Public Certification Service for Individuals by Local Government

Okayama-ken Certificate Authority Certification Practice Statement

Ver. 1 . 5

July 8, 2013

Okayama Prefecture

History of revision

Ver	Date	Contents of Revision
1.0	January 29, 2004	First version
1.1	January 19, 2005	Revision incidental to the revision of enforcement regulations etc.
1.2	November 1, 2006	Revision incidental to a legal reform
1.3	September 19, 2008	Revision incidental to the update of Private Key of Certificate Authority etc.
1.4	April 12, 2010	Revision incidental to the change of contact address
1.5	July 8, 2013	Revision incidental to the enforcement of the Act to Partially Change the Basic Resident Registration Act (Act No.77 of 2009)

1. Introduction

This Practice Statement shall stipulate the operation policies concerning the certification business of JPKI prefectural Certificate Authority of Okayama prefecture (hereinafter called "Okayama-ken CA"), which issues the Electronic Certificate (The certificate of a user shall be called "Electronic Certificate" hereinafter) etc. of a person who is recorded in the basic resident registration to facilitate the computerization of procedures such as applications, reporting etc. between residents and national or local public authorities. The composition of this Practice Statement is compliant with RFC (Request For Comments) 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" issued by the Internet Engineering Task Force's (IETF) Public-Key Infrastructure X.509 (PKIX) Working Group. However, as for the part where other rules should be seen, only the title shall be shown and the reference contents shall be shown clearly.

1-1 General

Okayama-ken CA shall issue the Electronic Certificate to a person who is recorded in the basic resident registration kept by the municipality in response to application; issue certificates required for the operation of Okayama-ken CA, and issue and exchange Cross Certificates with the JPKI Bridge Certificate Authority (hereinafter called "JPKI BCA"), which is established to implement cross-certification with other prefectural CA concerning the Public Service for Individuals and GPKI CA. Also, it shall create revocation information (Information concerning the revocation of Electronic Certificate etc. The same shall apply hereinafter.); the revocation record (CRL/ARL) (List where information concerning the revocation of Electronic Certificate is recorded. The same shall apply hereinafter); and the revocation information file (Archive of revocation record (CRL) The same shall apply hereinafter).These will be provided upon request of a signature verifier specified in Paragraph 4, Article 17 of the Act on Certification Business of Local Governments in Relation to Electronic Signatures (hereinafter called the Basis Law) or a group signature verifier specified in Paragraph 6 of the same article. Finally, Okayama-ken CA shall not deem that Certificate Policy (CP) and Certification Practice Statement (CPS) are independent entities, but designate this Practice Statement as an operation policy on the certification business of Okayama-ken CA.

1-2 Identification

The numerical identifiers of CP of Okayama-ken CA shall be as follows.

Okayama-ken CA Electronic Certificate Policy etc.

Electronic Certificate Policy and Okayama-ken CA Cross Certificate Policy

1.2.392.200149.8.5.1.1.10

Electronic Certificate Policy and Okayama ken CA Cross Certificate Policy for Tests

1.2.392.200149.8.5.1.0.10

Official Status Certificate Validation Server Certificate Policy

1.2.392.200149.8.5.1.200

Official Status Certificate Validation Server Certificate Policy for Tests

1.2.392.200149.8.5.1.0.200

OCSP Responder Certificate Policy

1.2.392.200149.8.5.1.300

1-3 Operational Structure and Scope of Certificate

1-3-1 Persons concerned

(1) Minister of Internal Affairs and Communications

The Minister of Internal Affairs and Communications shall appoint the designated certification authority under the provisions of the Basis Law.

(2) Prefectural Association for JPKI

The Prefectural Association for JPKI (hereinafter called "the Association") shall be responsible for administrative matters such as communications and oversee vital matters related to the operation of the system of the Public Certification Service for Individuals.

(3) Governor of Okayama prefecture

The Governor of Okayama prefecture shall prepare the function of Okayama-ken CA (Certificate Authority of Okayama prefecture) shown in the following.

(4) Okayama-ken CA

Okayama-ken CA shall issue certificates and ensure management of revocation information such as issuance of the Electronic Certificate and other certificates, creation of revocation records (CRL/ARL) and provision of the means to check the validity of the Electronic Certificate in cooperation with the mayor of the municipality. In addition, it shall make a response to the compromise of Private Key of the Governor of Okayama prefecture and to emergency situations such as accident occurrence etc. It shall also provide the means to check the validity of the Official Status Certificate and the Professional Status Certificate, which are required for the validation of the electronic signature of the document which a user receives online from a national or local public authority

(5) JPKI BCA

JPKI BCA shall issue the certificate to implement cross-certification with prefectural CA and Government Public Key Infrastructure Bridge CA (hereinafter called GPKI BCA) according to the Practice Statement which the Association develops.

(6) Designated Certification Authority

The designated certification authority shall be entrusted by the Governor of Okayama prefecture and conduct administrative operations concerning the implementation of certification business (hereinafter called "certification work") under the provisions of the Basis Law.

(7) Mayor of Municipality

The mayor of municipality of Okayama prefecture shall receive applications for issuance or revocation of the Electronic Certificate; shall implement the identity verification of an applicant; and shall deliver the Electronic Certificate which Okayama-ken CA issues to an applicant.

(8) Applicant / User

An applicant shall be a person who files an application for the issuance of the Electronic Certificate etc. according to Paragraph 1, Article 3 of the Basis Law. (An application may be done by a proxy. However, in this case, the requirement of Article 5 of Ordinance for Enforcement of the Act on Certification Business of Local Governments in Relation to Electronic Signatures

(hereinafter called “the Ordinance of the Basis Law”) should be satisfied.). A user shall be a person who is recorded in the basic resident registration and who has obtained the Electronic Certificate.

A user may use the Electronic Certificate in online applications, reporting etc. to national or local public authorities. A user may request the Governor of Okayama prefecture or designated certification authority to disclose user’s certification business information (record of issuance of the Electronic Certificate, revocation information and revocation file, the same shall apply hereinafter.), and correct, add or delete all or part of the certification business information concerning said disclosure. Also, if a user disagrees with the certification work etc., a user may request the Minister of Internal Affairs and Communications to conduct an investigation based on the Administrative Appeal Act. A user shall check the validity of the Official Status Certificate and the Professional Status Certificate required for the validation of electronic signature of the document a user received online from national or local public authorities

(9) Signature Verifier

A person among the following persons or organizations who gave notification regarding the reception of the provision of the means to check the validity of the Electronic Certificate in advance according to Paragraph 1, Article 17 of the Basis Law and was given access rights.

① Administrative agency etc. specified in Paragraph 2, Article 2 of the Act on Use of Information and Communications Technology in Administrative Procedures (hereinafter “Administrative Agency etc.”) .

② Court

③ A person who is appointed, registered, and certified or accredited as a person who is provided with the necessary matters accompanying procedures such as application and reporting etc. to administrative agencies in electronic form, and who provides them to administrative agencies, or who answers inquiries by the administrative office under the provisions of the law.

④ A certified certification business operator specified in Article 8 of “the Act on Electronic Signatures and Certification Business” (hereinafter “Electronic Signature Act”).

⑤ A person who implements the specified certification business specified in Paragraph 3, Article 2 of the Electronic Signature Act and is accredited as a person who meets the standards specified in Order for Enforcement of the Act on Certification Business of Local Governments in Relation to Electronic Signatures (hereinafter “the Order of the Basic Law”) by the Minister of Internal Affairs and Communications.

⑥ A group which provides electronic records required for procedures such as applications, reporting etc. to administrative agencies and courts and is designated by the Order of the Basic Law.

A signature verifier shall be provided with the means to check the validity of the Electronic Certificate through, for example the provision of the revocation record (CRL/ARL) by Okayama prefecture CA and signature verifier shall verify the Electronic Certificate concerning online application and reporting by a user.

(10) Signature Checker

A person who is designated by the Order of the Basis Law under the provision of Paragraph 5, Article 17 of the Basic Law.

A signature checker shall be provided with the confirmation results of the verification of validity of the Electronic Certificate by the following group signature verifier and shall verify the Electronic Certificate concerning online application and reporting etc. form a user.

(11) Group Signature Verifier

A person among the following persons or organizations gave notification regarding the reception of the provision of the means to check the validity of the Electronic Certificate in advance according to Paragraph 5, Article 17 of the Basis Law and was given access rights.

① A group for which a person implements procedures such as application, reporting etc. to

administrative agencies and a court at the request of anyone else in accordance with the provision of the law and which is specified by the Order of the Basis Law.

② A group or an organization where a person carries out procedures such as providing electronic records required for application, reporting etc. to administrative agencies and a court and which is specified by the Order of the Basic Law.

A group signature verifier shall be provided with the means to check the validity of the Electronic Certificate such as provision to said party of the revocation record (CRL/ARL) by Okayama ken CA; shall check the validity of the Electronic Certificate (usually attached to the online application) and report of a user received from a signature checker, and the result shall be sent to the signature checker.

(12) Signature Verifier etc.

Signature verifier and Group signature verifier

1-3-2 Applicability / Application Environment

The types and use of the service shall be as follows.

① Issuance of the Electronic Certificate for the following applications

- Electronic signatures for online applications/reporting of procedures conducted by administrative agencies and courts
- Identity verification which a signature verifier etc. implements
- Identity verification which a signature checker implements. Note that the validity period of the Electronic Certificate shall be 3 years after the date of issuance.

② Issue of the Cross Certificate for the following use

- Cross certification with GPKI BCA via JPKI BCA. Note that the validity period of the Cross Certificate shall be 5 years after the date when the Cross Certificate becomes effective.

③ Issuance of the Official Status Certificate Validation Server Certificate for the following applications

- Provision of the means to check the validity of the Official Status Certificate or the Professional Status Certificate which is required for the validation of an electronic signature of the document received by a user online from national or local public authorities.

Please note that the validity period of Official Status Certificate Validation Server Certificate shall be 1 year from the date when the Official Status Certificate Validation Server Certificate becomes effective.

④ Issuance of the OCSP Responder Certificate for the following application

- When signature verifiers etc. provide the means to check the validity of the Electronic Certificate through the OCSP Responder inquiry method

Please note that the validity period of the OCSP Responder Certificate shall be 1 year from the date when the OCSP Responder Certificate becomes effective.

1-3-3 Responsible Person of Certification Practice Statement

The responsible person of this Practice Statement shall be the Governor of Okayama prefecture.

1-3-4 Contact Address

The contact for inquiry about this Practice Statement is as follows.

Okayama Prefectural Government
Address：2-4-6 Uchisange, Kita-ku Okayama City 700-8570 JAPAN
Department：Information Policy Division
Reception time：8:30 ~ 17:15
Phone：086-226-7432
FAX：086-235-9737
e-mail address：joho@pref.okayama.lg.jp

2. General Provisions

2-1 Obligations

2-1-1 Obligations of the Minister of Internal Affairs and Communications

(1) Appointment of designated certification authorities, suspension and abolition permission, removal of designation, notification to the Governor of Okayama prefecture and public notice
(2) Order to the designated certification authority required for the supervision
(3) Reporting requirements regarding the designated certification authority and implementation of on-site inspection
(4) Permissions for election and dismissal of board members of the designated certification authority, and orders of dismissal
(5) Permission and change of order regarding Certification Work Management Rules and the business plan developed by the designated certification authority
(6) Response to complaints against designated certification authority decisions
(7) Development of technical standards concerning facilities for the certification business
(8) Research and study on the technical evaluation concerning the certification business
(9) Administrative work concerning the accreditation of a signature verifier
(10) Requirements regarding reporting on the implementation status of operations against a signature verifier etc.
(11) Publicity of information concerning the Public Certification Service for Individuals to users

2-1-2 Obligations of the Governor of Okayama prefecture

(1) Issuance of the Electronic Certificate by the mayor of municipality based on the notification of name / date of birth / sex / address (hereinafter “Four Basic Information Items”) (If an applicant is a foreign resident, and his or her nickname is written in the resident record concerning said foreign resident, Four Basic Information items and a nickname are required. The same shall apply hereinafter) and Public Key
(2) Presentation of accurate information concerning the cross-certification between Okayama-ken CA and JPKI BCA and exchange of the Cross Certificate
(3) Issuance of the Self-signed Certificate
(4) Issuance of the Link Certificate
(5) Issuance of the certificate concerning operations
(6) Identity verification and creation of revocation information when receiving online revocation application from a user
(7) Creation of revocation information when revocation application has been received from a user at a municipality office service window
(8) Creation of revocation information when changing address or user name or death
(9) Creation of revocation information when matters verified for user's Electronic Certificate do not corroborate with matters recorded in said Electronic Certificate
(10) Creation of the revocation information of all certificates which have been issued by said Private Key and reporting to JPKI BCA in the case of compromise of Private Key of the Governor of Okayama prefecture (i.e., when control over Private Key is lost due to leak etc., or when such loss is suspected. The same shall apply hereinafter.)
(11) Provision of the method to check the validity of the Electronic Certificate (method to respond to the inquiry regarding the revocation information with OCSP (hereinafter called “OCSP Responder Inquiry Method) and method to provide the revocation record (CRL / ARL)) to signature verifiers etc.
(12) Provision of the method of checking the validity of the Official Status Certificate or the Professional Status (national or local authorities) Certificate for a user
(13) Creation of report on the status of provision of revocation information and revocation information files, and presentation
(14) Disclosure of certification business information in response to disclosure request
(15) Correction of the certification business information in response to correction request

(16) Generation of Key Pair of the Governor of Okayama prefecture and safe management of Private Key
(17) Implementation of audits, Implementation of improvements etc. based on the result of an audit
(18) Establishment of the facilities for the certification business
(19) The issuance, updating and revocation operations of each certificate shall be subject to this Practice Statement.
(20) Storage of all issued certificates and revocation records (CRL/ARL) for the required period and storage of Audit Logs and the information related to issuance, updating and revocation of each certificate for the required period
(21) The operation of the system shall always be monitored accurately for the purpose of 24-hour stable operation.
(22) Regarding revocation information, the revocation record (CRL/ARL), whose validity period is 72 hours, shall be issued every 24 hours.
(23) Response to complaints and inquiries from users
(24) Commission of the certification work to a designated certification authority, reporting to the Minister of Internal Affairs and Communications and public announcement
(25) Notification regarding revocation information such as transfer etc. to a designated certification authority
(26) Direction to a designated certification authority as necessary
(27) Requirement regarding reporting to a designated certification authority and implementation of on-site inspection
(28) Cancellation of commission of a designated certification authority, reporting to the Minister of Internal Affairs and Communications and public announcement
(29) Approval of issuing fee of Electronic Certificate and fee for information provision set by a designated certification authority
(30) Implementation of consultation on expenses for certification work with designated certification authorities and its delivery
(31) Implementation of certification work in cases where a designated certification authority suspends or abolishes the certification work
(32) Conclusion of the agreements with signature verifiers etc.
(33) Requirements concerning reporting on business implementation status to a signature verifier etc.
(34) Adequate handling of information on certification business
(35) Confidentiality of information on certification business
(36) Notification regarding and presentation of information on the Public Certification Service for Individuals to users
(37) Creation and decisions related to this Practice Statement

2-1-3 Obligations of Mayor of Municipality

(1) Identity verification of an applicant or a revocation applicant in the case of issuing or revoking (authenticity, identity)
(2) Confirmation that the proxy applicant is a true proxy
(3) Checking of the revocation requirements related to the revocation application
(4) Confirmation that other application procedures are conducted appropriately
(5) Provision of equipment that generates Key Pair with proper strength (equipment that generates Key Pair of an applicant, hereinafter “Key Pair Generator”)
(6) Notification of Four Basic Information Items of an applicant and Public Key of an applicant to the Governor of Okayama prefecture
(7) Notification of the revocation application to the Governor of Okayama prefecture
(8) Delivery of the Electronic Certificate and the Self-signed Certificate of the Governor of Okayama prefecture to a user
(9) Explanation to applicants and users regarding the limitations of utilization of the Electronic Certificate and penalties for unfair use etc.
(10) Maintenance and safety management of the system including Key Pair Generators and terminals at the reception window

(11) Response to audits and implementation of improvements based on the results of audits
(12) Proper handling of information on certification business
(13) Confidentiality of information on certification business
(14) Collection of issuing fees from an applicant for issuance of the Electronic Certificate
(15) Reception of disclosure requests of information on certification business and requests for correction etc.
(16) Initialization of passwords, unlocking (to release the condition where the IC Card cannot be used as a measure to prevent abuse when more than 5 passwords are entered incorrectly), and deletion of Key Pair etc.
(17) Support to users regarding the acquisition of User Client Software (software needed to use the Electronic Certificate) for user terminals
(18) Response to complaints and inquiries from users
(19) Notification regarding and presentation of information on the Public Certification Service for Individuals to users h

2-1-4 Obligation of Designated Certification Authority

(1) Implementation of the certification work commissioned by the Governor of Okayama prefecture (Implementation of the items of (1) ~ (13), (16) and (18) ~ (22) in 2-1-2 Obligations of the Governor of Okayama prefecture in this Practice Statement)
(2) Development of the Certification Work Management Rules
(3) Creation of business plans and income and expenditure budgets, submission of business reports and the settlement of accounts
(4) Establishment of Certification Business Information Protection Committee
(5) Proper handling of the information on certification business
(6) Confidentiality of the information on certification business
(7) Disclosure in response to disclosure requests of the information on certification business
(8) Corrections in response to correction requests of the information on certification business
(9) Response to complaints and inquiries from users
(10) Collection of fees for information provision from signature verifiers etc.

2-1-5 Obligations of Users

(1) Description of correct contents in the issuance application form and the revocation application form etc. of the Electronic Certificate
(2) Safe management of Private Key and IC Card where said private key is stored
(3) Regular change and safe management of passwords that activate Private Key stored in IC Card
(4) Immediate revocation application in the case of compromise of Private Key
(5) Prohibition of unintended use of the Electronic Certificate
(6) Payment of issuing fees

2-1-6 Obligations of Signature Verifiers

(1) Verification of the Electronic Signature obtained through the use of the Electronic Certificate issued by Okayama-ken CA
(2) Verification of the Electronic Certificate issued by Okayama-ken CA (whether said Electronic Certificate is issued by the Governor of Okayama prefecture, whether said Electronic Certificate is revoked)
(3) Prohibition of use of the Electronic Certificate for the purposes other than conducting authentication of users by verifying the Electronic Signature in online applications, reporting etc. from users
(4) Conclusion of agreements with the Governor of Okayama prefecture when revocation information and revocation information files are provided
(5) Reception of reporting requirements from the Minister of Internal Affairs and Communications and the Governor of Okayama prefecture and implementation
(6) Confidentiality and proper use of revocation information etc.

(7) Security of revocation information etc.
(8) Payment of fees for information provision

2-1-7 Obligations of Group Signature Verifiers

(1) Confirmation that the Electronic Certificate issued from Okayama-ken CA is not revoked
(2) Prohibition of use of Electronic Certificate for purposes other than conducting authentication of users by verifying the Electronic Signature concerning a user received from a signature checker
(3) Conclusion of agreements with the Governor of Okayama prefecture when revocation information and revocation information files are provided
(4) Acceptance of reporting requirements from the Minister of Internal Affairs and Communications and the Governor of Okayama prefecture and implementation
(5) Confidentiality and proper use of revocation information etc.
(6) Security of the revocation information etc.
(7) Payment of fees for information provision

2-1-8 Obligations of Signature Checkers

(1) Verification of the Electronic Signature obtained through the use of the Electronic Certificate issued by Okayama-ken CA
(2) Verification of the Electronic Certificate issued from Okayama ken CA (whether said Electronic Certificate is issued by the Governor of Okayama prefecture, whether said Electronic Certificate is revoked)
(3) Prohibition of use of the Electronic Certificate for purposes other than conducting the authentication of a user by verifying the Electronic Signature in online applications, reporting etc. from a user
(4) Confidentiality and proper use of response of a group signature verifier
(5) Security of group signature verifier response

2-1-9 Obligation of Repository

After creating the revocation record (CRL/ARL), Okayama ken CA shall disclose it in the Repository in order for a signature verifier etc. to check the validity of the Electronic Certificate.

And it shall store and disclose other information.

2-2 Responsibilities

2-2-1 Responsibilities of the Minister of Internal Affairs and Communications

The Minister of Internal Affairs and Communications shall appoint the designated certification authority, and shall be responsible for management and supervision to ensure the designated certification authority implements safe and proper certification work according to the Basis Law.

2-2-2 Responsibilities of the Governor of Okayama prefecture

Regarding issuance of the Electronic Certificate, the Cross Certificate, the Self-signed Certificate, the Link Certificate and other certificates required for operation, creation of the revocation record (CRL/ARL) concerning those certificates and provision of the means to check the validity of the Electronic Certificate and the Official Status Certificate or the Professional Status Certificate, the Governor of Okayama prefecture shall conduct operations appropriately for a user and a signature verifier according to this Practice Statement.

If the certification work is entrusted to a designated certification authority, the Governor shall be responsible for management and supervision to ensure the designated certification authority implements safe and proper certification work.

2-2-3 Responsibilities of Mayor of Municipality

Regarding issuance of the Electronic Certificate, reception of the revocation application, identity verification etc., the mayor of municipality shall conduct operations appropriately according to this Practice Statement.

2-2-4 Responsibilities of Designated Certification Authority

A designated certification Authority shall be commissioned by the Governor of Okayama prefecture and it shall implement the following certification work. Regarding issuance of the Electronic Certificate, the Cross Certificate, the Self-signed Certificate, the Link Certificate and other certificates required for the operations, creation of the revocation record (CRL/ARL) concerning those certificates and provision of the means to check the validity of the Electronic Certificate and the Official Status Certificate or the Professional Status Certificate, it shall conduct operations appropriately for a user and a signature verifier according to this Practice Statement.

2-2-5 Responsibilities of Users

A user shall use this service in accordance with this Practice Statement.

2-2-6 Responsibilities of Signature Verifiers

A signature verifier shall verify the Electronic Certificate in accordance with this Practice Statement.

2-2-7 Responsibilities of Group Signature Verifiers.

Group Signature verifiers shall check the validity of the Electronic Certificate according to this Practice Statement.

2-2-8 Responsibilities of Signature Checkers

A signature checker shall verify the Electronic Certificate in accordance with this Practice Statement.

2-3 Responsibilities in Finance

The Governor of Okayama prefecture shall never assume liability for the damages caused by any action where there are no reasons attributable to Okayama-ken CA.

If there are reasons attributable to Okayama-ken CA, the Governor of Okayama prefecture shall make restitution in the range specified in laws and regulations.

2-4 Interpretation and Execution

2-4-1 Applicable Law

The Basis Law and other relative laws and regulations

2-4-2 Segmentation and Integration of Service, Change and Notification of Operational Structure etc.

If the operational structure etc. are changed, such changes shall immediately be released to users, signature verifiers etc. in the following manner.

- Website of the Association
- Website of Okayama prefecture

And if a designated certification authority changes the name or the location of the office, it should report to the Minister of Internal Affairs and Communications and the Governor of Okayama prefecture.

2-4-3 Acceptance of Supervision Order, Reporting and On-site Inspection

If the Minister of Internal Affairs and Communications gives supervision orders concerning the implementation of certification work etc., and if the Governor of Okayama prefecture gives instructions to appropriately conduct the certification work, a designated certification authority should accept it.

And also, if the Minister of Internal Affairs and Communications and the Governor of Okayama prefecture require the report on the implementation status of certification work etc. or on-site inspection, a designated certification authority should accept it.

2-4-4 Settlement of Dispute Related Procedures

In the case of a lawsuit concerning this Practice Statement, the Okayama District Court shall have the exclusive jurisdiction of the first instance for all parties.

2-5 Fees

The fee concerning issuance of the Electronic Certificate, provision of revocation information and the revocation information file and disclosure of the information on certification business shall be set based on the provisions of the Basis Law etc..

2-6 Disclosure and Repository

2-6-1 Disclosure of Information concerning Okayama-ken CA

Okayama-ken CA shall disclose the following information on the Website of the Association.

- The Basis Law and relevant laws and regulations
- This Practice Statement
- Name of CA which conducted the cross-certification with Okayama-ken CA
- Name of CA which cancelled the cross-certification with Okayama-ken CA
- Information concerning the compromise of Private Key of the Governor of Okayama prefecture

Okayama-ken CA shall disclose the following information in Repository of JPKI.

- Self-signed Certificate
- Cross Certificate
- Link Certificate
- Revocation record (ARL) of Self-signed Certificate, Cross Certificate and Link Certificate
- Revocation record (CRL) of Electronic Certificate of a user

2-6-2 Frequency of Disclosure

The updating frequency of the information which is disclosed shall be as follows.

- Regarding the stipulations of the Basic Law, relevant laws and regulations, the latest version of this Practice Statement etc., shall always be posted on the Web.
- Each issuance of the Self-signed Certificate, the Cross Certificate and the Link Certificate shall be disclosed and updated.
- The revocation record (CRL/ARL) shall be updated once a day.

2-6-3 Control of Access to Public Information

Regarding the stipulations of the Basic Law, relevant laws and regulations, access to this Practice Statement etc. shall not be restricted.

Regarding the following information in Repository, access shall not be restricted.

- Self-signed Certificate
- Cross Certificate
- Link Certificate

・Revocation record (ARL) of Self-signed Certificate, Cross Certificate and Link Certificate

However, regarding the revocation record (CRL) of Electronic Certificate of a user which is disclosed in Repository, access shall be restricted.

2-6-4 Requirements related to Repository

Repository may be used 24 hours a day, every day of the year. However, Repository may be temporarily unavailable due to regular maintenance work etc..

2-7 Compliance Audit

2-7-1 Frequency of Compliance Audit

The Governor of Okayama prefecture shall implement annual regular compliance audits by an auditor. The Governor shall implement an audit other than a regular audit as needed.

2-7-2 Identification and Qualifications of Auditor

The audit of Okayama ken CA shall be implemented by a person acquainted with audit work and certification business.

2-7-3 Relation between Auditor and Audited Department

The Governor of Okayama prefecture shall appoint a person who does not have an interest or stake in Okayama-ken CA as an auditor.

2-7-4 Inspection Items

The auditor shall check mainly if the certification business is compliant with the Basis Law, relevant laws and regulations, this Practice Statement etc..

2-7-5 Handling of Audit Result

The audit result shall be submitted to the Governor of Okayama prefecture as an audit report by an auditor. The Governor of Okayama prefecture shall notify each mayor of municipality and a designated certification authority of the audit report as needed.

2-7-6 Response to Audit Findings

A designated certification authority shall check the audit findings, and respond appropriately according to the importance and the urgency. The results shall be reported to the Governor of Okayama prefecture after evaluation. The Governor of Okayama prefecture shall check that a designated certification authority has taken measures in response to the audit findings.

2-8 Confidentiality and Protection of Personal Information

2-8-1 Handling of Classified Information and Personal Information

Okayama-ken CA shall classify information whose leak may result in the damage of the credibility of certification business of Okayama-ken CA. In addition, the personal information of a user shall be duly protected.

Regarding classified information and information including personal information of a user, a chief administrator of documents and electronic record medium which include said information (CA chief administrator specified in “5-2-2-1 Personnel in Okayama ken CA” in this Practice Statement) shall be appointed to safely manage them. If personal information is leaked, measures shall be taken according to the procedures prescribed separately.

2-8-2 Non-Classified Information

The information which is expressly shown as disclosure information among the information which Okayama prefecture holds, such as the Self-signed Certificate, the Link Certificate, the Cross

Certificate, the Official Status Certificate Validation Server Certificate, the OCSP Responder Certificate, as well as the respective revocation information for each of the above, this Practice Statement etc. shall not be classified

2-8-3 Disclosure of Certificate Revocation Information

Okayama-ken CA shall disclose the revocation information of the Self-signed Certificate, the Link Certificate and the Cross Certificate which it issues, and the certificates concerning operation. The details of the reason for revocation shall not be disclosed. Also, the revocation information of the Electronic Certificate is provided exclusively to a signature verifier based on the Basis Law.

2-8-4 Information Disclosure to Law Enforcement Agency

Not specified

2-8-5 Information Disclosure in Civil Proceeding

Not specified

2-8-6 Information Disclosure upon Request from Certificate User

If a user makes a request for disclosure of the information on his or her own certification business, such disclosure shall take place after identity verification.

2-8-7 Information Disclosure for Other Reasons

Not specified

2-8-8 Correction of Information upon Request from Certificate Users

If a user makes a request for correction etc. of the information on his or her own certification business, such correction shall be implemented after identity verification.

2-9 Intellectual Property Rights

Not specified

3. Identification and Authentication

3-1 First Application for Certificate Issuance

3-1-1 Name Form

The name of an issuance nominee and a user of the Electronic Certificate shall be set according to the form of X.500 Distinguished Name (DN).

3-1-2 Requirements concerning Meaning of Name

The name of issuance nominee of the Electronic Certificate shall be recorded with the official title of the prefectural governor.

The Four Basic Information Items of a user which are stored in the Electronic Certificate shall be recorded in the extended area of the Electronic Certificate. The information of the extended area where Four Basic Information Items of a user are stored is shown below.

subjectAltName		
	common Name	Name (If a user is a foreign resident, and his or her nickname is written in the resident record concerning said foreign resident, Name and Nickname)
	dateOfBirth	Date of birth
	gender	Sex
	address	Address

3-1-3 Rule to Interpret the Name Form

According to X.500 Distinguished Name

3-1-4 Uniqueness of Name

The subject field of the Electronic Certificate which Okayama-ken CA issues shall be allotted uniquely.

3-1-5 Means to Settle the Dispute concerning Name

Not specified

3-1-6 Recognition / Certification / Role of Trademark

Not specified

3-1-7 Type and Form of Name Recorded in the Extended Area of Electronic Certificate

Name, nickname (only if a person who wishes to file an application for the Electronic Certificate is a foreign resident and his or her nickname is written in the resident record concerning said foreign resident), address, date of birth, and sex of a user shall be recorded in Chinese characters, hiragana, katakana, alphabet, Arabic numbers or others.

3-1-8 Rules concerning the Recording Method of Name which is Recorded in the Extended Area of Electronic Certificate

Regarding Chinese characters which are used for the recording of names etc., only the Chinese characters in（JISX0208、JISX0212）(type of character), i.e. those adopted at the window terminals of the municipality of residence, may be used.

If a Chinese character which cannot be used is included in the name etc., a similar Chinese character which exists (hereinafter called "Alternative Character") shall be used by user's selection.

If Alternative Characters are used, that shall be shown in the extended area.

3-1-9 Requirements concerning Identification and Authentication of User

In the first issuance application, the identity verification of an applicant shall be implemented according to the following methods. However, if doubt arises in the identity verification, the Electronic Certificate shall not be issued.

① Confirm that said applicant is a person who is recorded in the basic resident registration by checking Four Basic Information Items written in the issuance application form against the record in the basic resident registration. (Check of authenticity)

② Confirm that the applicant is a person who is recorded in the basic resident registration by checking ID with a picture etc. which has been issued by a public body (Documents specified in Paragraph 1, Article 6 of the Ordinance of the Basis Law) (Identity Check)

3-1-10 Requirements concerning Identification and Authentication in the case of Proxy Application

In the case of application by a proxy, the identity verification of a proxy and the existence of the authority of representation shall be checked by the following methods.

① Check the power of attorney with registration by a principal and seal, the seal registration certificate concerning said seal, the response to the inquiry document concerning said applicant and the papers which the mayor of municipality of residence considers appropriate

② Implement the identity verification of a proxy through the latter's presentation of ID with a picture etc. issued by a public body (Documents specified in Paragraph 1, Article 5 of the Ordinance of the Basis Law)

3-1-11 Checking Private Key Ownership Evidence

An applicant shall generate Key Pair based on the Basis Law and relevant laws and regulations using Key Pair Generator which is set up in the municipal office of residence.

3-2 Updating the Electronic Certificate

When updating the Electronic Certificate, the identity verification of a user shall be implemented in the following way. However, if any doubt arises during the identity verification, the Electronic Certificate shall not be issued.

① Confirm that said applicant is a person who is recorded in the basic resident registration by checking Four Basic Information Items written in the updated application against the record in the basic resident registration. (Check of authenticity)

② Confirm that the applicant is a person who is recorded in the basic resident registration by having the latter present ID with a picture etc. issued by a public body (Check of identity)

Note that Private Key concerning the Electronic Certificate which is revoked due to the update shall be deleted in the prescribed manner by the user.

3-3 Reissue after Revocation

The same procedure of identity verification that is implemented in the first issuance application shall be done.

3-4 Revocation Application

3-4-1 Revocation Application to Cancel Use of Service

An applicant shall file an online application with the Electronic Signature by Private Key of a user or written application at the window of the municipal office of residence.

The identity verification of a user shall be conducted by the verification of the Electronic

Signature in the case of online application. In the case of written application at the window of the municipal office of residence, the same procedure of identity verification that is implemented in the issuance of the Electronic Certificate shall be done.

3-4-2 Revocation Application in the Case of Compromise of Private Key of User

An applicant shall go to the window of the municipal office immediately and file a revocation application in writing at the window.

The identity verification of a user shall be conducted according to the same procedure of identity verification that is implemented in the issuance of the Electronic Certificate.

4. Operational Requirements

4-1 Issuance Application of Electronic Certificate

4-1-1 Issuance Application / Reception Procedure

The issuance application / reception procedure of the Electronic Certificate shall be as follows.

① An applicant shall submit the issuance application and IC Card to the municipality of residence. In the case of update, an applicant shall submit the IC Card where the Electronic Certificate is stored.

② The mayor of municipality of residence shall check the authenticity of a user by checking against the record of the basic resident registration, and verify the identity of an applicant by the latter's presentation of ID with a picture etc. issued by a public body such as a driver's license and a passport. However, if doubt arises during the identity verification, the Electronic Certificate shall not be issued.

③ An applicant shall generate Key Pair using Key Pair Generator which is set up at the window of the municipal office of residence. An applicant shall notify the municipality (window) of Public Key.

Application by a proxy may be conducted according to the following procedure. However, if doubt arises in (1) or (2), the Electronic Certificate shall not be issued.

(1) A proxy shall submit or present a power of attorney with registration by a principal and seal (only if the seal registration certificate concerning said seal is attached), and a driver's license or a passport to check the identity of a proxy.
(2) A proxy shall submit the response to the inquiry document to said applicant by mail or by other methods which the mayor of municipality of residence considers appropriate to confirm that an applicant is a principal and said application is based on the applicant's will regarding the issuance application of the Electronic Certificate, and present the papers which the mayor of municipality of residence considers appropriate.
(3) A proxy shall generate Key Pair using Key Pair Generator and notify the municipality of Public Key. However, the password shall be entered (activation of Private Key) by the mayor of municipality of residence.

4-1-2 Issuance Application Form, Necessary Description

In the issuance application, the following items shall be entered.

- Date of application
- Name (furigana), nickname (only if a person who wishes to file an application for the Electronic Certificate is a foreign resident and his or her nickname is written in the resident record concerning said foreign resident), address, date of birth, sex and alternative characters for name, nickname and address
- In the case of application by a proxy, name and address of a proxy in addition to the above items

4-1-3 Electronic Record Medium of Private Key

It shall be stored in a tamper-resistant IC Card.

4-2 Issuance of Electronic Certificate

4-2-1 Issuance Procedure

The issuance procedure of the Electronic Certificate shall be as follows.

① The mayor of municipality of residence shall notify the Governor of Okayama prefecture of Four Basic Information Items and Public Key of an applicant.

② The Governor of Okayama prefecture shall issue the Electronic Certificate and notify the

mayor of municipality of residence.

4-2-2 Form of Electronic Certificate

According to ITU-T Recommendation X.509 (03/2000), name of a user, nickname, address, date of birth and sex shall be recorded in Chinese characters, hiragana, katakana, alphabet, Arabic number etc. in the extended area.

If alternative characters are used in the extended area of the record for name, nickname and address, that shall be recorded in the extended area.

subjectAltName		
	commonName	Name (If the applicant is a foreign resident, and his or her nickname is written in the resident record concerning said foreign resident, Name and Nickname)
	dateOfBirth	Date of birth
	gender	Sex
	address	Address
	substituteCharacterOfCommonName	Information on the use of substitute characters for name
	substituteCharacterOfAddress	Information on the use of substitute characters for address

4-2-3 Rejection of Issuance Application

When falling under the next event, the Governor of Okayama prefecture shall reject the issuance application.

・An applicant has already obtained a valid Electronic Certificate and there is no description in the revocation record (CRL).

If it should be issued doubly, the Governor of Okayama prefecture shall revoke the later Electronic Certificate (date of issuance) as soon as double issuance becomes clear.

4-3 Delivery of Electronic Certificate

4-3-1 Delivery Procedure

The delivery procedure of the Electronic Certificate shall be as follows.

① The mayor of municipality of residence shall record the Electronic Certificate and the Self-signed Certificate of the Governor of Okayama prefecture in the IC Card of an applicant.

② The mayor of municipality of residence shall notify an applicant of the notes concerning the use of this service, and deliver a duplicate of the Electronic Certificate.

4-3-2 Notices

The mayor of municipality of residence shall notify a user of the following matters.

・To manage the highly Private Key and the IC Card, which is the latter's electronic record medium, and password to activate IC Card on user's own responsibility.

・To notify the municipality (window) immediately and implement the revocation application when Private Key or IC Card, which is the latter's electronic record medium, is lost or stolen. .

4-4 Revocation and Suspension of Electronic Certificate

4-4-1 Reason for Revocation by Authority

4-4-1-1 Reason for Revocation by Authority

The reasons for revocation of the Electronic Certificate shall be as follows.

・Change of Four Basic Information Items etc. of a user

・If the matters written in the Electronic Certificate of a user are different from those written in the resident record concerning the user of said Electronic Certificate

・If double issuance of the Electronic Certificate is confirmed

・Compromise of Private Key of the Governor of Okayama prefecture

4-4-1-2 A person who can Revoke Certificate

The Governor of Okayama prefecture

4-4-1-3 Revocation Procedure resulting from Compromise of Private Key of the Governor of Okayama Prefecture

When the compromise of Private Key of the Governor of Okayama prefecture occurs, all Electronic Certificates signed with said Private Key shall be revoked by the authority, shall be recorded in the revocation record (CRL/ARL) and shall be published on the Web etc..

4-4-2 Revocation by Application from User

4-4-2-1 Reason for Revocation by Application from User

The reasons for revocation by application shall be as follows.

・Cancellation of this service

・Occurrence of the compromise of Private Key of a user

4-4-2-2 Revocation Application Procedure to Cancel Use of Service

As for the revocation procedure to cancel the use of this service, use of either one of the following procedures should be applied.

① Receive the online application with the Electronic Signature. Notify a user of the reception of the revocation application online.

② Receive the written revocation application at the window of the municipal office of residence. Request revocation processing from the Governor of Okayama prefecture. Deliver the papers where the reception of the revocation application is described to a user.

4-4-2-3 Revocation Application Procedure in the Case of Compromise of Private Key of User

The revocation procedure in the case of compromise of Private Key of a user shall be as follows.

① Receive the written revocation application in the municipality of residence.

② Request revocation processing from the Governor of Okayama prefecture. Deliver the papers where the completion of the revocation processing is described to a user.

4-4-2-4 Recovery Method when Electronic Certificate of a User is revoked

The Electronic Certificate whose revocation processing has been done shall not be recovered, but a new Electronic Certificate shall be issued by new application procedure.

4-4-2-5 Recovery Method in the Case of Compromise of Private Key of User

A new Electronic Certificate is issued by new application procedure.

4-4-3 Requirements related to Revocation Record (CRL/ARL)

Reflecting the revocation information whose reception is completed by the set time, a new revocation record (CRL/ARL) shall be created once a day, and the created revocation record (CRL/ARL) shall be disclosed immediately to a permitted signature verifier etc..

Also, the provision of the revocation record (CRL/ARL) to a permitted signature verifier etc. shall be available 24 hours a day, every day of the year. During regular maintenance work etc., however, it may be temporarily unavailable.

4-4-4 Revocation Information Provision Methods

4-4-4-1 Revocation Information Provision Methods

The validity of the Electronic Certificate shall be checked according to the following two methods.

① OCSP Responder Inquiry Method (Use of OCSP specified in RFC2560)

② Revocation Record (CRL/ARL) Provision Method (Use of LDAPV3 Protocol specified in RFC2251)

4-4-4-2 Content of Responses related to OCSP Responder Inquiry Method

In response to online inquiries for information to identify an issuer of the Electronic Certificate and serial number, “Valid”, “Unclear” or “Invalid” of said Electronic Certificate at the time of inquiry shall be displayed, and the reason for revocation when it has been revoked shall be given. The reasons for revocation shall be as follows.

Reason for Revocation		
1	keyCompromise	The compromise of Private Key of a user occurred.
2	cACompromise	The compromise of Private Key of the Governor of Okayama prefecture occurred.
3	affiliationChanged	The contents of the Electronic Certificate were changed.
4	superseded	The Electronic Certificate was updated.
5	cessationOfOperation	The Electronic Certificate is not needed. (is not used)

4-4-4-3 Requirements regarding OCSP Responder Inquiry Method

It is necessary to notify the Governor of Okayama prefecture in advance and be granted access rights.

4-4-4-4 Content of Responses related to Revocation Record (CRL/ARL) Provision Method

The format of the revocation record (CRL/ARL) shall comply with ITU-T Recommendation X.509(03/2000).

In principle, the revocation record (CRL) shall be sectional CRL created by each municipality, and the serial number of the revoked Electronic Certificate, the reason for revocation (same as the reason for revocation in “4-4-4-2 Content of Response related to OCSP Responder Inquiry Method” in this Practice Statement) and the date of revocation shall be recorded in it. A signature verifier etc. shall properly obtain the revocation record (CRL/ARL) stored in Repository to verify the Electronic Certificate.

4-4-4-5 Requirements regarding Provision of Revocation Record (CRL/ARL)

It is necessary to notify the Governor of Okayama prefecture in advance and be granted

access rights.

4-4-5 Requirement regarding Suspension

The suspension of the Electronic Certificate which the Governor of Okayama prefecture issues shall not be done.

4-4-6 Suspension Applicant

Not specified

4-4-7 Request Procedure for Suspension

Not specified

4-4-8 Period of Suspension

Not specified

4-4-9 Issuance Frequency of Revocation Record (CRL/ARL)

The revocation record (CRL/ARL), whose valid period is 72 hours, shall be issued every 24 hours. However, if the compromise of Private Key of the Governor of Okayama prefecture occurs, the revocation record (CRL/ARL) shall be issued immediately.

4-4-10 Maximum Delay Time of Revocation Record (CRL/ARL) Issuance

Before the valid period of the latest revocation record (CRL/ARL) expires, a new revocation record (CRL/ARL) shall be issued.

4-4-11 Check of Revocation Record (CRL/ARL)

A signature verifier shall check the validity of the Electronic Certificate by the revocation record (CRL/ARL) which the Governor of Okayama prefecture issues.

4-5 Preparation of Report on the Provision Status of Revocation Information etc.

A designated certification authority shall prepare reports on the provision status of the revocation information and the revocation information files related to storage. A designated certification authority shall publish said report in an official gazette, keep it in the office of a designated certification authority and submit it for public inspection for 5 years.

The contents of the report shall be as follows.

- Destination of the revocation information etc.
- Date when the revocation information etc. is provided
- Number of revocation information items etc. provided
- How to provide the revocation information etc.

4-6 Application for Issuance of Cross Certificate

The application to JPKI BCA for issuance of the Cross Certificate shall be conducted according to the procedure established by JPKI BCA.

4-7 Issuance of Cross Certificate

The Governor of Okayama prefecture shall check the authenticity of an operator of JPKI BCA according to the prescribed procedure. After the completion of the connection test according to the procedure established by JPKI BCA, the Governor shall issue the Cross Certificate with the signature of the Governor of Okayama prefecture in response to the certificate issuance request

which is submitted by JPKI BCA.

4-8 Reception of Cross Certificate

The Governor of Okayama prefecture shall receive the Cross Certificate issued by JPKI BCA according to the prescribed procedure, and deliver a receipt to JPKI BCA. In the same manner, the Governor of Okayama prefecture shall deliver the Cross Certificate which was issued to JPKI BCA according to the prescribed procedure, and receive the receipt. With these reception checks, mutual reception of the Cross Certificate is confirmed as completed.

In addition, the Governor of Okayama prefecture shall create the Cross Certificate Pair (pair of the Cross Certificate which was exchanged with JPKI BCA) and register it in Repository.

4-9 Updating of Cross Certificate

The Governor of Okayama prefecture shall update the Cross Certificate and the Cross Certificate Pair in the following cases (1) – (4).

Here, each procedure of issuance application, issuance and reception in the updating of the Cross Certificate shall comply with "4-6 Application for Issuance of Cross Certificate", "4-7 Issuance of Cross Certificate" and "4-8 Reception of Cross Certificate" in this Practice Statement. And also, the Cross Certificate Pair in Repository shall be updated immediately.

(1) When the period of validity of the Cross Certificate which was issued by JPKI BCA is about to expire.

(2) When the period of validity of the Cross Certificate which was issued to JPKI BCA is about to expire.

(3) When the contents of the Cross Certificate which was issued by JPKI BCA were changed.

(4) When the contents of the Cross Certificate which was issued to JPKI BCA were changed.

4-10 Revocation of Cross Certificate

4-10-1 Reasons for Revocation

If the following events occur in Okayama-ken CA or JPKI BCA, Okayama-ken CA shall revoke the Cross Certificate which was issued to JPKI BCA, and JPKI BCA shall revoke the Cross Certificate which was issued to Okayama-ken CA.

- Compromise of Private Key.
- Update of the Cross Certificate
- Completion of the cross certification (including the case of completion of the cross certification which results from a violation of the Cross Certification Standard)

4-10-2 Applicant of Revocation

The revocation application from JPKI BCA to Okayama-ken CA shall be conducted by a JPKI BCA officer.

The revocation application from Okayama-ken CA to JPKI BCA shall be conducted by the Governor of Okayama prefecture.

4-10-3 Revocation Application and Revocation Processing Procedure

The revocation application of the Cross Certificate shall be conducted based on the procedure established by JPKI BCA.

4-11 Security Audit Procedure

4-11-1 Security Audit Procedure

An internal auditor (refer to "5-2-1 Personnel with High Liability and their Roles" in this Practice Statement) shall conduct the security audit to check abnormal events such as fraudulent manipulation etc. by checking the log where the events that occurred in Okayama-ken CA system and Repository are recorded against the business records etc..

4-11-2 Information which is Recorded in Audit Logs

Audit Logs such as Access Logs and Operation Logs (regarding important events concerning the security in Okayama-ken CA system and Repository) shall be recorded.

- Operation / Running Logs concerning the issuance procedure
- Operation / Running Logs concerning the revocation procedure
- All access / Running Logs concerning the validity check
- Operation Logs concerning the generation of Key Pair of the Governor of Okayama prefecture
- System Access Log, account books etc.
- records of Entrance/Exit of the facilities of Okayama-ken CA

The following information shall be included in Audit Logs.

- Type of event or processing
- Date of occurrence
- Result of processing
- Identification information concerning the origin of the event (ID of operator, system name etc.)

4-11-3 Audit Log Inspection Cycle

An inner auditor shall implement security audit weekly.

4-11-4 Audit Log Storage Period

It shal1 be stored for one year.

4-11-5 Protection of Audit Log

Regarding Audit Logs, measures to prevent someone from changing data shall be taken. In addition, Audit Logs shall be backed up in external memory media etc., and shall be stored in lockable storage cabinets installed in rooms whose entrance/exit management is conducted appropriately.

The browse and deletion of Audit Logs shall be carried out duly by an internal auditor.

4-11-6 Backup Procedure of Audit Logs

Audit logs shall be backed up daily and stored in external memory media etc. monthly.

4-11-7 Notice of Audit Log Inspection

The inspection of Audit Logs shall be done without notifying persons who brought about the events.

4-11-8 Verification of Vulnerability

By inspecting Audit Logs, the vulnerability of operation and system security shall be evaluated.

4-11-9 Audit Log Collection System

The Audit Log collection shall be one function of Okayama-ken CA system, and important events concerning security shall be collected as Audit Logs from the start-up.

4-12 Storage of Record (Archive)

4-12-1 Information to be Stored on Paper

4-12-1-1 Type of Stored Information

The following information shall be stored.

（Governor of Okayama prefecture）

・Documents concerning the creation of this Practice Statement
・Documents concerning the implementation of Key Ceremony
・Documents concerning agreement with a signature verifier etc.
・Documents concerning the disclosure/correction of information on certification business
・Audit Report

（Designated Certification Authority）

・Documents concerning the appointment / change of a designated certification authority
・Certification Work Management Rules
・Documents concerning the facilities and safety measures
・Documents concerning　business plans and the income / expenditure budget
・Business reports / Settlement of accounts
・Documents concerning the disclosure / correction of information on certification business
・Report on the provision status of the revocation information and the revocation information file
・Documents concerning fees

（Mayor of Municipality）

・Documents concerning application for issuance of the Electronic Certificate (Issuance Application Form etc.)
・Documents concerning the application for revocation of the Electronic Certificate (Revocation Application Form etc.)
・Documents concerning disclosure / correction of the information on certification business

4-12-1-2 Storage Period

The storage period shall be 10 years. However, that of the documents concerning the applications for issuance of the Electronic Certificate shall be 13 years.

4-12-1-3 Protection of Stored Information

Regarding the information stored with a designated certification authority, measures to prevent someone from changing the data shall be taken, it shall be stored in lockable storage cabinets installed in the room whose entrance/exit management is conducted appropriately, and environmentally friendly protective measures (temperature, humidity etc.) shall be taken. Information stored in the municipality and the prefecture shall be stored in an appropriate place

4-12-1-4 Verification of Stored Information

The condition and the readability of papers where the stored information is included shall be checked once a year.

4-12-2 Information to be Stored as Digital Data

4-12-2-1 Type of Stored Information

The following information shall be stored with a designated certification authority.

・Revocation Application Form (in the case of online application to the Governor of Okayama prefecture)
・Electronic Certificate
・Cross Certificate
・Self-signed Certificate
・Link Certificate
・Server Certificate of Certificate Validation Servers
・OCSP Responder Certificate
・Revocation information
・Revocation record（CRL/ARL）
・Revocation information file
・Provision method regarding record of history of use of revocation（CRL/ARL）
・OCSP Responder Inquiry Method use history
・System Logs (Monitoring Logs, Start-Stop Logs, Operation Logs)

4-12-2-2 Storage Period

The storage period shall be 10 years. However, that of the issued Electronic Certificate shall be 13 years, and that of the revocation information shall be from the date when said revocation information is recorded through the expiration date of the valid period of the Electronic Certificate concerning said revocation information.

4-12-2-3 Protection of Stored Information

Regarding the stored information, access shall be controlled and measures to prevent someone from changing the data shall be taken.

The information shall be stored in external memory media etc. monthly, and stored in lockable storage cabinets installed in rooms whose entrance/exit management is conducted appropriately.

4-12-2-4 Stored Information Backup Procedure

The stored information shall be backed up daily and stored in external memory media etc. monthly.

4-12-2-5 Requirements regarding Time Stamps in Records

Time Stamps (time information) shall be added in the stored information.

4-12-2-6 Verification of Stored Information

The readability of external memory media etc. where stored information is recorded shall be checked once a year.

4-13 Updating the Key of the Governor of Okayama Prefecture

The Key Pair of the Governor of Okayama prefecture shall be updated every 5 years.

In the update of Key Pair, the Link Certificate which constructs the certification path of the old Public Key and new Public Key shall be issued and disclosed in Repository.

4-14 Compromise of Key and Disaster Recovery

4-14-1 Coping with Destruction of Hardware, Software or Data

If hardware, software or data are destroyed, the recovery work shall be conducted immediately with hardware, software or data for backup.

4-14-2 Coping with Compromise of Private Key of the Governor of Okayama Prefecture

Shall be handled as follows.

- Electronic Certificate issuance operations shall be stopped.
- All Electronic Certificates, Cross Certificates etc. which were signed with said Private Key shall be revoked , recorded in the revocation records (CRL/ARL) and disclosed.
- JPKI BCA shall be notified.

4-14-3 Securing of Facilities in the Event of Disaster

If the facilities are damaged by disaster etc., spare equipment shall be secured and operated with backup data.

4-15 Handling of Claims / Inquiries

The Governor of Okayama prefecture, a designated certification authority and the mayor of municipality shall appropriately and immediately handle the claims and inquiries concerning the certification work etc.

4-16 System Operation

Safe and appropriate system operation shall be carried out. The details shall be specified separately.

4-17 Completion of Certification Business

Not specified

4-18 Suspension or Abolition of Certification Work

If a designated certification authority suspends or abolishes all or a part of certification work etc., it shall obtain permission form the Minister of Internal Affairs and Communications.

And, if it results in the implementation of the certification work by the Governor of Okayama prefecture, the designated certification authority shall perform the following tasks.

- Take over the certification work to be taken over to the Governor of Okayama prefecture
- Deliver the accounts books, documents, materials and electronic records media concerning the certification work to be taken over to the Governor of Okayama prefecture
- Perform other tasks which are deemed necessary by the Minister of Internal Affairs and Communications or the Governor of Okayama prefecture

5. Security Management in the Physical Aspect, in terms of Procedures and Personal Affairs

5-1 Security Management -- Physical Aspect

5-1-1 Okayama-ken CA

5-1-1-1 Position and Construction of Facilities

The facilities of Okayama-ken CA shall be constructed in locations where they will not easily suffer damage from floods, earthquakes, fires and other disasters; the building shall be earthquake-proof and fireproof structures, and measures to prevent illegal intrusion shall be taken. And also, the equipment etc. that are used shall be installed in safe places protected from disasters and illegal intrusion.

5-1-1-2 Physical Access

According to the importance of operations undertaken in each room in the facility of Okayama-ken CA, entrance/exit management shall be done in plural security levels. Authentication shall be done with IC Card and biometric authentication devices by which a person having operational authority can be identified.

According to the work of each personnel which is specified in "5-2 Security Management in Procedure" in this Practice Statement, the authority of entrance/exit of each room shall be given by the chief administrator of Okayama-ken CA.

Watchmen shall be deployed in the facility of Okayama-ken CA to monitor it through the monitoring system 24 hours a day, every day of the year.

5-1-1-3 Electric Power and Air Conditioning

Okayama-ken CA shall secure electric power sufficient for operating equipment etc., and take measures against temporary blackouts, power failures and changes in voltage and frequency. If commercial power is not supplied, a change to power supply by a power generator should be carried out within a certain time.

The operating environment of equipment and the working environment of personnel shall be maintained by installing air conditioning equipment.

5-1-1-4 Measures against Floods

Leakage detection equipment shall be installed in the buildings and rooms where the equipment of Okayama-ken CA are installed, and waterproofing measures shall be taken for the ceilings and floors.

5-1-1-5 Measures against Earthquakes

The buildings where the equipment of Okayama-ken CA are installed shall be earthquake-proof structures, and measures to prevent devices and fixtures from falling and dropping shall be taken.

5-1-1-6 Measures against Fire

The buildings where the equipment of Okayama-ken CA are installed shall be fireproof structures, the rooms shall be fireproof compartments and firefighting equipment shall be installed.

5-1-1-7 Measures against Electromagnetic Waves

According to the importance of the work which is conducted in each room of the facility of Okayama-ken CA, equipment to prevent electromagnetic pulse attacks and information leakage through electromagnetic waves shall be installed.

5-1-1-8 Management of Media (Magnetic Media etc.)

Media including stored information and backup data shall be stored in lockable storage cabinets installed in rooms whose entrance/exit management is conducted appropriately, and suitable carrying in/out management shall be done according to the prescribed procedures.

5-1-1-9 Waste Disposal

Regarding the documents and memory media including the information treated as confidential, appropriate waste disposal shall be carried out according to the prescribed procedures.

5-1-1-10 Off-Site Backup

Not specified

5-1-2 Municipality Facilities

5-1-2-1 Position and Construction of Facilities

The facilities shall be those in the municipality of residence.

5-1-2-2 Physical Access

Key Pair Generator and the terminals at the reception window shall be installed where employees of municipality of residence can monitor them sufficiently. Also, maintenance concerning Key Pair Generator and terminals of reception window shall be conducted appropriately.

A person who conducts identity verification etc. of a user shall operate the terminals of reception window. The operator shall be authenticated using ID/ password method.

5-1-2-3 Management of Stored Information

The documents concerning “4-12-1-1 Type of Stored Information” in this Practice Statement shall be stored in an appropriate place.

5-1-2-4 Waste Disposal

Regarding the disposal of documents and memory media including information treated as confidential, the terminals at reception window, Key Pair Generator etc., appropriate waste disposal shall be carried out according to the prescribed procedure.

5-2 Security Management in Procedure

5-2-1 Personnel with High Liability and their Roles

5-2-1-1 Personnel in Okayama-ken CA

The personnel involved in the operation of the system of Okayama-ken CA shall be as follows.

(1) Chief Administrator of CA

The chief administrator of CA shall be a person responsible for the operation of Okayama-ken CA, and shall perform the following functions.

- Supervision of the certification business
- Supervision of response to cases where the compromise of Private Key of the Governor of Okayama prefecture has occurred and emergencies such as disasters
- Work instruction to personnel and check of work results
- Maintenance of the key to control the function of HSM (device to safely manage Private Key of the Governor of Okayama prefecture) (hereinafter called “Management Key”)

・Management of response to requests for the disclosure of the information on certification business
・Management of response to the requests for the correction of information on certification business
・Management of response to inquiries and claims
・Management of Certification Business Information Protection Committee
・Preparation of account books concerning certification business
・Creation of reports on provision status of the revocation information etc.
・Management of entrance/exit
・Response to compliance audits and management of corrective implementation of the findings
・Supervision concerning the administration and operation of Okayama-ken CA
・Management of personal information

(2) Manager of Private Key

A manager of Private Key shall be a person responsible for the operations concerning the use of Private Key etc. of the Governor of Okayama prefecture, and shall perform the following functions. The operations shall be implemented by plural managers of Private Key.

・Storage management of backup medium of Private Key etc. of the Governor of Okayama prefecture
・Generation of Private Key etc. of the Governor of Okayama prefecture and operation of HSM in the issuance of the Self-signed Certificate
・Operation of HSM in the updating of Private Key etc. of the Governor of Okayama prefecture
・Operation of HSM in the backup of Private Key etc. of the Governor of Okayama prefecture and restoration from backup

(3) Person in charge of reception

A person in charge of reception shall conduct issuance of the Cross Certificate etc., reception of updates and revocation application, coordination of operations with JPKI BCA and management of application forms etc.

(4) Examiner

An examiner shall conduct the examination operations related to issuance, updating and applications for revocation of the Cross Certificate, etc..

(5) Approver

An approver shall conduct certification business for examination results of issuance application, update application and revocation application related to the Cross Certificate etc. from an examiner.

(6) Senior Operator

A senior operator shall conduct the following operations regarding the use of Private Key of the Governor of Okayama prefecture and the operations shall be implemented by plural senior operators.

・Activation and deactivation of HSM
・Issuance, updating and revocation processing of the Self-signed Certificate
・Issuance, updating and revocation processing of Cross Certificate
・Issuance, updating and revocation processing of the Official Status Certificate Validation Server Certificate
・Issuance, updating and revocation processing of the OCSP Responder Certificate

・Registration of setting and change of Okayama-ken CA Electronic Certificate Policy
Operations management of Okayama-ken CA System

(7) Repository Operator

A repository operator shall conduct operations concerning setting management of Repository.

(8) General Operator

A general operator shall conduct operations related to and maintenance of network equipment etc.

(9) Internal Auditor

An internal auditor shall conduct operations concerning the logs of Okayama-ken CA system and Repository.

・Inspection of Audit Log

・Deletion of audited Log

5-2-1-2 Personnel of Municipality

Personnel of the municipality shall conduct strict identity verification in issuance and revocation of the Electronic Certificate, administrative work concerning issuance and revocation, and appropriate management etc. of equipment used in administrative work.

5-2-2 Separation of Personnel's Official Authority and Work Instruction Method in Okayama-ken CA

The separation of personnel's official authority and the work instruction method is as follows.

① Separation of authority

Jobs shall be separated from the standpoint of human security, and plural personnel who have the authority shall conduct operations and management of the facility.

② Authority of a chief administrator of CA

Regarding the instruction of important business, a chief administrator of CA shall instruct personnel individually according to the prescribed procedure which is specified separately.

③ Authority of a senior operator

A senior operator shall instruct a general operator about specific tasks and check the results based on the prescribed procedure which is specified separately. In addition, a senior operator shall implement the registration appropriate for the authority of personnel and issue a certificate.

5-2-3 Identification of Personnel and Authentication Requirement in Okayama-ken CA

・When personnel operate the system, the system shall identify and authenticate that the operating personnel are properly authorized.

・The authentication of personnel shall be done with IC Card and a password. Passwords shall be changed periodically.

・The private information which personnel can access according to the role shall be minimized.

5-3 Security Management in Personnel Affairs in Okayama-ken CA

5-3-1 Check of Personal Background of Personnel and Permission Procedure

According to the prescribed examination procedure, background of individual personnel shall be checked by documentary examination (resume, recommendations etc.) before employment.

5-3-2 Personnel Training Procedures

According to the education and training plans, training required for personnel shall be conducted.

5-3-3 Rotation, Frequency and Sequence

A chief administrator of CA shall specify the rotation method of the operations in writing.

5-3-4 Actions which are not Permitted

If personnel perform actions which are not permitted, predetermined disciplinary measures shall be taken.

5-3-5 Documents Provided to Personnel

Personnel may browse the documents (operation procedure manuals, operating manuals etc.) according to their respective access rights.

6. Technical Security Management

6-1 Generation of Key Pair and Installation

6-1-1 Key of the Governor of Okayama prefecture

6-1-1-1 User who Generates Key Pair of the Governor of Okayama Prefecture and Generation method

Key Pair of the Governor of Okayama prefecture shall be generated by plural managers of Private key with the equipment specified in “6-1-1-3 Hardware / Software to generate Key Pair” in this Practice Statement.

6-1-1-2 Key Length

2048-bit RSA key shall be used.

6-1-1-3 Hardware / Software to Generate Key Pair

HSM equivalent to FIPS140-1 Level 3

6-1-1-4 Utilization Purpose of Private Key

For electronic signature

6-1-1-5 Reception of Public Key of JPKI BCA

Okayama-ken CA shall receive Public Key of JPKI BCA safely and surely in the exchange of the Cross Certificate.

6-1-1-6 Distribution of Public Key of the Governor of Okayama prefecture

The Self-signed Certificate shall be stored in the IC Card in the issuance of an Electronic Certificate, and shall be distributed to users. In addition, it shall be distributed to a signature verifier safely and surely.

6-1-2 Key of User

6-1-2-1 User who generates key pair of the Governor of Okayama Prefecture and Generation method

A user shall generate it with Key Pair Generator of the municipality of residence.

6-1-2-2 Safe Provision of Public Key of User to Municipality of Residence

The municipality of residence shall receive Public Key stored in IC Card directly from users.

6-1-2-3 Key Length

1024-bit RSA key shall be used.

6-1-2-4 Hardware / Software to Generate Key Pair

Key Pair Generator of the municipality of residence

6-1-2-5 Utilization Purpose of Private Key

For electronic signature

6-2 Protection of Private Key

6-2-1 Private Key of the Governor of Okayama Prefecture

6-2-1-1 Standard Required for Storage of Private Key

It shall be protected with HSM equivalent to FIPS140-1 Level 3.

6-2-1-2 Control of Private Key by Plural Persons

Private Key shall be protected with HSM controlled by plural managers of Private Key.

6-2-1-3 Escrow of Private Key

The escrow of Private Key shall not be executed.

6-2-1-4 Backup of Private Key

The backup of Private Key shall be carried out by plural managers of Private Key.

Private Key, which is backed up from HSM, shall be encrypted and stored safely. Managers of Private Key shall not take it out of the room where backup media are stored.

6-2-1-5 Storage of Private Key (Archive)

An archive of Private Key shall not be created.

6-2-1-6 Storage of Private Key in Cryptographic Module

Private Key shall be generated in HSM by plural managers of Private Key, and shall be stored in Cryptographic Module.

6-2-1-7 Activation of Private Key

Private Key shall be activated by plural managers of Private Key.

6-2-1-8 Deactivation of Private Key

Private Key shall be deactivated by plural managers of Private Key.

6-2-1-9 Abolition of Private Key

Regarding the abolition of Private Key in Cryptographic Module, plural managers of Private Key shall render Cryptographic Module completely inoperative through initialization etc. If Cryptographic Module is removed from the room, Cryptographic Module shall be destroyed physically.

In addition, Cryptographic Module for backup of Private Key which is abolished shall be abolished.

6-2-2 Private Key of User

6-2-2-1 Standard Required for Storage of Private Key

It shall be protected by Tamper-Resistant IC Card (Private Key cannot be read out physically) where card application conformable to “JPKI Card Application External Interface Specifications 1.1” is installed.

6-2-2-2 Escrow of Private Key

The Governor of Okayama prefecture shall not accept the escrow of Private Key from a user and the escrow of Private Key by a user shall not be permitted.

6-2-2-3 Backup of Private Key

Private Key shall be stored in IC Card, and the backup shall not be conducted.

6-2-2-4 Storage of Private Key in Cryptographic Module (IC Card)

Private Key of a user shall be generated with Key Pair Generator of the municipality of residence, and shall be stored in IC Card of a user. After storage in IC Card, Private Key generated with Key Pair Generator shall be completely deleted from Key Pair Generator.

6-2-2-5 Activation of Private Key

Private Key of a user shall be activated by a user with a password

6-2-2-6 Deactivation of Private Key

Private Key shall be deactivated by the operation of IC Card.

6-2-2-7 Abolition of Private Key

Regarding the abolition of Private Key of a user, a user shall abolish it with the terminals at reception window and Key Pair Generator of the municipality of residence.

6-3 Other Aspects concerning Key Pair Generation Management

6-3-1 Key of the Governor of Okayama Prefecture

6-3-1-1 Storage of Public Key

Public Key shall be included in the Self-signed Certificate and stored in the archive where the measures to prevent someone from changing data are taken for the period specified in “4-12 Storage of Record (Archive)” in this Practice Statement.

6-3-1-2 Use Period of Public Key and Private Key

The validity period of the Self-signed Certificate of the Governor of Okayama prefecture shall be 10 years. The use period of Private Key shall be 5 years after the date the key is generated and the key shall be updated every 5 years.

However, when the security of secret code is judged to have become vulnerable, a change of cryptosystem may be considered and the key may be updated at the time.

6-3-2 Key of User

The use period of Public Key and Private Key of a user shall be 3 years after the date when the key is generated.

However, when the security of secret code is judged to have become vulnerable, the change of cryptosystem may be considered and the key may be updated at the time.

6-4 Activation Data

6-4-1 Key of the Governor of Okayama Prefecture

6-4-1-1 Generation and Installation of Activation Data

The activation data of HSM where Private Key of the Governor of Okayama prefecture is stored shall be set by Management Key.

6-4-1-2 Protection of Activation Data

Management Key required for the activation of HSM where Private Key of the Governor of Okayama prefecture is stored shall be stored safely.

6-4-2 Key of User

6-4-2-1 Generation and Installation of Activation Data

The activation data (password) of Private Key of a user shall be set in IC Card by the user with Key Pair Generator when Key Pair is generated.

6-4-2-2 Protection of Activation Data

The activation data of Private Key of a user shall be changed periodically and stored safely.

6-5 Computer Security Management

6-5-1 Requirement concerning Computer Security Function

The system of Okayama-ken CA shall be equipped with use of reliable OS, access control, function of personnel's identification and authentication, Audit Log, collection function of archive data, recovery function of system etc.

6-5-2 Computer Security Evaluation

The security evaluation of the system shall be conducted as needed.

6-6 Life-Cycle Security Management

6-6-1 Security Management for System Development

The development, correction or change of the system concerning this service shall be conducted through a reliable organization and in a reliable environment according to the prescribed procedure. The system which has been developed, corrected or changed shall be introduced after the validation in test environment and approval by the chief administrator of CA. The system specifications and the report on validation shall be documented and stored.

6-6-2 Security Management for System Operation

6-6-2-1 Okayama-ken CA

To maintain the system concerning this service, the security check of OS and software shall be done periodically and the results of validation shall be documented and stored.

6-6-2-2 Municipality

To maintain the system concerning this service, the security management of OS and software of Key Pair Generator and the terminals at reception window shall be conducted appropriately.

6-7 Network Security Management

To prevent unauthorized access, the network service which permits passing through an external network shall be minimized. In addition, sufficient security protection measures such as detection of intrusion shall be taken.

The disclosed information within the information which is held in Repository shall be provided via Fire Wall.

6-8 Technical Management of Cryptographic Module

It shall be specified in "6-1-1-3 Hardware / Software to Generate Key Pair" and "6-2-1-1 Standard Required for Storage of Private Key" in this Practice Statement.

7. Contents of Certificate and Revocation Record (CRL/ARL)

7-1 Certificate

7-1-1 Electronic Certificate

The Electronic Certificate shall include the following information. The details shall be specified in Profile Specifications.

- Version number (Version number of X.509 Certificate format)
- Serial number (Number to identify the certificate issued in Okayama-ken CA)
- Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said Electronic Certificate)
- Information on issuer (The name of the Governor of Okayama prefecture who issued said Electronic Certificate is written with X.500 Distinguished Name)
- Start date of validity period (Date when said Electronic Certificate is issued)
- End date of validity period (3 years after the date of issuance)
- Public Key (Public Key of a user)
- Extended information (Four Basic Information Items of a user and intended use of Key etc. are included.)

7-1-2 Cross Certificate

The Cross Certificate which is required in the cross certification with JPKI BAC shall include the following information. The details shall be specified in Profile Specifications.

- Version number (Version number of X.509 Certificate format)
- Serial number (Number to identify the certificate issued in Okayama-ken CA)
- Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said Cross Certificate)
- Information on issuer (The name of the Governor of Okayama prefecture who issued said Cross Certificate is written with X.500 Distinguished Name)
- Start date of validity period (Date when said Cross Certificate becomes effective)
- End date of validity period (5 years after the date when said Cross Certificate becomes effective)
- Public Key (Public Key of Cross Certification CA)
- Extended information

7-1-3 Self-signed Certificate

The Self-signed Certificate of the Governor of Okayama prefecture shall include the following information. The details shall be specified in Profile Specifications.

- Version number (Version number of X.509 Certificate format)
- Serial number (Number to identify the certificate issued in Okayama-ken CA)
- Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said Self-signed Certificate)
- Information on issuer (The name of the Governor of Okayama prefecture who issued said Self-signed Certificate is written with X.500 Distinguished Name)
- Start date of validity period (Date when said Self-signed Certificate is issued)
- End date of validity period (10 years after the date of issuance)
- Public Key (Public Key of the Governor of Okayama prefecture)
- Extended information

7-1-4 Link Certificate

The Link Certificate which is required when the Governor of Okayama prefecture updates Key shall include the following information. The details shall be specified in Profile Specifications.

・Version number (Version number of X.509 Certificate format)
・Serial number (Number to identify the certificate issued in Okayama-ken CA)
・Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said Link Certificate)
・Information on issuer (The name of the Governor of Okayama prefecture who issued said Link Certificate is written with X.500 Distinguished Name)
・Start date of validity period（OldWithNew：Date when previous-generation Key Pair was generated, NewWithOld：Date when new-generation Key Pair was generated）
・End date of validity period（OldWithNew：End date of the validity period of previous-generation Self-signed Certificate, NewWithOld：End date of the validity period of previous-generation Self-signed Certificate）
・Public Key（OldWithNew：Previous-generation Public Key, NewWithOld：New-generation Public Key）
・Extended information

7-2 Revocation Record (CRL/ARL)

7-2-1 Revocation Record of Electronic Certificate (CRL)

The revocation record of the Electronic Certificate (CRL) shall include the following information. The details shall be specified in CRL Profile in Profile Specifications.

・Version number (Format version number of CRL)
・Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said CRL)
・Information on issuer (The name of the Governor of Okayama prefecture who issued said CRL is written with X.500 Distinguished Name)
・Start date of validity period (Date when said CRL becomes effective)
・End date of validity period (3 days after the date when said CRL becomes effective)
・Date of next update (1 day after the date when said CRL becomes effective)
・Information on revoked certificate (serial number, revocation date, revocation reason)
・Extended information

7-2-2 Revocation Record of Cross Certificate (ARL)

The revocation record (ARL) of the Cross Certificate shall include the following information. The details shall be specified in ARL Profile in Profile Specifications.

・Version number (Format version number of ARL)
・Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said ARL)
・Information on issuer (The name of the Governor of Okayama prefecture who issued said ARL is written with X.500 Distinguished Name)
・Start date of validity period (Date when said ARL becomes effective)
・End date of validity period (3 days after the date when said ARL becomes effective)
・Date of next update (1 day after the date when said ARL becomes effective)
・Information on revoked certificate (serial number, revocation date, revocation reason)
・Extended information

7-2-3 Revocation Record of Self-signed Certificate (ARL)

The revocation record of the Self-signed Certificate (ARL) shall include the following information. The details shall be specified in ARL Profile in Profile Specifications.

・Version number (Format version number of ARL)
・Signature algorithm (Information on the algorithm which was used when the Governor of

Okayama prefecture signed on to said ARL)

- Information on issuer (The name of the Governor of Okayama prefecture who issued said ARL is written with X.500 Distinguished Name
- Start date of validity period (Date when said ARL becomes effective)
- End date of validity period (3 days after the date when said ARL becomes effective)
- Date of next update (1 day after the date when said ARL becomes effective)
- Information on revoked certificate (serial number, revocation date, revocation reason)
- Extended information

7-2-4 Revocation Record of Link Certificate (ARL)

The revocation record of the Link Certificate (ARL) shall include the following information. The details shall be specified in ARL Profile in Profile Specifications.

- Version number (Format version number of ARL)
- Signature algorithm (Information on the algorithm which was used when the Governor of Okayama prefecture signed on to said ARL)
- Information on issuer (The name of the Governor of Okayama prefecture who issued said ARL is written withX.500 Distinguished Name
- Start date of validity period (Date when said ARL becomes effective)
- End date of validity period (3 days after the date when said ARL becomes effective)
- Date of next update (1 day after the date when said ARL becomes effective)
- Information on revoked certificate (serial number, revocation date, revocation reason)
- Extended information

8. Management of Certification Practice Statement

8-1 Change Management of Certification Practice Statement

The Governor of Okayama prefecture shall change this Practice Statement as needed.

8-2 Disclosure and Notification

If this Practice Statement is changed, the Governor of Okayama prefecture shall disclose the changed Practice Statement on the Web immediately. This shall be the notification to a user, a signature verifier etc., and a signature checker.

8-3 Procedure related to Approval of Certification Practice Statement

It shall become effective subject to decision of the Governor of Okayama prefecture.