (issuer signature)			Digital signature of Application CA
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
	ENCRYPTED (signature value)		

7.2 Server certificate profile

Table 7-2 Application CA server certificate profile

Area name	Critical flag	Value	Description
version (version number)		2	v3 integer
serial Number (serial number)		Example: 23	Certificate serial number, integer
signature algorithm ID (signature algorithm)			Application CA signature algorithm
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption

issuer name (issuer name)		ou=Application CA,
		o=Japanese Government,
		c=JP
			Application CA distinguished name (DN) in English
			PrintableString

validity period (certificate validity period)			Validity period of certificate
notBefore (starting date)		Example: 010401000000Z	Starting date of certificate validity period YYMMDDHHMMSSZ
notAfter (termination date)		Example: 040401000000Z	Termination date of certificate validity period YYMMDDHHMMSSZ

subject name (subject name)		Example:
		cn=xxx.yyy.go.jp,
		ou=Ministry of Internal Affairs and Communications,
		o= Japanese Government,
		c=JP
			Subject distinguished name (DN) in English (DN is composed of four RDNs.)
			cn is server FQDN.
			PrintableString

subject public key info (subject pubic key information)			Public key algorithm
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.1	Server public key algorithm identifier, RSA encryption
parameter (parameter)		NULL	No value for RSA
public key (public key)		BIT STRING	Server public key, bit string
extensions (certificate extension area)			
authorityKeyIdentifier (certification authority key identifier)	FALSE		Certification authority key identifier
keyIdentifier		OCTET STRING	Application CA key identifier
subjectKeyIdentifier (subject key identifier)	FALSE	OCTET STRING	Subject key identifier
keyUsage (key usage)	TRUE		A key usage purpose is specified.
digitalSignature		1	[0]
keyEncipherment		1	[2]
extendedKeyUsage (extended key usage)	FALSE		An extended key usage purpose is specified.
KeyPurposeId		id-kp-serverAuth	Server certification by TLS or SSL
certificatePolicies (certificate policy)	FALSE		
policyIdentifier			OID
certPolicyId		0.2.440.100145.8.4.1.11.10	Server certificate policy OID id-apca-cp-tls.server10
policyQualifiers			Policy qualifiers (pointer to CPS or user notification information)
policyQualifierId		id-qt-cps	CPS

qualifier		http://www.gpki.go.jp/apca/cpcps/index.html	Application CACPS URI, IA5 string
issuerAltName (issuer alternative name)	FALSE	ou=アプリケーション CA, o=日本国政府, c=JP	Application CA distinguished name (DN) in Japanese, UTF8String
cRLDistributionPoints (CRL distribution points)	FALSE		
distributionPoint			Distribution point
fullName (non abbreviated name)		http://dir.gpki.go.jp/ApplicationCA.crl	CRL distribution point is specified by URI. IA5 string
distributionPoint			DistributionPointName
fullName (non abbreviated name)		http://dir.gpki.hq.admix.go.jp/ApplicationCA.crl	CRL distribution point is specified by URI. IA5 string
issuer’s signature (issuer signature)			Digital signature of Application CA
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
	ENCRYPTED (signature value)		

7.3 Code signing certificate profile

Table 7-3 Application CA code signing certificate profile

Area name	Critical flag	Value	Description
version (version number)		2	v3 integer
serial Number (serial number)		Example: 23	Certificate serial number, integer
signature algorithm ID (signature algorithm)			Application CA signature algorithm

algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption

issuer name (issuer name)		ou=Application CA,
		o=Japanese Government,
		c=JP
			Application CA distinguished name (DN) in English
			PrintableString

validity period (certificate validity period)			Certificate validity period
notBefore (starting date)		Example: 010401000000Z	Starting date of certificate validity period YYMMDDHHMMSSZ
notAfter (termination date)		Example: 040401000000Z	Termination date of certificate validity period YYMMDDHHMMSSZ

subject name (subject name)		Example: cn= Ministry of Internal Affairs and Communications,
		ou=Ministry of Internal Affairs and Communications,
		o= Japanese Government,
		c=JP
			Subject distinguished name (DN) in English (DN is composed of four RDNs.)
			PrintableString

subject public key info (subject public key information)			Public key algorithm
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.1	Code signing public key algorithm identifier, RSA encryption
parameter (parameter)		NULL	No value for RSA
public key (public key)		BIT STRING	Code signing public key, bit string

extensions (certificate extension area)			
authorityKeyIdentifier (certification authority key identifier)	FALSE		Certification authority key identifier
keyIdentifier		OCTET STRING	Application CA key identifier
subjectKeyIdentifier (subject key identifier)	FALSE	OCTET STRING	Subject key identifier
keyUsage (key usage)	TRUE		A key usage purpose is specified.
digitalSignature		1	[0]
extendedKeyUsage (extended key usage)	FALSE		An extended key usage purpose is specified.
KeyPurposeId		id-kp-codeSigning	Code signing
certificatePolicies (certificate policy)	FALSE		
policyIdentifier			OID
certPolicyId		0.2.440.100145.8.4.1.1.20	Code signing certificate policy OID id- apca-cp-ds.class20
policyQualifiers			Policy qualifier (pointer to CPS or user notification information)
policyQualifierId		id-qt-cps	CPS
qualifier		http://www.gpki.go.jp/apca/cpcps/index.html	Application CACPS URI, IA5 string
issuerAltName (issuer alternative name)	FALSE	ou=アプリケーション CA, o=日本国政府, c=JP	Application CA distinguished name (DN) in Japanese, UTF8String

cRLDistributionPoints (CRL distribution points)	FALSE		
distributionPoint			Distribution point
fullName (non abbreviated name)		http://dir.gpki.go.jp/ApplicationCA.crl	A CRL distribution point is specified by URI. IA5 string
distributionPoint			DistributionPointName
fullName (non abbreviated name)		http://dir.gpki.hq.admix.go.jp/ApplicationCA.crl	A CRL distribution point is specified by URI. IA5 string
issuer’s signature (issuer signature)			Digital signature of Application CA
algorithm identifier (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
	ENCRYPTED (signature value)		

7.4 CRL profile

Table 7-4 Application CA Certificate Revocation List profile

Area name	Critical flag	Value	Description
version (version number)		1	v2 CRL integer
signature (signature algorithm)			Signature algorithm
algorithmIdentifier			Algorithm identifier and signature algorithm area (signatureAlgorithm) are made equal.
algorithm (algorithm identifier)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (issuer)		ou=Application CA, o=Japanese Government, c=JP	Application CA distinguished name (DN) in English

			Printable string
thisUpdate (update date of this time)		Example: 010501000000Z	Update date and time of this time YYMMDDHHMMSSZ
nextUpdate (update date of the next time)		Example: 010503000000Z	Update date and time of the next time YYMMDDHHMMSSZ
revokedCertificates (revoked certificate)			Revoked certificate entry (list of the following set)
userCertificate		Example: 10002	A revoked certificate is specified by an integer.
revocationDate		Example: 010501000000Z	Revocation date and time YYMMDDHHMMSSZ
crlEntryExtensions (revoked certificate entry extension)	FALSE		(extension area for each revoked certificate)
reasonCode			Reason code
unspecified			[0] undefined
keyCompromise			[1] Key compromise state
cACompromise			[2]CA key compromise state
affiliationChanged			[3] Change of position
superseded			[4] Overwrite
cessationOfOperation		Example: 1	[5] Service stop
certificateHold			[6] Certificate hold
↓			
Next revoked certificate			

Extension area			
crlExtensions (certificate revocation list extension)			
authorityKeyIdentifier (CA key identifier)	FALSE		CA key identifier. Should be the same as certificate extension
keyIdentifier		OCTET STRING	Application CA key identifier

cRLNumber (CRL number)	FALSE	Example: 32	Sequence number, integer
	ENCRYPTED (signature value)		

8. Compliance audit and other assessments

The IA and RA shall have a compliance audit mechanisms in place to ensure that the requirements of this CP/CPS are being implemented and enforced as defined in "8.1 Frequency or circumstances of assessment" and "8.6 Communication of results".

Any LRA shall be assessed for operations and managements by the IA and RA.

8.1 Frequency or circumstances of assessment

The IA and RA shall have audits carried out annually by an auditor. If necessary, the IA and RA shall conduct other audits in addition to the regular audits.

8.2 Identity/ qualifications of assessor

The IA and RA audits shall be conducted by a person who is fully versed in audit and authentication operations.

8.3 Assessor's relationship to assessed entity

A person who has no relationship with the IA and RA shall be selected as the auditor for the Application CA.

8.4 Topics covered by assessment

Audit shall be carried out primarily to ascertain whether authentication operations are being conducted in accordance with this CP/CPS and the operations manual.

8.5 Actions taken as a result of deficiency

If any serious deficiencies or matters requiring urgent action are identified through an audit, the IA and RA shall take immediate action as determined by the Sterling committee. If there is a report concerning the alleged compromise of the CA private key, it shall be treated as an emergency situation, and appropriate procedures shall be implemented accordingly.

The Sterling committee shall decide whether or not to suspend the Application CA operations until remedial action has been taken with regard to such serious deficiencies or matters requiring urgent action that have been identified through an audit.

The Sterling committee shall confirm that the Application CA has taken actions in response to the deficiencies.

8.6 Communication of results

The results of the Application CA audits shall be submitted by the auditor as reports to the Application CA director, which shall, in turn, report audit results to the Sterling committee.

Audit reports shall be retained for a period of five years.

9. Other business and legal matters

9.1 Fees

No stipulation

9.2 Financial responsibility

No stipulation

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The Application CA shall treat information as confidential if its disclosure could harm the credibility and integrity of the authentication operations of the Application CA.

9.3.2 Information not within the scope of confidential information

Of the information held by the Application CA, items that are expressly intended for disclosure, such as certificates, revocation information and this CP/CPS and so on, are not considered confidential.

9.3.3 Responsibility to protect confidential information

Confidential information, including documents and storage media saving confidential information, shall be administered safely by appointing an information manager according to "laws related to protection of personal information held by governmental organizations", "implementation orders of laws related to protection of personal information held by governmental organizations" and so on.

The Application CA shall disclose subscriber's confidential information when a law-enforcement organization formally requests information disclosure according to legal bases, when a request based on wheels of justice or administrative procedure is made, or when a subscriber requests disclosure of information the subscriber presented to the Application CA.

9.4 Privacy of personal information

Personal information shall be protected appropriately according to "laws related to protection of personal information held by governmental organizations", "implementation orders of laws related to protection of personal information held by governmental organizations" and so on.

9.5 Intellectual Property Right

The intellectual property rights of the CA key pair, server certificate, code signing certificate, CRL, self-signed certificate, and this CP/CPS belong to the Application CA.

However, it is not always true for the intellectual property rights of the key pairs and the subject names in server certificates and code signing certificates.

9.6 Representation and warranties

9.6.1 Representations and warranties of IA and RA

The IA and RA shall have following representations and warranties related to CA operations:

- Issuance, re-key, and revocation of self-signed certificates, server certificates, and code signing certificates in accordance with this CP/CPS.
- Publication of information defined in "2.2 Publication of certification information"
- Every 24 hours it shall update the CRL that is to remain valid for 48-hours.
- The IA and RA shall control the CA private key securely.
- If it shall be occurred the CA private key compromise, the IA and RA shall quickly publish information of the compromise event.
- The IA and RA shall store audit logs and archive data concerning certificate issues, re-keys and revocation, for the required period.
- The IA and RA shall monitor system operations.
- The IA and RA shall appropriately review LRA information shall be submitted.
- The IA and RA shall confirm authenticity of the LRA when issuance, re-key, and revocation request of certificates be accepted.
- The IA and RA shall define standards and procedures of LRA operation, included the following:
    - Standard and procedures related to LRA operations for certificate requests
    - Standard and procedures related to LRA security measures should be conducted
    - Standard and procedures related to LRA operation logs should be collected
- The IA and RA shall take hold on circumstances of compliance above standards and procedures

9.6.2 LRA representations and warranties

The LRA shall have following represents and warranties related to LRA operations:

- The LRA shall certainly confirm authenticity of acceptance and subscribers, and submitted requests, when subscribers submit request for issuance, re-key and revocation of certificates.
- The LRA shall securely operate issuance, re-key and revocation of certificates to the IA and RA with the use of the LRA system.
- The LRA shall notify subscribers of completions of issuance and revocation.
- The LRA shall store securely subscriber information during each request operations of certificate.
- The LRA shall observe the rule of standards and procedures defined by the IA and RA.
- The LRA shall report to the IA and RA circumstances of compliance with the above standards and procedures.

9.6.3 Subscriber representations and warranties

The subscriber shall have representations and warranties compliance defined in "4.5.1 Subscriber private key and certificate usage" and the following rules:

- The subscriber shall request to LRA with correct information for issuance and revocation of certificates.
- The subscriber shall confirm certificates whether or not correct, in receipt of certificates from the LRA.
- The subscriber shall quickly request to the LRA, in case of the certificate information described shall be changed.

9.6.4 Relying party representations and warranties

The relying party shall have represents and warranties compliance defined in "4.5.2 Relying party public key and certificate usage".

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

No stipulation

9.8 Limitations of liability

No stipulation

9.9 Indemnities

No stipulation

9.10 Term and termination

9.10.1 Term

This CP/CPS shall be valid by approval of the Sterling committee.

This CP/CPS shall be not invalid before the terminate conditions defined in "9.10.2 Termination".

9.10.2 Termination

When the Application CA is terminated, this CP/CPS shall be invalid, excluding the conditions defined in "9.10.3 Termination effect and continuity of effect".

9.10.3 Effect of termination and survival

Even when a subscriber terminates certificate usage or when the Application CA operation are terminated, the provisions in "9.3 Confidentiality of business information", "9.4 Privacy of personal information ", "9.5 Intellectual Property Right", and "9.14 Governing Law" shall be applied to the subscriber, relying party, and Application CA regardless of any reasons of termination.

9.11 Individual notices and communications with participants

The point of contact concerning notifications, requests, demands, asks, and other communications is the Government Information Systems Planning Division, Administrative Management Bureau, Ministry of Internal Affairs and Communications, this CP/CPS requires and allows. The point of contact is stipulated in "1.5.2 Contact person".

9.12 Amendments

9.12.1 Procedure for amendment

If necessary, this CP/CPS shall be changed by approval of the Sterling committee.

9.12.2 Notification method and period

In case of this CP/CPS changed by approval of the Sterling committee, it shall be published quickly the changed CP/CPS. The CP/CPS publication shall be assumed as notification to subscribers and relying parties.

9.12.3 Circumstances under which OID must be changed

No stipulation

9.13 Dispute resolution provisions

No stipulation

9.14 Governing law

Japanese law shall apply to any disputes arising from authentication services under this CP/CPS.

9.15 Compliance with applicable law

No stipulation

9.16 Miscellaneous provisions

No stipulation

9.17 Other provisions

No stipulation