DNSSEC Practice Statement for the jprs Zone (.jprs DPS)

1. INTRODUCTION

This document, "DNSSEC Practice Statement for the jprs Zone (.jprs DPS)" states ideas of policies and practices of Japan Registry Services Co., Ltd. (JPRS) with regard to DNSSEC operations for the jprs zone.

1.1. Overview

JPRS has published .jprs DPS to provide operational information about DNSSEC (*1) for the jprs zone. To accomplish comprehensive investigation into the ideas of operational security, policies, practices and procedures of DNSSEC service for the jprs zone (".jprs DNSSEC Service"), .jprs DPS adopts the DPS framework (*2) which has been proposed and discussed in IETF Domain Name System Operations (DNSOP) Working Group.

Chapters of this document are shown as follows.

1. INTRODUCTION
2. PUBLICATION AND REPOSITORIES
3. OPERATIONAL REQUIREMENTS
4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS
5. TECHNICAL SECURITY CONTROLS
6. ZONE SIGNING
7. COMPLIANCE AUDIT
8. LEGAL MATTERS

----

*1: DNSSEC (DNS Security Extensions) is a set of specifications for enabling origin authentication and data integrity verification of DNS response, by composing digital signatures on it. The fundamental specifications of DNSSEC are described in following RFCs, where DNS resource records such as DS, DNSKEY, RRSIG and NSEC are newly defined.

- RFC 4033
  DNS Security Introduction and Requirements
  https://www.ietf.org/rfc/rfc4033.txt

- RFC 4034
  Resource Records for the DNS Security Extensions
  https://www.ietf.org/rfc/rfc4034.txt

- RFC 4035
  Protocol Modifications for the DNS Security Extensions
  https://www.ietf.org/rfc/rfc4035.txt

*2: DPS (DNSSEC Practice Statement) is a document in which operator states ideas of security, policies, practices and procedures with regard to operational issues of DNSSEC. DPS framework is described in following RFC.

- RFC 6841
  A Framework for DNSSEC Policies and DNSSEC Practice Statements
  https://www.ietf.org/rfc/rfc6841.txt

1.2. Document Name and Identification

DNSSEC Practice Statement for the jprs Zone (.jprs DPS)
Version: 1.6
Available on: 2022/10/25
Effective on: 2022/10/25

1.3. Community and Applicability

In this section, associated entities and their roles regarding .jprs DNSSEC Service are described.

1.3.1. Registry

JPRS is the Registry for the .jprs domain names. The Registry administrates registrations of .jprs domain names and operates DNS servers for the jprs zone. As for .jprs DNSSEC Service, the Registry generates signing keys (KSK and ZSK) (*3) of the jprs zone and composes digital signatures for the jprs zone. Further, through registering DS resource record(s) of the Registry into the root zone, the Registry enables origin authentication and data integrity verification of resource records in the jprs zone by using KSK of the root zone as a trust anchor (*4).

----

*3: Signing key is a pair of public key and private key used for signing resource records in a zone. KSK is abbreviation for key signing key, while ZSK for zone signing key.

*4: Trust anchor is information cryptographically equivalent to KSK of given zone that DNSSEC-aware resolvers use to establish a chain of trust from the given zone to the querying zone.

1.3.2. .jprs Registrar

.jprs Registrar of the .jprs domain names is an entity who has concluded an agreement with the Registry for agency operations on .jprs domain name registrations. .jprs Registrar submits various requests regarding registrations of domain name information, including DS resource records in the jprs zone.

1.3.3. Registrant

Registrant is an entity who has registered .jprs domain name(s) info the Registry. For deploying DNSSEC into the Registrant's domain name(s), Registrant generates signing keys and composes digital signatures on Registrant's zone ("Registrant Zone"). Registrant enables origin authentication and data integrity verification of Registrant Zone by registering DS resource record(s) into the Registry through .jprs Registrar. In some cases, Registrant requests "DNS Provider", who provides operation services for authoritative DNS servers, to generate signing keys, compose digital signatures on Registrant Zone and generate DS resource record(s).

1.3.4. Relying party

Relying party is all the entity related to .jprs DNSSEC Service, including DNS Providers, caching DNS server operators and users who utilize their services. Here we call the DNS Provider who manages Registrant Zone as "Registrant Zone Manager". In some cases, Registrant him/her-self may be Registrant Zone Manager.

1.3.5. Auditor

Auditor is an entity who audits whether .jprs DNSSEC Service is operated along with .jprs DPS or not.

1.3.6. Applicability

.jprs DPS is applied to the jprs zone. DNS users are able to conduct origin authentication and verify data integrity of DNS responses from the jprs zone. Registrant Zones are under Registrant's policy and outside the scope of .jprs DPS.

1.4. Specification Administration

1.4.1. Specification administration organization

Japan Registry Services Co., Ltd. (JPRS)

1.4.2. Contact information

Japan Registry Services Co., Ltd. (JPRS) .jprs DPS contact
Telephone: +81-3-5215-8451
(9:00-18:00 excluding Saturdays, Sundays, national holidays or the period from December 29 to January 3)
E-mail: info@jprs.jp

1.4.3. Specification change procedures

.jprs DPS is revised annually and/or in case of arising legitimate needs, by DPS Management Officer (Section 4.2.1). After an approval of its revised contents by DNSSEC Steering Committee (Section 4.2.1), the revised .jprs DPS becomes publicly available in such a way as described in chapter 2.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

2.1.1. Operational entity

The entity that operates repositories is JPRS as a Registry.

2.1.2. Locations of the repositories

.jprs DPS (Japanese)
https://nic.jprs/doc/jprs-dps-ja.pdf

.jprs DPS (English)
https://nic.jprs/doc/jprs-dps-en.pdf

2.1.3. Access Controls on Repositories

The Registry does not perform particular access controls on .jprs DPS except for read only access.

2.2. Publication of Public Keys

The Registry makes to be able to establish a chain of trust of DNSSEC by registering a DS resource record of the jprs zone into the root zone. Therefore, the Registry does not explicitly publish KSK public key of the jprs zone as a trust anchor.

The Registry will publish KSK and ZSK public keys of the jprs zone during key rollovers described in Section 6.4 are carrying out. The DNSKEY resource records of the KSK and ZSK public keys are published during the key rollovers by registering in jprs zone.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of Domain Names

The purpose of the registration of domain names in the jprs zone is to use as an identifier on the Internet, and its meaning is the uniqueness of the domain name in the .jprs domain name space which our company manages. There is no other meanings except this.

3.2. Identification and Authentication of Registrant Zone Manager

Authentication of applicant related to Registrant Zone is conducted by .jprs Registrar who exclusively manages the Registrant's domain name registration into the jprs zone ("Associated .jprs Registrar"). The Registry employs prescribed authentication procedures to check whether data registration requests, including registration of DS resource record(s), are carried out by Associated .jprs Registrars or not.

3.3. Registration of Delegation Signer (DS) Resource Records

A Registrant Zone can be verified as a DNSSEC-aware zone when DS resource record(s) of the Registrant Zone is registered into the jprs zone. The specification of DS resource record on registration is described in Section 4.1 of RFC 5910.

- RFC 5910
  Domain Name System (DNS) Security Extensions Mapping For the Extensible Provisioning Protocol (EPP)
  https://www.ietf.org/rfc/rfc5910.txt

3.3.1. Who can request registration

The Registry registers DS resource records for Registrant Zones into the jprs zone based on the requests from Associated .jprs Registrars. Associated .jprs Registrars confirm the intentions of registration with Registrants before requesting the registrations to the Registry.

3.3.2. Procedure for registration request

Registrant asks Associated .jprs Registrar for registering DS resource record(s) into the jprs zone. Associated .jprs Registrar proceeds the request of registration to the Registry based on the Registrant's intention, according to the procedures defined by the Registry. Upon the request from Associated .jprs Registrar, the Registry registers DS resource record(s) into the jprs zone. The time required for registering a DS resource record into the jprs zone after receiving the registration request by the Registry depends on the update schedule of .jprs DNS.

When a DS resource record corresponding to a signing key used in a given Registrant zone is published in the jprs zone, which is operated by the Registry, and digitally signed with a signing key of the Registry, a chain of trust from the jprs zone to the Registrant Zone comes to be established.

3.3.3. Emergency registration request

Not applicable in this document.

3.4. Method to Prove Possession of Private Key

The Registry does not specify requirements of validation checks made by Associated .jprs Registrar whether the Registrant Zone Manager possesses private key corresponding to DS resource record on registration or not.

3.5. Removal of DS Resource Record

DNSSEC-verification of the Registrant Zone becomes unavailable by removing Registrant's DS resource record from the jprs zone.

3.5.1. Who can request removal

The Registry removes DS resource records for the Registrant Zones from the jprs zone based on the requests from Associated .jprs Registrars. Associated .jprs Registrars confirm the intentions of removal with the Registrants before requesting removals.

3.5.2. Procedure for removal request

Registrant asks Associated .jprs Registrar for removing DS resource record(s) from the jprs zone. Associated .jprs Registrar proceeds request of removal from the Registry based on the Registrant's intention, according to the procedures defined by the Registry. Upon the request from Associated .jprs Registrar, the Registry removes DS resource record(s) from the jprs zone. The time required for removing a DS resource record from the jprs zone after receiving the removal request by the Registry depends on the update schedule of .jprs DNS.

3.5.3. Emergency removal request

Not applicable in this document.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

The Registry installs important facilities and equipment related to .jprs DNSSEC Service ("the Important Facilities") at a place where is not easily affected by disasters including water exposures, earthquakes, fires and thunder strikes ("the Important Facility Room"). The Registry takes building structures so that the room will be earthquake/fire-proofed and protected from trespassing. The location of the Important Facility Room is not indicated inside/outside of the building.

4.1.2. Physical access

With regard to the Important Facility Room, the Registry controls entry and exit from the room by conducting the identification of relevant person and checking of the entry permission. The Registry does not permit person who has no entry permission to enter the room. If entry of such person is unavoidable, the person will be allowed to enter by receiving one-time entry permission beforehand and accompanied by person who has entry permission.

4.1.3. Power and air conditioning

The Registry ensures sufficient supply of electric power to the Important Facilities and takes countermeasures against temporary blackout, electric power failure and fluctuation of voltage/frequency. Further, the Registry maintains and manages air conditioning facilities in order to avoid harmful effects to machines and equipment in use.

4.1.4. Water exposures and earthquakes

The Registry takes waterproofing measures for the Important Facility Room to minimize damages due to water exposures. Further, the building where facilities and equipment related to .jprs DNSSEC Service are housed has quakeproof structure, and measures are taken to prevent equipment and fixtures from toppling or falling.

4.1.5. Fire prevention and protection

The Registry installs the Important Facilities in a fire protection zone. Further, in this zone, fire prevention measures are taken for electric power supplying facilities and air conditioning, in addition to fire alarm apparatus and fire extinguishing facilities.

4.1.6. Media storage

The Registry stores recording media containing important archive/backup data related to .jprs DNSSEC Service in a storage cabinet(s) within a room where entry and exit are controlled appropriately.

4.1.7. Waste disposal

The Registry appropriately carries out disposal processing of documents/recording media including confidential information related to .jprs DNSSEC Service by prescribed methods, such as zeroing data or cutting up media.

4.1.8. Off-site backup

The Registry separately stores the specified important information related to .jprs DNSSEC Service in lockable cabinets in the Important Facility Rooms set at multiple sites which are sufficiently remote.

4.2. Procedural Controls

4.2.1. Trusted role

Followings are the roles related to operations of .jprs DNSSEC Service.

Role (abbreviation)

- Descriptions

DNSSEC Steering Committee (DSC)

- Supervision of .jprs DNSSEC Service
- Approval of revised .jprs DPS

Chief DPS Management Officer (cDMO)

- Appointment of DPS Management Officer
- Confirmation of revised .jprs DPS

DPS Management Officer (DMO)

- Drafting/revision of .jprs DPS

Chief DNSSEC Signing Key Officer (cSKO)

- Appointment of DNSSEC Signing Key Operator

DNSSEC Signing Key Operator (SKO)

- Activation of KSK used for .jprs DNSSEC Service
- Generation/Deletion of KSK/ZSK used for .jprs DNSSEC Service
- Rollover of KSK/ZSK used for .jprs DNSSEC Service
- Composition of signature for the jprs zone by KSK/ZSK
- Registration of DS resource record(s) of the jprs zone into the root zone
- Recording of KSK-related operations for .jprs DNSSEC Service

- Other operations under the instruction of cSKO

Chief DNSSEC Key Activation Observer (cKAO)

- Appointment of DNSSEC Key Activation Observer

DNSSEC Key Activation Observer (KAO)

- Observation of activation of KSK used for .jprs DNSSEC Service

----

Chief DNSSEC Key Ceremony Recording Officer (cKRO)

- Appointment of DNSSEC Key Ceremony Recording Officer

DNSSEC Key Ceremony Recording Officer (KRO)

- Recording of DNSSEC Key Ceremony

DNSSEC Operations Auditor (Auditor)

- Audit of DNSSEC Operations

4.2.2. Number of persons required per task

SKO consists of multiple personnel. In case of KSK-related operation including the key activation, KAO joins in the operation with SKO members.

4.2.3. Identification and authentication for each role

Permissions to operate the Important Facilities are authorized for each operator. In using the Important Facilities, only authorized operations are granted after operators are authenticated.

4.2.4. Tasks requiring separation of duties

The same person is not assigned as both SKO and KAO at the same time. This is to ensure that KSK is not activated by SKO him/her self.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Persons who have "Trusted Role" as described in Section 4.2.1 are limited to full time employees of the Registry or those who are specifically approved by the Registry.

4.3.2. Background check procedures

Not applicable in this document.

4.3.3. Training requirements

The Registry gives trainings to persons who have "Trusted Role" as described in 4.2.1 as follows:

- Before having roles of listed in "4.2.1 Trusted Role", required trainings for the roles are performed.
- When operational procedure is changed, affected descriptions in operation manuals are updated promptly and trainings associated with the change are provided.

The Registry periodically examines the necessity of re-training for persons who have "Trusted Role" as described in 4.2.1. Re-training is provided as necessary.

4.3.4. Job rotation frequency and sequence

Not applicable in this document.

4.3.5. Sanctions for unauthorized actions

Not applicable in this document.

4.3.6. Contracting personnel requirements

Not applicable in this document.

4.3.7. Documentation supplied to personnel

The Registry discloses a set of required documents for operations in .jprs DNSSEC Service to the personnel and ensures that they are fully acquainted with the documents.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

In order for detecting incorrect/illegal operations and proving legitimacy of operations related to .jprs DNSSEC Service, the Registry records following events as "the Audit Logs":

- Events of access to facilities for .jprs DNSSEC Service

- Events of operations using signing keys
  - Activation of KSK used for .jprs DNSSEC Service
  - Generation/Deletion of KSK/ZSK used for .jprs DNSSEC Service
  - Rollover of KSK/ZSK used for .jprs DNSSEC Service
  - Composition of signature for the jprs zone by KSK/ZSK
  - Registration of DS resource record(s) of the jprs zone into the root zone
- Events of confirmation for recorded facts in the Audit Logs

The record of events includes date and time of event, entity that initiated event and contents of event.

4.4.2. Frequency of processing log

The Registry automatically checks the Audit Logs in a frequency sufficient to monitor promptly whether serious security incidents occur or not. If any records to be dealt with are detected, immediate notification will be made to appropriate personnel.

4.4.3. Retention period for audit log information

The Registry keeps the Audit Logs for at least 3 months in a manner of being able to access them promptly. Archives of the Audit Logs are kept for at least 3 years.

4.4.4. Protection of audit log

The Registry limits access to the Audit Logs to only necessary personnel in order to protect the Audit Logs from browse, modification or deletion by unauthorized parties.

4.4.5. Audit log backup procedures

The Registry backups the Audit Logs on external media storage periodically. This media is stored in lockable cabinet(s) in a room where entry and exit are controlled appropriately.

4.4.6. Audit collection system

Online Audit Log collection system is a component of the system used for .jprs DNSSEC Service (".jprs DNSSEC Service System"), and is installed in the same place as that of .jprs DNSSEC Service System. Offline Audit Logs are recorded by the Trusted Roles described above and stored in secure storage cabinet(s) at facility managed by the Registry.

4.4.7. Vulnerability assessments

The Registry carries out vulnerability monitoring as described in Section 4.4.2 in order to detect unauthorized actions such as break-in attempt on .jprs DNSSEC Service System. Vulnerability assessments on the system are also taken as necessary.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

If the private key of the jprs zone is (likely to be) compromised, the Registry carries out emergency rollover of the signing key. When .jprs DNSSEC Service becomes discontinued due to accidents or disasters, the Registry attempts to restart .jprs DNSSEC Service as quickly as possible.

4.5.2. Corrupted computing resources, software, and/or data

When important hardware, software or data related to .jprs DNSSEC Service is broken/damaged, the Registry attempts to recover it promptly using backup-ed hardware, software or data according to the prescribed recovery plan.

4.5.3. Entity private key compromise procedures

When the KSK of the jprs zone becomes compromised, the Registry carries out the following procedures:

- Re-generation of KSK of the jprs zone;
- Composition of signature for DNSKEY resource records in the jprs zone by re-generated KSK; and
- Replacement of DS resource record registered in the root zone with the one corresponding to re-generated KSK.

When the ZSK of the jprs zone becomes compromised, the Registry carries out the following procedures:

- Re-generation of ZSK of the jprs zone;
- Composition of signature for DNSKEY resource records containing re-generated ZSK by KSK of the jprs zone; and
- Composition of signatures for authoritative records in the jprs zone by re-generated ZSK.

4.5.4. Business continuity and IT disaster recovery capabilities

For cases where continuation of .jprs DNSSEC Service is disabled due to damage on the facilities by a disaster, the Registry attempts to recover the service shortly on the remote backup-site configured beforehand.

In addition, if the Registry cannot practice the DNSSEC key ceremony by the normal procedure due to a disaster or other reasons, the Registry will practice the DNSSEC key ceremony according to the emergency response procedure determined beforehand.

4.6. Entity Termination

In order to prepare for cases where continuation of .jprs DNSSEC Service is disabled due to termination of the Registry, information necessary for .jprs DNSSEC Service is deposited into escrow agent, according to the following document.
.jprs Registry Agreement
https://www.icann.org/en/about/agreements/registries/jprs/

In case of termination of the Registry, .jprs DNSSEC Service will be also terminated in accordance with the operation termination procedures defined by the Registry.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Signing key used for .jprs DNSSEC Service is generated by multiple SKO in offline system installed in the Important Facility Room (".jprs DNSSEC Service Offline System"). KSK of the jprs zone is generated by software inside the dedicated cryptographic module connected to the system. ZSK of the jprs zone is generated in the system and stored in removable media in which all the data are encrypted ("the Encryption Media").

5.1.2. Public key delivery

The Registry deploys KSK public key and ZSK private/public key into .jprs DNSSEC Service System by using the Encryption Media. KSK public key is not distributed to relying parties in any other way of DNS protocols.

5.1.3. Public key parameters generation and quality checking

The Registry periodically confirms that generation of signing key is conducted with appropriate parameters in the context of technological trends.

5.1.4. Key usage purposes

The Registry uses the signing keys only for generating signatures for the jprs zone and does not use them for any other purposes.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic module standards and controls

Not applicable in this document.

5.2.2. Private key multi-person control

Operations using KSK private key are performed by multiple SKO.

5.2.3. Private key escrow

Private keys of the jprs zone are not escrowed.

5.2.4. Private key backup

SKO backups multiple copies of KSK private key into separate cryptographic modules. These cryptographic modules are stored in lockable cabinets inside the Important Facility Rooms mentioned in 4.1.8.

5.2.5. Private key storage on cryptographic module

Not applicable in this document.

5.2.6. Private key archival

Obsolete private keys are not archived, except for backups mentioned above.

5.2.7. Private key transfer into or from a cryptographic module

Once KSK private key is installed in the cryptographic module, it cannot be retrieved. In case of using KSK private key installed in the cryptographic module, operation by multiple SKO is required.

For installing ZSK private key into the Encryption Media, operation by multiple SKO is also required.

5.2.8. Method of activating private key

KSK private key is activated by multiple SKO in .jprs DNSSEC Service Offline System and the fact is observed by KAO. ZSK private key is activated by multiple SKO. The active status of ZSK signing key continues until the usage period is finished.

5.2.9. Method of deactivating private key

Once KSK private key is used by SKO it is deactivated immediately and the fact is observed by KAO. ZSK private key is deactivated by multiple SKO before it reaches upper limit of the usage period described in Section 5.3.2.

5.2.10. Method of destroying private key

KSK/ZSK private key is destroyed by SKO in a manner it cannot be used again.

5.3. Other Aspects of Key Pair Management

5.3.1. Life cycle states for management

The following is the life cycle states of KSK for key management:

- Generation of KSK
- Registration of KSK into the jprs zone and the root zone
- Deletion of KSK from the root zone and the jprs zone
- Destroying of KSK

The following is the life cycle states of ZSK for key management:

- Generation of ZSK
- Registration of ZSK into the jprs zone
- Activation of ZSK
- Inactivation of ZSK
- Deletion of ZSK from the jprs zone
- Destroying of ZSK

5.3.2. Key usage periods

The upper limit of usage period for KSK is one year plus appropriate period for transition. The upper limit of usage period for ZSK is one month. The Registry may change these periods as necessary.

5.4. Activation Data

5.4.1. Activation data generation and installation

Activation data is a set of passphrases used to activate KSK. Each SKO generates passphrase individually and install it into .jprs DNSSEC Service Offline System.

5.4.2. Activation data protection

SKO protects activation data in a sufficiently secure manner.

5.4.3. Other aspects of activation data

In order to prepare for emergencies, SKO seals a copy of activation data in envelope(s) with tamper trail. In case of arising necessity to break this seal, it will be done under control of cSKO.

5.5. Computer Security Controls

On the important components of .jprs DNSSEC Service System ("the Important Components"), only minimum necessary software defined by the Registry runs. All the important operations on the Important Components will be logged. All the authentication credentials used to access the Important Components are properly controlled. The Important Components are monitored continuously, and if any abnormalities or illegal operations on them are detected, the Registry takes appropriate countermeasures promptly.

5.6. Network Security Controls

Firewalls are applied to networks on which .jprs DNSSEC Service is deployed, and access from outside of the networks is limited to minimum necessary protocols defined by the Registry.

5.7. Timestamping

The Registry obtains time for .jprs DNSSEC Service Offline System from reliable time source(s) and synchronizes the system clocks with it. As for .jprs DNSSEC Service System, the Registry obtains time from NTP (Network Time Protocol) and synchronizes the system clocks. The synchronized times are used for timestamping for the audit logs described in Section 4.4 and inception/expiration time for validity period of RRSIG.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

The Registry controls each process at system development and evaluates the system prior to deploying it, in order to maintain the quality and security of .jprs DNSSEC Service System.

5.8.2. Security management controls

As security controls of .jprs DNSSEC Service System, the registry undertakes countermeasures such as entering/leaving controls, staff controls including training, operation controls including authority control and system controls including intrusion protection and virus protection.

5.8.3. Life cycle security controls

The Registry evaluates periodically whether the development of .jprs DNSSEC Service System is controlled under prescribed manner. Moreover, the Registry gathers information related to security, surveys technical trends, and evaluates/improves the system as necessary.

6. ZONE SIGNING

6.1. Key Lengths, Key Types, and Algorithms

The key types of signing keys of the jprs zone are KSK and ZSK. Therefore, the secure entry point (SEP) bit of KSK specified in RFC 4034 is set, and the SEP bit of ZSK is unset.
Algorithms defined by the protocol standards are adopted for signing keys of the jprs zone. Algorithm and key length for signing key that are considered secure for the usage period are adopted. Therefore, the algorithm for both KSK and ZSK is RSASHA256 specified in RFC 5702, and the key length of KSK is 2048 bits and that of ZSK is 1024 bits.

6.2. Authenticated Denial of Existence

For authenticated denial of existence in the jprs zone, the method using NSEC3 resource records with Opt-Out flag specified in RFC 5155 is adopted. The values of hash algorithm, iterations and salt are set to SHA-1, no extra iterations and empty salt, respectively.

6.3. Signature Format

The signature format for resource records in the jprs zone is RSA/SHA-2 specified in RFC 5702.

6.4. Key Rollover

6.4.1. Zone Signing Key Rollover

In the jprs zone, rollover of ZSK is carried out on a monthly basis by the pre-publish method described in RFC 6781.

6.4.2. Key Signing Key Rollover

In the jprs zone, rollover of KSK is carried out on an annual basis by the double signature method described in RFC 6781.

6.5. Signature Validity Period and Re-signing Frequency

In the jprs zone, signature validity period for KSK is around 2 months, while that for ZSK is around 1 month. Re-signing frequencies for KSK and ZSK are per month and per week, respectively.

6.6. Verification of Resource Records

The Registry verifies that all the resource records are conformant with the protocol standards before they are published on the jprs zone.

6.7. Resource Records TTL

In the jprs zone, TTL of DNSKEY and the corresponding RRSIG is set to 86400 (1 day). TTL of DS and the corresponding RRSIG is set to 7200 (2 hr.). TTL of NSEC3 and the corresponding RRSIG is set to 900 (15min.), which is the same as negative cache value for the jprs zone. Those TTLs may be changed into appropriate values along with technical trends.

7. COMPLIANCE AUDIT

A regular audit for .jprs DNSSEC Service is done by Auditor described in Section 1.3.5. The audit reports are provided to the Registry. The Registry applies operational improvements to .jprs DNSSEC Service as necessary.

8. LEGAL MATTERS

The Registry has no legal responsibilities for the matters described in .jprs DPS. When operating .jprs DNSSEC Service, the Registry follows the laws of Japan and the rules defined by the Registry.

Registration Policies (.jprs)
https://nic.jprs/doc/jprs-registration-policies.pdf

Update History:

Version 1.0 (19 Mar. 2014)

- Published the initial version of this document

Version 1.1 (29 Jun. 2015)

- Changed the name and explanation of trusted roles
- Fixed some typographical errors and omissions

Version 1.2 (1 Oct. 2015)

- Changed the qualifications, experience, and clearance requirements
- Fixed some typographical errors and omissions

Version 1.4 (1 Aug. 2019)

- Changed to update base version

Version 1.5 (1 Sep. 2021)

- Revised the trusted roles
- Fixed some typographical errors and omissions

Version 1.6 (25 Oct. 2022)

- Clarified description regarding measures to be taken when the key ceremony cannot be held due to a disaster, etc.
- Revised specification for NSEC3 parameters