Japanese Government Public Key Infrastructure (GPKI)

# Application Certification Authority2(Root) Certificate Policy and Certification Practice Statement

Issued March 11th, 2013

Amended July 12th, 2013

Amended March 25th, 2014

Amended December 5th, 2014

Approved by the Inter-ministerial Council of Government Information Systems

1. Introduction ..... 1
1.1 Overview ..... 1
1.2 Document name and identification ..... 1
1.3 PKI participants ..... 2
1.3.1 Certification authorities ..... 2
1.3.2 Issuing Authority (IA) and Registration Authority (RA) ..... 2
1.3.3 Subscriber ..... 3
1.3.4 Relying parties ..... 3
1.3.5 Other participants involved ..... 3
1.4 Certificate usage ..... 3
1.5 Policy Administration ..... 3
1.5.1 Organization administering the document ..... 3
1.5.2 Contact person ..... 3
1.5.3 Person determining CPS suitability for the policy ..... 4
1.5.4 CPS approval procedures ..... 4
1.6 Definitions and acronyms ..... 4
2. Publication and repository responsibilities ..... 13
2.1 Repository ..... 13
2.2 Publication of certification information ..... 13
2.3 Time or frequency of publication ..... 13
2.4 Access controls on repositories ..... 13
3. Identification and authentication ..... 14
3.1 Naming ..... 14
3.1.1 Types of Names ..... 14
3.1.2 Need for names to be meaningful ..... 14
3.1.3 Anonymity or pseudonymity of subscribers ..... 14
3.1.4 Rules for interpreting various name forms ..... 14
3.1.5 Uniqueness of names ..... 14
3.1.6 Recognition, authentication, and role of trademarks ..... 14
3.2 Initial identity validation ..... 14
3.2.1 Method to prove possession of private key ..... 14
3.2.2 Authentication of organization identity ..... 14
3.2.3 Authentication of individual identity ..... 15
3.2.4 Non-verified subscriber information ..... 15
3.2.5 Validation of authority ..... 15
3.2.6 Criteria for interoperation ..... 15

3.3 Identification and authentication for re-key requests ..... 15
3.3.1 Identification and authentication for routine re-key ..... 15
3.3.2 Identification and authentication for re-key after revocation ..... 15
3.4 Identification and authentication for revocation request ..... 15
4. Certificate life-cycle operational requirements ..... 16
4.1 Certificate application ..... 16
4.1.1 Who can submit a certificate application ..... 16
4.1.2 Enrollment process and responsibilities ..... 16
4.2 Certificate application processing ..... 16
4.3 Certificate issuance ..... 16
4.4 Certificate acceptance ..... 16
4.5 Key pair and certificate usage ..... 16
4.5.1 Subscriber private key and certificate usage ..... 16
4.5.2 Relying party public key and certificate usage ..... 17
4.6 Certificate Renewal ..... 17
4.7 Certificate re-key ..... 17
4.8 Certificate modification ..... 17
4.9 Certificate revocation and suspension ..... 17
4.9.1 Conditions for revocation ..... 17
4.9.2 Who can request revocation ..... 18
4.9.3 Procedure for revocation request ..... 18
4.9.4 Revocation request grace period ..... 18
4.9.5 Time period which CA must process the revocation request ..... 18
4.9.6 Revocation checking requirement for relying parties ..... 18
4.9.7 CRL issuance frequency ..... 18
4.9.8 Maximum latency for CRLs ..... 18
4.9.9 On-line revocation/ status checking availability ..... 19
4.9.10 On-line revocation checking requirements ..... 19
4.9.11 Other forms of available revocation information ..... 19
4.9.12 Special requirements related to key compromise ..... 19
4.9.13 Circumstances for suspension ..... 19
4.9.14 Who can request suspension ..... 19
4.9.15 Procedure for suspension request ..... 19
4.9.16 Limits on suspension period ..... 19
4.10 Certificate status services ..... 19
4.10.1 Feature in operation ..... 19

4.10.2 Service availability ..... 19
4.10.3 Optional specification ..... 20
4.11 End of subscription ..... 20
4.12 Key escrow and recovery ..... 20
5. Administration of Facilities and Operations ..... 21
5.1 Physical controls ..... 21
5.1.1 Site location and construction ..... 21
5.1.2 Physical access ..... 21
5.1.3 Power and air conditioning ..... 21
5.1.4 Water exposures ..... 21
5.1.5 Protect against earthquake-damaged ..... 22
5.1.6 Fire prevention and protection ..... 22
5.1.7 Media storage ..... 22
5.1.8 Waste disposal ..... 22
5.1.9 Offsite backup ..... 22
5.2 Procedural control ..... 22
5.2.1 Trusted roles ..... 22
5.2.2 Number of persons required per task ..... 25
5.2.3 Identification and authentication for each role ..... 25
5.2.4 Role requiring separation of duties ..... 25
5.3 Personnel controls ..... 25
5.4 Audit logging procedures ..... 25
5.4.1 Types of events recorded ..... 25
5.4.2 Frequency of processing log ..... 26
5.4.3 Retention period for audit log ..... 26
5.4.4 Protection of audit log ..... 26
5.4.5 Audit log backup procedures ..... 26
5.4.6 Audit collection system ..... 26
5.4.7 Notification to event-causing subject ..... 26
5.4.8 Vulnerability assessments ..... 26
5.5 Records archival ..... 27
5.5.1 Types of records archived ..... 27
5.5.2 Retention period for archive ..... 27
5.5.3 Protection of archive ..... 27
5.5.4 Archive backup procedures ..... 27
5.5.5 Requirements for time-stamping of records ..... 27

5.5.6 Archive collection system ..... 27
5.5.7 Procedures to obtain and verify archive information ..... 27
5.6 Key changeover ..... 27
5.7 Compromise and disaster recovery ..... 28
5.7.1 Incident and compromise handling procedures ..... 28
5.7.2 Computing resources, software, and/ or data are corrupted ..... 28
5.7.3 Entity private key compromise procedures ..... 28
5.7.4 Business continuity capabilities after a disaster ..... 28
5.8 CA or RA termination ..... 29
6. Technical security controls ..... 30
6.1 Key pair generation and installation ..... 30
6.1.1 Key pair generation ..... 30
6.1.2 Private key delivery to subscriber ..... 30
6.1.3 Public key delivery to the certificate issuer ..... 30
6.1.4 CA public key delivery to relying parties ..... 30
6.1.5 Key sizes ..... 30
6.1.6 Public key parameters generation and quality checking ..... 30
6.1.7 Key usage purposes ..... 30
6.2 Private key protection and cryptographic module engineering controls ..... 30
6.2.1 Cryptographic module standards and controls ..... 31
6.2.2 Private key (n out of m) multi-person control ..... 31
6.2.3 Private key escrow ..... 31
6.2.4 Private key backup ..... 31
6.2.5 Private key archival ..... 31
6.2.6 Private key transfer into or from a cryptographic module ..... 31
6.2.7 Private key storage on cryptographic module ..... 31
6.2.8 Method of activating private key ..... 31
6.2.9 Method of deactivating private key ..... 31
6.2.10 Method of destroying private key ..... 31
6.2.11 Cryptographic module Rating ..... 32
6.3 Other aspects of key pair management ..... 32
6.3.1 Public key archival ..... 32
6.3.2 Certificate operational periods and key pair usage periods ..... 32
6.4 Activation data ..... 32
6.4.1 Activation data generation and installation ..... 32
6.4.2 Activation data protection ..... 32

6.4.3 Other aspects of activation data ..... 32
6.5 Computer security controls ..... 32
6.5.1 Specific computer security technical requirements ..... 33
6.5.2 Computer security rating ..... 33
6.6 Life cycle technical controls ..... 33
6.6.1 System development controls ..... 33
6.6.2 Security management controls ..... 33
6.6.3 Life cycle security controls ..... 33
6.7 Network security controls ..... 33
6.8 Time-stamping ..... 34
7. Certificate and CRL profiles ..... 35
7.1 Self-signed certificate ..... 35
7.2 Subordinate CA certificate ..... 37
7.3 Subordinate CA certificate（OCSP） ..... 40
7.4 OCSP server certificate ..... 44
7.5 CRL ..... 46
8. Compliance audit and other assessments ..... 48
8.1 Frequency or circumstances of assessment ..... 48
8.2 Identity/ qualifications of assessor ..... 48
8.3 Assessor's relationship to assessed entity ..... 48
8.4 Topics covered by assessment ..... 48
8.5 Actions taken as a result of deficiency ..... 48
8.6 Communication of results ..... 49
9. Other business and legal matters ..... 50
9.1 Fees ..... 50
9.2 Financial responsibility ..... 50
9.3 Confidentiality of business information ..... 50
9.3.1 Scope of confidential information ..... 50
9.3.2 Information not within the scope of confidential information ..... 50
9.3.3 Responsibility to protect confidential information ..... 50
9.4 Privacy of personal information ..... 50
9.5 Intellectual Property Right ..... 51
9.6 Representation and warranties ..... 51
9.6.1 Representations and warranties of IA and RA ..... 51
9.6.2 Subscriber representations and warranties ..... 51
9.6.3 Relying party representations and warranties ..... 51

9.6.4 Representations and warranties of other participants ..... 52
9.7 Disclaimers of warranties ..... 52
9.8 Limitations of liability ..... 52
9.9 Indemnities ..... 52
9.10 Term and termination ..... 52
9.10.1 Term ..... 52
9.10.2 Termination ..... 52
9.10.3 Effect of termination and survival ..... 52
9.11 Individual notices and communications with participants ..... 52
9.12 Amendments ..... 53
9.12.1 Procedure for amendment ..... 53
9.12.2 Notification method and period ..... 53
9.12.3 Circumstances under which OID must be changed ..... 53
9.13 Dispute resolution provisions ..... 53
9.14 Governing law ..... 53
9.15 Compliance with applicable law ..... 53
9.16 Miscellaneous provisions ..... 53
9.17 Other provisions ..... 53

# 1. Introduction

This document is the English version of " Japanese Government Public Key Infrastructure (GPKI) Application Certification Authority2(Root) Certificate Policy and Certification Practice Statement(March 11th, 2013　Approved by the Inter-ministerial Council of Government Information Systems)".　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 Authority2(Root)　(hereinafter referred to as “Application CA2(Root)”).

This is the top layer for the subordinate Certification Authority which issues server certificates, code signing certificates and document signing certificates.

These certificates enable implementation of encrypted communications between business servers of organizations including offices and ministries and signature on software and documents.

Application CA2 (Root) strive to comply with the latest version of AICPA/CICA, WebTrust Program for Certification Authorities and CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly.

This Application CA2 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 CA2(Root) issues subordinate CA certificate to GPKI Application Certification Authority2(Sub) (hereinafter referred to as “Application CA2(Sub)”).

The Application CA2(Root) 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 CA2(Root).

## 1.2 Document name and identification

The certificate policy of the Application CA2(Root) covers the certificate policy for the subordinate CA certificate of the Application CA2(Root).　The identifiers of the policies are as follows:

- Subordinate CA certificate policy:　0.2.440.100145.8.4.1.101.110

## 1.3 PKI participants

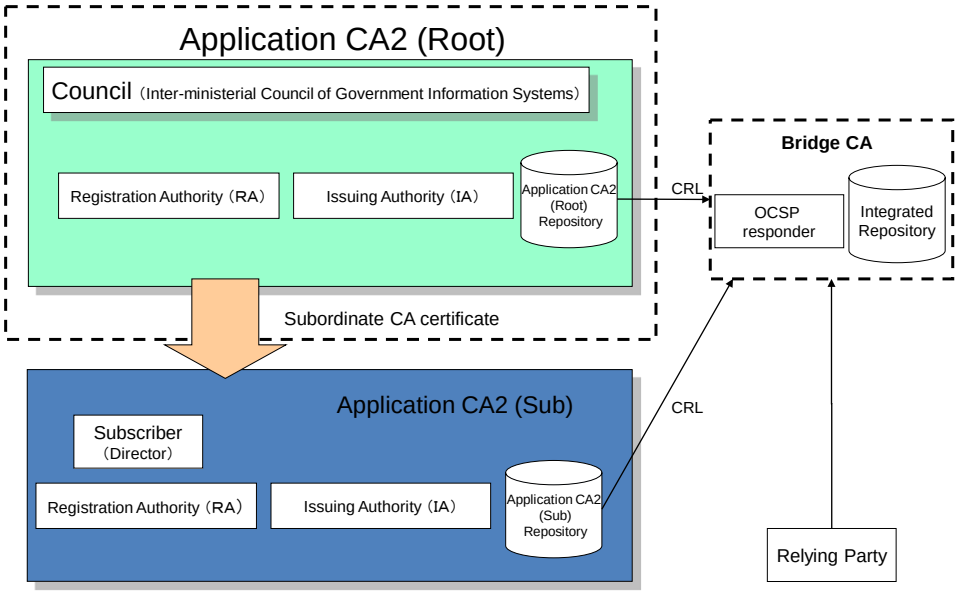


Fig. 1-1 Organization Diagram

### 1.3.1 Certification authorities

The Inter-Ministerial Council of Government Information Systems makes the decision concerning operations of the Application CA2(Root).

The role of the Governing Council in relation to Application CA2(Root) operations shall be as follows:

- Decision concerning the CP/CPS of the Application CA2(Root)
- Decision concerning action to CA private key compromise state
- Decision concerning action to emergencies such as occurrence of disasters

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

Application CA2(Root) director, IA key administrator, Reception personnel, and reviewer perform operation services such as administration of the CA private key.

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 CA2 director.

Application CA2 administrator, assistant Application CA2 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 Subscriber

The subscriber on this CP/ CPS is the Application CA2(Root) director.

The subscriber administers certificates issued from the Application CA2(Root), and uses the certificates in accordance with this CP/CPS.

#### 1.3.4 Relying parties

The relying party who verifies a certificate checks the validity of the certificate of subordinate CA certificate using the Certificate Revocation List (CRL) or OCSP responder issued by the Application CA2.

#### 1.3.5 Other participants involved

No stipulation

### 1.4 Certificate usage

The Application CA2(Root) as the top CA for subordinate CA issues the subordinate CA certificate to the Application CA2(Sub). When relying parties want to verify the certificate, they can do it based on the self-signed certificate.

### 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 CA2 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 CA2(Root).

### 1.5.4 CPS approval procedures

The Application CA2(Root)'s CP/CPS for the Application CA2(Root) 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 subordinate CA 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 CA2, 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.

- 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.

- OCSP（Online Certificate Status Protocol）

A name of protocol which is on-line base checking the validity of corresponding certificates.

An OCSP responder is a server which verifies the validity of a certificate specified by a relying party and returns the result for the verification of the certificate to the relying party.

The Application CA2(Root) provides the OCSP responder which is in accordance with RFC2560 and RFC5019.

- 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, CRL profiles, 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 because it is almost impossible to apply prime factor analysis to an integer produced by multiplying two sufficiently large, different prime numbers.

- SSL/TLS (Secure Socket Layer/Transport Layer Security)

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.509

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 CA2(Root) repository

  This is used to store certificates and CRL issued by the Application CA2(Root). (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

- subordinate CA certificate

  The public certificate issued by Application CA2(Root) ensures the trustworthy of the subordinate CA.

- 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.

- 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.

- 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 CA2 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 RFC5280.

- 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 CA2(Root) 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 CA2(Root) registers the following information held in the Application CA2(Root) repository in the integrated repository and publishes them:

- Self-signed certificate of the Application CA2(Root)
- CRL

(2) The publication in web site

The Application CA2(Root) publishes the following information on web site:

- Self-signed certificate of the Application CA2(Root) and its finger print
- Information about the CA private key compromises
- The CP/CPS and their revision history

(3) The publication in OCSP responder

The Application CA2(Root) provides the OCSP responder to verify the status of the certificate for the relying party by on-line.

## 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 CA2(Root) 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 CA2(Root) shall be determined according to the format of the X.500 Distinguished Name (DN).

### 3.1.2 Need for names to be meaningful

The name used in a Subordinate CA certificate is the name of an Application CA2(Sub).

### 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 CA2(Root).

### 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 subordinate CA certificate, the Application CA2(Root) 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 subordinate CA certificate, the Application

CA2(Root) shall verify the authenticity of the organization to which the subscriber belongs based on the prescribed procedure.

#### 3.2.3 Authentication of individual identity

The Application CA2(Root) does not issue certificates to individuals.

#### 3.2.4 Non-verified subscriber information

No stipulation

#### 3.2.5 Validation of authority

The appropriateness of authority is confirmed according to the procedures defined in "3.2.2 Authentication of organization 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".

# 4. Certificate life-cycle operational requirements

## 4.1 Certificate application

### 4.1.1 Who can submit a certificate application

The Application CA2(sub) director shall perform application of the subordinate CA certificate.

### 4.1.2 Enrollment process and responsibilities

The Application CA2(sub) director shall perform application of the subordinate CA certificate and the director shall apply accurate appropriate information on their certificate applications.

## 4.2 Certificate application processing

The Application CA2(Root) shall check whether the application contents registered are appropriate in accordance with the implementation of the procedure defined in "3.2.1 Method to prove possession of private key" and "3.2.2 Authentication of organization identity" .

## 4.3 Certificate issuance

The Application CA2(Root) signs to the certificate subscription request of the Application CA2(Sub) with the CA private key then issues a subordinate CA certificate.

## 4.4 Certificate acceptance

The subscriber shall check the contents of the subordinate CA certificate without delay. If the subscriber detects any problems, the subscriber shall notify the Application CA2(Root) about the problem.

The Application CA2(Root) assumes acceptance of the subordinate CA certificate to be completed If the subscriber doesn't notify about the 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 subordinate CA certificate in accordance with this CP/CPS.

- Administer the subordinate CA certificate and private key corresponding to the certificates safely.
- Inform the Governing Council about 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 subordinate CA certificate is obliged to:

- Check the use purpose of the subordinate CA certificate.
- Check that the subordinate CA certificate are not tampered.
- Verify the validation of the subordinate CA certificate.

### 4.6 Certificate Renewal

When the Subordinate CA certificate renewal is needed, renewal is processed in accordance with the procedure defined in "4.2 Certificate application processing" and "4.3 Certificate issuance".

### 4.7 Certificate re-key

No stipulation

### 4.8 Certificate modification

When the cases that the subordinate CA certificate information are modified, the subordinate CA certificate shall be issued according to the procedures stipulated in "4.2 Certificate application processing" and "4.3 Code signing certificate". When a subordinate CA 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 Conditions for revocation

The subordinate CA certificate is revoked when the following certificate revocation reasons occurred for the Application CA2(Root) or the Application CA2(Sub) :

- Compromise of CA private key.
- Violation of CP/CPS
- End of authentication business
- Modification of contents described in the certificate.

#### 4.9.2 Who can request revocation

The Application CA2(Sub) director shall perform revocation of the subordinate CA certificate.

#### 4.9.3 Procedure for revocation request

The Application CA2(Root) shall check whether the application contents registered are appropriate in accordance with the implementation of the procedure defined in "3.2.2 Authentication of organization identity".

The Application CA2(Root) shall perform revocation processing of the subordinate CA certificate and register the CRL in the integrated repository.

#### 4.9.4 Revocation request grace period

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

#### 4.9.5 Time period which CA must process the revocation request

The Application CA2(Root) shall proceed revocation application procedure immediately.

When an already-issued certificate is revoked, its revocation processing is not cancelled.

#### 4.9.6 Revocation checking requirement for relying parties

The relying party shall check the validity of a trusting and using certificate. The Application CA2(Root) publishes the CRL in the integrated repository and provides the OCSP responder so that the validity can be checked.

#### 4.9.7 CRL issuance frequency

The Application CA2(Root) issues CRL within 90days after the previous issuance of CRL.

#### 4.9.8 Maximum latency for CRLs

The Application CA2(Root) reflects the issued CRL on the integrated repository promptly.

#### 4.9.9 On-line revocation/ status checking availability

The BCA maintains and administers the integrated repository and the OCSP responder. And the OCSP responder provides verification means for a certificate status by on-line.

#### 4.9.10 On-line revocation checking requirements

The validity of a certificate shall be checked either by the CRL which is published in the integrated repository or the OCSP responder which provides the status of the certificate.

#### 4.9.11 Other forms of available revocation information

No stipulation

#### 4.9.12 Special requirements related to key compromise

When CA private key of the Application CA2(Sub) is compromised, it will be revoked immediately and report to the Governing Council.

#### 4.9.13 Circumstances for suspension

The Application CA2(Root) does 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

#### 4.10.1 Feature in operation

The status of a certificate can be checked using the CRL or the OCSP responder.

#### 4.10.2 Service availability

The integrated repository and the OCSP responder are operated 24x7. Operation may be temporarily stopped by maintenance,etc.

#### 4.10.3 Optional specification

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 Application CA2(Root) 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 Application CA2(Root) 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 CA2(Root) director as stipulated in "5.2 Procedural controls".

Security guards shall be stationed in the Application CA2(Root) facilities, and it shall also be monitored 24x7 by surveillance systems.

### 5.1.3 Power and air conditioning

The Application CA2(Root) 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 Application CA2(Root) 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 Application CA2(Root) 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 Application CA2(Root) 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 Application CA2(Root) 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 Application CA2(Root) shall dispose documents and memory devices that contain confidential information of in accordance with the prescribed procedures.

#### 5.1.9 Offsite backup

When the Application CA2(Root) stores media of important data at an off-site location separate from the Application CA2(Root) facilities, the Application CA2(Root) shall assure security of a transport route, also device a security countermeasure, commensurate to that of the Application CA2(Root) facilities, to the facility in which the media are retained.

### 5.2 Procedural control

#### 5.2.1 Trusted roles

(1) Application CA2 director

Application CA2 director is responsible for operation of the Application CA2(Root) and performs:

- Establishment of Application CA2 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 CA2(Root) 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 accepts applications and adjusts communication with applicants, and administers application documents.

(4) Reviewer

Reviewer shall perform reviews of applications.

(5) Application CA2 administrator

Application CA2 administrator is responsible for operations of the Application CA2(Root) 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 CA2(Root)
- Control of a key required for HSM operations (hereafter referred to as "operation key")

(6) Assistant application CA2 administrator

The assistant application CA2 administrator is acting Application CA2 administrator, and shall perform the following task in place of Application CA2 administrator:

- Provision of work instructions to senior IA operators and general IA operators, and confirmation of results
- Operations control of the Application CA2(Root)
- Control of the operation key required for HSM operations

(7) Senior IA operator

Senior IA operators perform the following task related to the Application CA2(Root) 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 CA2(Root) system start and stop
- Application CA2(Root) repository start and stop
- Administration of the Application CA2(Root) system reconfiguration
- Administration of system reconfiguration relating to database backups, restoration and archive operations for the Application CA2(Root) system

(8) General IA operator

General IA operators perform the following task related to certificates issued from the Application CA2(Root) system. The operations shall be performed by multiple general IA operators.

- Registration and modification of the certificate policy
- Processing of issues, re-keys and revocations for operator certificates
- Issues, re-keys and revocations of subordinate CA certificates to Application CA2(Sub).
- Issues, re-keys and revocations of OCSP server certificates to OCSP responder.
- Administration of Application CA2(Root) 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 CA2(Root) system and

Application CA2(Root) repository (hereafter referred to as "audit log"):

- Audit log inspect
- Deletion of unnecessary audit log

#### 5.2.2 Number of persons required per task

In the Application CA2(Root), 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 CA2 administrator from Application CA2 director.

Application CA2 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 CA2(Root) 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 CA2(Root) 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 CA2(Root) system and the Application CA2(Root) repository are recorded in the audit logs including the access

log and operations 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 seven 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 CA2(Root) 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 within every 17years.

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 Application CA2(Root) 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 are 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 subordinate CA certificate
- Discarding and re-generating of the CA private key
- Reissuing of subordinate CA certificate

When CA private key of Application CA2(Sub) is compromised, it will be revoked immediately and report to the Governing Council.

### 5.7.4 Business continuity capabilities after a disaster

If the Application CA2(Root) 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 Application CA2(Root) 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 CA2(Root), the Application CA2(Root) shall notify about the storage organization and the disclosure method and the Application CA2(Root)'s backup and archive data, no later than 90 days before the termination of operations. Then the Application CA2(Root) performs 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.

### 6.1.2 Private key delivery to subscriber

The Application CA2(Root) does not deliver a private key to the subscriber.

### 6.1.3 Public key delivery to the certificate issuer

The public key of the Application CA2(Sub) is delivered by hand securely.

### 6.1.4 CA public key delivery to relying parties

The Application CA2(Root) 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.

### 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.

## 6.2 Private key protection and cryptographic module engineering controls

#### 6.2.1 Cryptographic module standards and controls

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

#### 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

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

#### 6.2.8 Method of activating private key

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

#### 6.2.9 Method of deactivating private key

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

#### 6.2.10 Method of destroying private 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.

#### 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

The public and private keys of the Application CA2(Root) shall be valid for 20 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

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.

#### 6.4.2 Activation data protection

The operation key and password required to activate the HSM in which the CA private key is stored shall be retained safely by the Application CA2(Root).

#### 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 CA2(Root) 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 CA2(Root) 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 CA2 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 CA2(Root) 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 Application CA2(Root) shall check development, operation, and maintenance of the 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 CA2(Root) repository shall be copied in the BCA integrated repository through a firewall. Proper security control measures shall be implemented to prevent unauthorized access or retrieval.

## 6.8 Time-stamping

The Application CA2(Root) 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

Table 7-1 Application CA2(Root) self-signed certificate

| Area name | Critical flag | Value | Description |
|---|---|---|---|
| Version<br>(version number) | | 2 | v3 integer |
| serial Number<br>(serial number) | | Example: 1 | Certificate serial number, integer |
| signature algorithm ID<br>(signature algorithm) | | | Application CA2(Root) signature algorithm |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| issuer name<br>(issuer name) | | cn=ApplicationCA2 Root,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Application CA2(Root) distinguished name (DN) in English PrintableString |
| validity period<br>(certificate validity period) | | | Validity period of certificate |
| notBefore<br>(issue date) | | Example: 010401000000Z | Start date of certificate validity periodYYMMDDHHMMSSZ |
| notAfter<br>(termination date) | | Example: 210401000000Z | Termination date of certificate validity period YYMMDDHHMMSSZ |
| subject name<br>(subject name) | | cn=ApplicationCA2 Root,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Application CA2(Root) distinguished name (DN) in English PrintableString |

| | | | |
|---|---|---|---|
| subject public key info<br>(subject public key information) | | | Public key algorithm |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.1 | Application CA2(Root) public key algorithm identifier, RSA Encryption |
| parameter<br>(parameter) | | NULL | No value for RSA |
| public key<br>(public key) | | BIT STRING | Application CA2(Root) public key, bit string |
| extensions<br>(certificate extension area) | | | |
| subjectKeyIdentifier<br>(subject key identifier) | FALSE | OCTET STRING | Subject key identifier |
| keyUsage<br>(key usage) | TRUE | | A key usage purpose is specified. |
| keyCertSign | | 1 | [5] |
| cRLSign | | 1 | [6] |
| subjectAltName<br>(subject alternative name) | FALSE | cn=アプリケーション CA2 Root,<br>ou=政府認証基盤,<br>o=日本国政府,<br>c=JP | Application CA2(Root) distinguished name (DN) in Japanese UTF8String |
| basicConstraints<br>(basic constraints) | TRUE | | Distinction between CA certificates and end entity certificate |
| cA | | cA=TRUE | Required (MUST) |
| issuer's signature<br>(issuer signature) | | | Digital signature of Application CA2(Root) |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | Sha256WithRSAEncryption |
| | ENCRYPTED (signature value) | | |

## 7.2 Subordinate CA certificate

Table 7-2 Application CA2(Root) Subordinate CA certificate

| Area name | Critical flag | Value | Description |
|---|---|---|---|
| version<br>(version number) | | 2 | v3 integer |
| serial Number<br>(serial number) | | Example: 1 | Certificate serial number, integer |
| signature algorithm ID<br>(signature algorithm) | | | Subordinate CA signature algorithm |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| issuer name<br>(issuer name) | | cn=ApplicationCA2 Root,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Application CA2(Root) distinguished name (DN) in English<br>PrintableString |
| validity period<br>(certificate validity period) | | | Validity period of certificate |
| notBefore<br>(starting date) | | Example: 010401000000Z | Start date of certificate validity period<br>YYMMDDHHMMSSZ |
| notAfter<br>(termination date) | | Example: 110401000000Z | Termination date of certificate validity period<br>YYMMDDHHMMSSZ |
| subject name<br>(subject name) | | Example:<br>cn=ApplicationCA2 Sub,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Subordinate CA distinguished name (DN) in English<br>PrintableString |
| subject public key info<br>(subject pubic key information) | | | Public key algorithm |

| | | | |
|---|---|---|---|
| algorithm identifier (algorithm identifier) | | 1.2.840.113549.1.1.1 | Subordinate CA public key algorithm identifier, RSA Encryption |
| parameter (parameter) | | NULL | No value for RSA |
| public key (public key) | | BIT STRING | Subordinate CA public key, bit string |
| extensions (certificate extension area) | | | |
| authorityKeyIdentifier (certification authority key identifier) | FALSE | | Certification authority key identifier |
| keyIdentifier | | OCTET STRING | Application CA2(Root) key identifier |
| 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] |
| certificatePolicies (certificate policy) | FALSE | | |
| policyIdentifier | | | OID |
| certPolicyId | | 0.2.440.100145.8.4.1.101.110 | Subordinate CA certificate policy OID id-apca-cp-tls.subca110 |
| policyQualifiers | | | Policy qualifiers (pointer to CPS or user notification information) |
| policyQualifierId | | id-qt-cps | CPS |
| qualifier | | http://www.gpki.go.jp/apca2/cpcps/index.html | Application CA2(Root)CPS URI, IA5 string |

| | | | |
|---|---|---|---|
| subjectAltName<br>(subject alternative name) | FALSE | Example:<br>cn=アプリケーション CA2 Sub,<br>ou=政府認証基盤,<br>o=日本国政府,<br>c=JP | Subordinate CA distinguished name (DN) in Japanese UTF8String |
| issuerAltName<br>(issuer alternative name) | FALSE | Example:<br>cn=アプリケーション CA2 Root,<br>ou=政府認証基盤,<br>o=日本国政府,<br>c=JP | Application CA2(Root) distinguished name (DN) in Japanese, UTF8String |
| basicConstraints<br>(basic constraints) | TRUE | | Distinction between CA certificates and end entity certificate |
| cA | | cA=TRUE | Required (MUST) |
| pathLenConstraint | | pathLenConstraint = 0 | The numbers of sub-subordinate CA certificates in the authentication path. |
| cRLDistributionPoints<br>(CRL distribution points) | FALSE | | |
| distributionPoint | | | Distribution point |
| fullName<br>(non abbreviated name) | | http://dir2.gpki.go.jp/ApplicationCA2Root.crl | CRL distribution point is specified by URI. IA5 string |
| distributionPoint | | | Distribution Point Name |
| fullName<br>(non abbreviated name) | | http://dir2.gpki.hq.admix.go.jp/ApplicationCA2Root.crl | CRL distribution point is specified by URI. IA5 string |
| issuer's signature<br>(issuer signature) | | | Digital signature of Application CA2 Root |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| | ENCRYPTED (signature value) | | |

7.3 Subordinate CA certificate（OCSP）

Table 7-3 Subordinate CA certificate（OCSP）

| Area Name | Critical flag | Value | Description |
|---|---|---|---|
| version<br>(version number) | | 2 | v3integer |
| serial Number<br>(serial number) | | Example: 1 | Certificate serial number, integer |
| signature algorithm ID<br>(signature algorithm) | | | Subordinate CA signature algorithm |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| issuer name<br>(issuer name) | | cn=ApplicationCA2 Root,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Application CA2(Root) distinguished name(DN) in English<br>PrintableString |
| validity period<br>(certificate validity period) | | | Validity period of certificate |
| notBefore<br>(issue date) | | Example: 141201000000Z | Start date of certificate validity period<br>YYMMDDHHMMSSZ |
| notAfter<br>(termination date) | | Example 241201000000Z | Termination date of certificate validity period<br>YYMMDDHHMMSSZ |
| subject name<br>(subject name) | | Example:<br>cn=ApplicationCA2 Sub,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Subordinate CA distinguishedname(DN) in English<br>PrintableString |
| subject public key info<br>(subject public key information) | | | Public key algorithm |

| | | | |
|---|---|---|---|
| algorithm identifier (algorithm identifier) | | 1.2.840.113549.1.1.1 | Subordinate CA public key algorithm identifier、RSA Encryption |
| parameter (parameter) | | NULL | No value for RSA |
| public key (public key) | | BIT STRING | Subordinate CA public key, bit string |
| extensions (certificate extension area) | | | |
| authorityKeyIdentifier (Certificate CA key identifier) | FALSE | | Certificate CA key identifier |
| keyIdentifier | | OCTET STRING | Application CA2(Root) key identifier |
| 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] |
| certificatePolicies (certificate policies) | FALSE | | |
| policyIdentifier | | | OID |
| certPolicyId | | 0.2.440.100145.8.4.1.101.110 | Subordinate CA certificate policy OID id-apca-cp-tls.subca110 |
| policyQualifiers | | | Policy qualifiers (pointer to CPS or user notification information) |
| policyQualifierId | | id-qt-cps | CPS |
| qualifier | | http://www.gpki.go.jp/apca2/cpcps/index.html | Application CA2(Root) CPS URI、IA5 string |

| | | | |
|---|---|---|---|
| subjectAltName (subject alternative name) | FALSE | Example: cn=アプリケーション CA2 Sub, ou=政府認証基盤, o=日本国政府, c=JP | Subordinate CA distinguishedname（DN） in Japanese, UTF8String |
| issuerAltName （issuer alternative name） | FALSE | Example: cn=アプリケーション CA2 Root, ou=政府認証基盤, o=日本国政府, c=JP | Application CA2(Root) distinguished name（DN） in Japanese, UTF8String |
| basicConstraints (basic constraints) | TRUE | | Distinction between CA certificates and end entity certificate |
| cA | | cA=TRUE | Required (MUST) |
| pathLenConstraint | | pathLenConstraint = 0 | The numbers of sub-subordinate CA certificates in the authentication path. |
| cRLDistributionPoints (CRL distribution points) | FALSE | | |
| distributionPoint | | | Distribution point |
| fullName (non abbreviated name) | | http://dir2.gpki.go.jp/ApplicationCA2Root.crl | CRL distribution point is specified by URI. IA5string |
| distributionPoint | | | DistributionPointName |
| fullName (non abbreviated name) | | http://dir2.gpki.hq.admix.go.jp/ApplicationCA2Root.crl | CRL distribution point is specified by URI. IA5string |
| authorityInfoAccess (authority info access) | FALSE | | |
| accessMethod | | id-ad-ocsp | OCSP |
| accessLocation | | http:// ocsp-root.gpki.go.jp | OCSP responder is specifiedby URI, IA5string |
| issuer's signature (issuer's signature) | | | Application CA2（Root） digital signature |

| | | | |
|---|---|---|---|
| algorithm identifier (algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| | ENCRYPTED (signature value) | | |

7.4 OCSP server certificate

Table 7-4 OCSP server certificate

| Area name | Critical flag | Value | Description |
|---|---|---|---|
| version<br>(version number) | | 2 | v3integer |
| serial Number<br>(serial number) | | Example: 1 | Certificate serial number, integer |
| signature algorithm ID<br>(signature algorithm) | | | OCSP server certificate signature algorithm |
| algorithm identifier<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| issuer name<br>(issuer name) | | cn=ApplicationCA2 Root,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | Application CA2（Root）distinguished name(DN) in English |
| validity period<br>(certificate validity period) | | | Validity period of certificate |
| notBefore<br>(issue date) | | Example: 141201000000Z | Start date of certificate validity period<br>YYMMDDHHMMSSZ |
| notAfter<br>(termination date) | | Example: 150401000000Z | Termination date of certificate validity period<br>YYMMDDHHMMSSZ |
| subject name<br>(subject name) | | Example:<br>cn=ApplicationCA2 Root OCSP Responder,<br>ou=GPKI,<br>o=Japanese Government,<br>c=JP | OCSP server certificate distinguished name(DN) in English |
| subject public key info<br>(subject public key information) | | | Public key algorithm |

| | | | |
|---|---|---|---|
| algorithm identifier (algorithm identifier) | | 1.2.840.113549.1.1.1 | OCSP server certificate public key algorithm identifier, RSA Encryption |
| parameter (parameter) | | NULL | No value for RSA |
| public key (public key) | | BIT STRING | OCSP server certificate public key, bit string |
| extensions (certificate extension area) | | | |
| authorityKeyIdentifier (certification authority key identifier) | FALSE | | Certification authority key identifier |
| keyIdentifier | | OCTET STRING | Application CA2(Root) 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 | FALSE | | |
| KeyPurposeId | | id-kp-ocspsigning | OCSPsigning |
| certificatePolicies (certificate policies) | FALSE | | |
| policyIdentifier | | | OID |
| certPolicyId | | 0.2.440.100145.8.4.1.102.141 | OCSP server certificate Policy OID id-apca-cp-ocsp.class141 |
| policyQualifiers | | | Policy qualifiers (pointer to CPS or user notification information) |
| policyQualifierId | | id-qt-cps | CPS |
| qualifier | | http://www.gpki.go.jp/apca2/cpcps/index.html | Application CA2（Root）CPS URI、IA5string |

| | | | |
|---|---|---|---|
| id-pkix-ocsp-nocheck | FALSE | | No need to verify OCSP certificate |
| issuer's signature<br>(issuer's signature) | | | ApplicationCA2（Root）digitalsignature |
| algorithm identifier<br>(アルゴリズム識別子) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| | ENCRYPTED (signature value) | | |

## 7.5 CRL

Table 7-5 Application CA2(Root) Certificate Revocation List

| Area name | Critical flag | Value | Description |
|---|---|---|---|
| version<br>(version number) | | 1 | v2 CRL integer |
| signature<br>(signature algorithm) | | | Signature algorithm |
| algorithmIdentifier | | | Algorithm identifier and signature algorithm area (signatureAlgorithm) are made equal. |
| algorithm<br>(algorithm identifier) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| issuer<br>(issuer) | | cn=ApplicationCA2 Root, ou=GPKI, o=Japanese Government, c=JP | Application CA2(Root) distinguished name (DN) in English<br>Printable string |
| thisUpdate<br>(update date of this time) | | Example:<br>010501000000Z | Update date and time of this time<br>YYMMDDHHMMSSZ |
| nextUpdate<br>(update date of the next time) | | Example:<br>010730000000Z | Update date and time of the next time<br>YYMMDDHHMMSSZ |
| revokedCertificates | | | Revoked certificate entry |

| | | | |
|---|---|---|---|
| (revoked certificate) | | | (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 CA2(Root) key identifier |
| cRLNumber (CRL number) | FALSE | Example: 32 | Sequence number, integer |
| | ENCRYPTED (signature value) | | |

# 8. Compliance audit and other assessments

The Application CA2(Root) shall have a compliance audit mechanisms in place to ensure that the requirements of this Application CA2(Root) are being implemented and enforced as defined in "8.1 Frequency or circumstances of assessment" and "8.6 Communication of results".

## 8.1 Frequency or circumstances of assessment

The Application CA2(Root) shall have audits carried out annually by an auditor. If necessary, the Application CA2(Root) shall conduct other audits in addition to the regular audits.

## 8.2 Identity/ qualifications of assessor

The Application CA2(Root) 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 Application CA2(Root) shall be selected as the auditor for the Application CA2(Root).

## 8.4 Topics covered by assessment

Audit shall be carried out primarily to ascertain of the Application CA2(Root) 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 Application CA2(Root) shall take immediate action as determined by the Governing Council. 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 Governing Council shall decide whether or not to suspend the Application CA2(Root) 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 Governing Council shall confirm that the Application CA2(Root) has taken

actions in response to the deficiencies.

### 8.6 Communication of results

The results of the Application CA2(Root) audits shall be submitted by the auditor as reports to the Application CA2 director, which shall, in turn, report audit results to the Governing Council.

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 CA2(Root) shall treat information as confidential if its disclosure could harm the credibility and integrity of the authentication operations of the Application CA2(Root).

### 9.3.2 Information not within the scope of confidential information

Of the information held by the Application CA2(Root), 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 "Act on the Protection of Personal Information Held by Administrative Organs", "Order for the enforcement of the Act on the Protection of Personal Information Held by Administrative Organs" and so on.

The Application CA2(Root) 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 CA2(Root).

## 9.4 Privacy of personal information

Personal information shall be protected appropriately according to "Act on the Protection of Personal Information Held by Administrative Organs", "Order for the

enforcement of the Act on the Protection of Personal Information Held by Administrative Organs " and so on.

## 9.5 Intellectual Property Right

The intellectual property rights of the CA key pair, subordinate CA certificate, CRL, self-signed certificate, and this CP/CPS belong to the Application CA2(Root).

However, it is not always true for the intellectual property rights of the key pairs and the subject names in subordinate CA certificate.

## 9.6 Representation and warranties

### 9.6.1 Representations and warranties of IA and RA

The Application CA2(Root) shall have following representations and warranties related to CA operations:

- Issuance, re-key, and revocation of self-signed certificates, subordinate CA certificate in accordance with this CP/CPS.
- Publication of information defined in "2.2 Publication of certification information"
- The Application CA2(Root) shall control the CA private key securely.
- If it shall be occurred the CA private key compromise, the Application CA2(Root) shall quickly publish information of the compromise event.
- The Application CA2(Root) shall store audit logs and archive data concerning certificate issues, re-keys and revocation, for the required period.

### 9.6.2 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.

### 9.6.3 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".

#### 9.6.4 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 Governing Council.

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

#### 9.10.2 Termination

When the Application CA2 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 CA2(Root) 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 CA2(Root) 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