FAITID DNSSEC
Practice Statement

Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID)

Version: 1.1

Date: 2019-Jul-25

Contents

Contents 2

1 Introduction 3
1.1 Overview 3
1.2 Document Name and Identification 3
1.3 Community and Applicability 3

1.4 3
1.4.1 Specification Administration Specification Administration Organization 3
1.4.2 Contact information 4
1.4.3 Specification Change Procedures 4
1.4.4 Specification Administration Organization 4

2 Publication and Repositories 4
2.1 Repositories 4
2.2 Publication of Public Keys 4

3 Operational Requirements 4
3.1 Registration of delegation signer (DS) resource records 4
3.2 Method to prove possession of private key 5
3.3 Removal of DS resource records 5
3.3.1 Who can request removal 5
3.3.2 Emergency removal request 5

4 Facility, Management, and Operational Controls 5
4.1 Physical controls 5
4.1.1 Site location and construction 5
4.1.2 Physical access 5
4.1.3 Power and air conditioning 5
4.1.4 Water exposures 5
4.1.5 Fire prevention and protection 6
4.1.6 Media storage 6
4.1.7 Media & Waste disposal 6
4.1.8 Off-site backup 6
4.2.1 Trusted roles 6
4.2.2 Number of persons required per task 6
4.3 Personnel controls 6
4.3.1 Qualifications, experience, and clearance requirements 6
4.3.2 Training requirements 6
4.3.3 Contracting personnel requirements 6
4.3.4 Documentation supplied to personnel 7
4.4 Audit logging procedures 7
4.4.1 Types of events recorded 7
4.4.2 Protection of audit log 7
4.5 Compromise and disaster recovery 7
4.5.1 Incident and compromise handling procedures 7
4.5.2 Entity private key compromise procedures 7

5 Technical Security Controls 7
5.1 Key Pair Generation and Installation 7

5.1.1 Key Pair Generation ... 7
5.1.2 Public Key Delivery ... 7
5.1.3 Key Usage Purposes ... 8
5.2 Private Key Protection and Cryptographic Module Engineering Controls ... 8
5.2.1 Cryptographic Module Standards and Controls ... 8
5.2.2 Private Key Backup ... 8
5.2.3 Method of Activating Private Key ... 8
5.2.4 Private Key Transfer Into or From a Cryptographic Module ... 8
5.2.5 Method of Deactivating Private Key ... 8
5.2.6 Method of Destroying Private Key ... 9
5.3 Other Aspects of Key Pair Management ... 9
5.4 Computer Security Controls ... 9
5.5 Network Security Controls ... 9
5.6 Timestamping ... 9
5.7 Life Cycle Technical Controls ... 9
5.7.1 System Development Controls ... 9
6 Zone Signing ... 9
6.1 Key Lengths, Key Types, and Algorithms ... 9
6.2 Authenticated Denial of Existence ... 9
6.3 Signature Format ... 10
6.4 Key rollover ... 10
6.5 Signature Lifetime and Re-Signing Frequency ... 10
6.6 Verification of Resource Records ... 10
6.7 Resource Records Time-to-Live ... 10
7 Compliance Audit ... 10
7.1 Frequency of Entity Compliance Audit ... 10
7.2 Identity and Qualifications of Auditor ... 10
7.3 Auditor's Relationship to Audited Party ... 10
7.4 Topics Covered by Audit ... 11
7.5 Actions Taken as a Result of Deficiency ... 11
7.6 Communication of Results ... 11
8 Legal Matters ... 11
8.1 Fees ... 11
8.2 Financial Responsibility ... 11
8.3 Term and Termination ... 11
8.4 Limitations of Liability ... 11
8.5 Dispute Resolution Provisions ... 11
8.6 Governing Law ... 11

1 Introduction

1.1 Overview

The purpose of this document is to enable stakeholders to determine the level of trust they wish to grant to FAITID DNSSEC management. This document details the policies and procedures employed by FAITID in operating those zones for which it offers DNSSEC service. This statement includes in particular all the TLDs under FAITID management.

This document conforms to the IETF Internet draft describing DNSSEC Policy (DP) and DNSSEC Practice Statement (DPS) documents [RFC-6841], or it's most current successor. It also draws from the DPS documents published by others and attempts to follow its general structure.

The scope of this document includes provisions for the generation, management, application, and rollover of DNSSEC keying material, with accompanying processes for the proper maintenance of signed zones and availability of public keys for validation of the signed data, for the purpose of providing secure, reliable, correct deployment of signed DNS records in accord with the DNSSEC standards for TLD zones within the responsibility of FAITID.

1.2 Document Name and Identification

FAITID DNSSEC Policy and Practice Statement version 1.1, published on 2019-Jul-26 (abbreviated as "DPS" from here on).

1.3 Community and Applicability

The target communities for this document include:

- authors and users of applications throughout the public Internet using DNSSEC validation, with a need to evaluate the level of trust to apply to FAITID TLDs and their child domains;
- registrars and registrants of domains in FAITID TLDs;
- relying parties intending to use FAITID DNSSEC data to configure trust anchors;
- and reviewers and auditors interested in comparing FAITID operations with the policies and processes described here.

The roles and responsibilities for each stakeholder is described as follows:

Registry: All zones covered by this document have FAITID as a single registry. It is the responsibility of the registry to sign those zones and make their public keys available to the general public. The registry also enables its registrants to submit the public keys of their child zones via Delegation Signer (DS) Resource Records that are

passed by the Registrar through the use of the appropriate EPP extension as defined in [RFC-5910] or it's most current successor. These are then included in the signed parent zone.

Registrar: The registrar for a child zone is responsible for securely collecting, verifying and passing the DS records from the Registrant to the Registry using the EPP extension specified in [RFC-5910] or it's most current successor. This includes authentication that the party submitting the keying material for a given zone is the party responsible for the zone.

Registrant: The Registrant must ensure proper DNSSEC data has been submitted to the Registrar to allow for the trust anchors to be inserted in the parent zone.

Relying Party: Public key material published by FAITID as a trust anchor can be used by anyone interested in using the signed zones as secure entry points for DNSSEC. The relying party needs to ensure that it is using the current trust anchors.

1.4

1.4.1 Specification Administration Specification Administration Organization

FAITID is the authority for execution and any change to the policies and procedures discussed in this document.

1.4.2 Contact information

The point of contact for all aspects of Registry Operations under the responsibility of FAITID could be found on Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID) website.

1.4.3 Specification Change Procedures

This DPS will be periodically reviewed by FAITID and updated from time to time.

1.4.4 Specification Administration Organization

Changes to the DPS are drafted, reviewed and approved by FAITID management. Application of the DPS is the responsibility of the assigned persons within FAITID.

Any change to the DPS needs to be approved by a management representative of Registry Operations, a Senior Manager and the Information Security Officer of FAITID.

The point of contact for this organization could be found on Foundation for Assistance for Internet Technologies and Infrastructure Development (FAITID) website.

The mechanism to communicate changes in the DPS will be decided on a case by case basis, considering the impact on the stakeholder community and the nature of the changes themselves.

2 Publication and Repositories

2.1 Repositories

DNSSEC-relevant information will be published on the website of FAITID.

2.2 Publication of Public Keys

FAITID will publish its Key Signing Keys in two formats.

Trust Anchor Format: This format can be directly included into a DNS resolver as a trust-anchor. It is equal to the specification of the DNSKEY resource record.

Delegation Signer (DS) Format: In this format, the public key is presented in a hash representation according to the DS Resource Record specification directly in the root zone.

2.2.1 Access Controls on Repositories

All keys are available with PGP signatures generated with the current FAITID key. Validation of PGP signature of the trust-anchor files is recommended. The PGP key will be signed by FAITID as the responsible party; signatories will be senior personnel for easy validation.

3 Operational Requirements

3.1 Registration of delegation signer (DS) resource records

The Registrar is responsible for collecting the required DNSSEC data from the Registrant, to be used in the parent zone by the Registry.

FAITID is responsible for the correct, timely generation of signed DNS data and for distributing it to DNS service providers for its zones.

3.2 Method to prove possession of private key

The Registrant is entirely and solely responsible for the correctness of the submitted key material.

3.3 Removal of DS resource records

The Registrar is responsible for receiving and processing the request to remove DS resource records from the Registrant. This information is then transmitted to FAITID for execution.

Removed DS records are removed from the active Registry database.

3.3.1 Who can request removal

The Registrant may contact the Registrar and request removal of the DS resource records via the regular channels set forth by the Registrar for this purpose.

3.3.2 Emergency removal request

Invalid DS keys may be removed from the DNS or the Registry database by FAITID.

All changes to the Registry information happen in near real time, so the process for Emergency requests is the same as for regular requests.

4 Facility, Management, and Operational Controls

4.1 Physical controls

4.1.1 Site location and construction

FAITID operates multiple sites in the Russian Federation. These include server-rooms in the FAITID office as well as secured cabinets in data centers for hot and backup operations. The operations described here will make use of all of those facilities for housing and running the specialized hardware and software as well as for supporting the management processes.

4.1.2 Physical access

As per FAITID Security Policy, all the facilities providing DNSSEC-related services have restricted access, limited to authorized personnel of FAITID or its contractors. Specific measures depend on the facility and the level of access required, and may include smartcards, biometrics, and other methods for access control by FAITID, its contractors or third-party data center operators.

4.1.3 Power and air conditioning

All facilities have Uninterruptible Power Supply (UPS) capabilities and air conditioning. The external data center sites have redundant systems in place in the event of a power failure.

4.1.4 Water exposures

To avoid the risk of water exposure, all FAITID facilities are on elevated floors. Data bearing facilities require evidence of proper water controls along with other environmental controls discussed in this document.

4.1.5 Fire prevention and protection

All facilities have fire detectors and gas extinguishers.

4.1.6 Media storage

Specific measures depend on the security classification of data involved, but all sensitive media is stored in a safe which is only accessible by FAITID Senior Management and specifically designated contractor personnel.

4.1.7 Media & Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information is rendered unreadable before disposal.

4.1.8 Off-site backup

System software Key Management Systems (which is a software equivalent of HSM , abbreviated as "KMS" from here on), and applications configuration are backed-up to storage systems spread across multiple data centers. Off-site backup media are stored protected from unauthorized access in a physically secure manner at remote location.

4.2 Procedural controls

4.2.1 Trusted roles

Activation data needed to make use of the private keys inside the KMSs is controlled by multiple key FAITID individuals.

4.2.2 Number of persons required per task

One key person must be authorized in the KMS in order to perform any signing operation.

Change of keys require the use of an additional *admin* person that enables these operations.

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Engineers taking part in the Trusted Roles have to have been working for the company for no less than one year and must have the qualifications necessary for the role they have been appointed to.

Managers taking part in the Trusted Roles need to have been working for the company for no less than a year.

4.3.2 Training requirements

Before an individual is authorized to use KMS, he or she must observe one regular key roll over process. There can be any reasonable number of observers for any given regular key roll over process.

4.3.3 Contracting personnel requirements

No person outside of the specified Trusted Roles can get access to the signer systems. If necessary, a team can perform certain tasks with the guidance of an external contractor. At no time is the contractor allowed to be the person performing the tasks on the system.

4.3.4 Documentation supplied to personnel

The regular procedures for backup and restore are available to all personnel involved. If major alterations to those procedures are made, the engineers of those teams will be informed accordingly.

4.4 Audit logging procedures

4.4.1 Types of events recorded

Physical access to the facilities used for our signing systems is logged automatically

on enter and exit. The main operation site requires personnel to be specifically granted permission to enter the suite in which the equipment is located and they will have to sign-in using a valid identification (passport, drivers license, etc.).

Log messages from the signer systems will be sent securely to a logging system and recorded for audit purposes.

4.4.2 Protection of audit log

Audit logs of our main operation site are kept by an external data center operator. These logs are not available to any of our employees and cannot be modified at the request of any of our employees.

4.5 Compromise and disaster recovery

Any relevant events relating to the secure operation of our systems will be announced through the appropriate channels at the time. FAITID and its contractors will invoke the relevant plans, including operations as described above and communications, in accordance with industry best practice.

4.5.1 Incident and compromise handling procedures

If an event leads to, or could lead to, a detected security compromise, we will perform an investigation to determine the nature of the incident. If we suspect the incident has compromised the private component of an active key, an emergency key roll-over procedure will be performed.

4.5.2 Entity private key compromise procedures

Upon the suspected or known compromise of a key, we will assess the situation, develop an action plan and implement the action plan with approval from the Information Security Officer and Senior Management. When we perform an emergency roll-over for a compromised KSK, we will continue to operate this key for at least the minimum time specified to retrieve our public key trust anchors.

5 Technical Security Controls

5.1 Key Pair Generation and Installation

5.1.1 Key Pair Generation

Both the Key Signing Key (KSK) and Zone Signing Key (ZSK) are generated via KMS in the signer systems. Parameters such as key length and cryptographic algorithm are set in accordance with Best Current Practice in similar systems, and will be updated from time to time as appropriate.

5.1.2 Public Key Delivery

The public key is retrieved from the signer system and then published as detailed in the section Publication and Repositories on page 6.

5.1.3 Key Usage Purposes

A key must only be used for one zone and cannot be reused.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

5.2.1 Cryptographic Module Standards and Controls

FAITID employs KMSs with the following features:

- Strong authentication of administrators and dual controls through the use of advanced quorum techniques to mitigate the threat of single "super users".
- Advanced separation of duties of key management activities between DNS, IT and security administrators to facilitate regulatory compliance.
- Centralized key management to support multiple DNS servers.

5.2.2 Private Key Backup

For purposes of disaster recovery in which all KMSs at all sites fail, material needed to reconstitute an uninitialized KMS is backed up. All private key backups are encrypted with an internal KMS key, which is backed up separately at KMS initialization time.

For both the KSK and the ZSK, these backups are kept at a secure off-site facility.

Access to the backups in any form requires authorization from Senior Management.

5.2.3 Method of Activating Private Key

Activation data needed to make use of the private keys inside the KMSs is controlled by multiple corporate officers and operations staff.

Guidelines on initialization are based on instructions for the KMSs and best practices used in support of DNSSEC elsewhere, including the root zone.

Key activation requires the authentication of administrators and dual controls through the use of advanced quorum techniques.

5.2.4 Private Key Transfer Into or From a Cryptographic Module

Private keys can only be transferred off the system in encrypted form and restored onto the back-up system by the teams described in the Trusted Roles section, as explained in the Key Backup section above.

5.2.5 Method of Deactivating Private Key

FAITID uses The KMS's provided functionality for the secure destruction of all key material.

The Private ZSK is stored in the online part of the KMS. It is in the active state as long as it is keeps the status "Active". Change of the ZSK status can be performed by the Domain Zone Administrator from the KMS management interface.

5.2.6 Method of Destroying Private Key

Access to the private KSK is automatically terminated immediately after the

competition of the signing procedure.

5.3 Other Aspects of Key Pair Management

FAITID will only publish the public keys currently relevant to the operation of its zones. No archive of public keys past their revocation is available.

Past or revoked key pairs are destroyed and not archived.

5.4 Computer Security Controls

FAITID ensures that the systems maintaining key software and data files are secure from unauthorized access. In addition, FAITID limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers. All this follows the current Security Policy.

5.5 Network Security Controls

Systems holding the signing infrastructure are inside a dedicated VLAN inside our network infrastructure. The only communications channel to those systems is through firewalls, which are limited to the minimal capabilities necessary for the operation of the system.

5.6 Timestamping

The signer systems securely synchronize their system clocks with a trusted time sources inside and outside our network.

5.7 Life Cycle Technical Controls

5.7.1 System Development Controls

As explained above, the signer systems employ DNS servers interfacing with KMSs that provide secure storage and processing involving private key material.

Only production-ready versions of DNS servers as well as the KMSs are used for FAITID, after thorough testing in our OT&E platform.

6 Zone Signing

6.1 Key Lengths, Key Types, and Algorithms

FAITID utilizes key lengths, types and algorithms considered as best practices at the time.

Currently, the DNSSEC system for FAITID TLDs will use 2048-bit RSA KSKs and 1024-bit RSA ZSKs. The signature algorithm will be RSA-encrypted SHA-256 hashes as per [RFC-4509] or it's most current successor.

6.2 Authenticated Denial of Existence

FAITID uses NSEC [RFC-4034] or it's most current successor to authenticate denial of existence of resource records.

6.3 Signature Format
The signatures will be RSA encrypted with SHA-256 hashes.

6.4 Key rollover
ZSKs are rolled over quarterly, with each ZSK cycle lasting ninety (90) days plus rollover time. They are published ten (10) days before use and remain published ten (10) days after the new key is in use for signing, to account for cached entries in the DNS and to facilitate rollover.

KSKs are rolled approximately every two to five years as appropriate, such as when there is a change in Best Common Practice for signature algorithms or parameters or the current key is believed to be compromised, KMS upgrade or replacement, or to exercise rollover mechanisms. New KSKs are propagated into the root as part of the regular KSK exchanges with ICANN.

A new KSK is published in the zone 60 days prior to use and remains published 20 days after it is no longer used to sign.

6.5 Signature Lifetime and Re-Signing Frequency
The RRSIG resource record in all zones under FAITID management has a lifetime of 30 days. Re-signing frequency is chosen to be half an hour.

6.6 Verification of Resource Records
FAITID operates monitoring systems that check DNSSEC signature validity. Alarms are raised when anomalies are detected.

6.7 Resource Records Time-to-Live
DNSKEY TTL is equal to the TTL used for the SOA record.

NSEC TTL is equal to the TTL used for the SOA record.

RRSIG TTL is equal to the lowest TTL of the record set type covered.

7 Compliance Audit

7.1 Frequency of Entity Compliance Audit
Every five years after the complete implementation of this DPS, a Compliance Audit may be performed to verify that practices remain compliant with the contents and intent of the DPS.

7.2 Identity and Qualifications of Auditor
The Compliance Audit will be performed by an independent entity with qualifications and experience with DNSSEC operations.

7.3 Auditor's Relationship to Audited Party
The selected auditor must not have commercial ties to FAITID or any of its related companies.

7.4 Topics Covered by Audit
The scope of the audit will focus on compliance with the DPS and its alignment with current industry best practices.

7.5 Actions Taken as a Result of Deficiency
Deficiencies or gaps in compliance with the DPS or deviations from the current industry best practices are to be collected in a findings reports that will be delivered to FAITID management team, who will assess and prioritize any findings and respond promptly with an action plan to bring the identified issues to resolution.

7.6 Communication of Results
The communication of the findings and action plans will be decided on a case by case basis by the respective management teams, considering safeguarding the stability of the DNS as well as best interests of all stakeholders.

8 Legal Matters

8.1 Fees
No fees are charged for any function related to DNSSEC.

8.2 Financial Responsibility
FAITID and its agents accept no financial responsibility for improper use of Trust Anchors or signatures or any other improper use under this DPS.

8.3 Term and Termination
This DPS applies until further notice. This DPS may be amended from time to time and it is in force until it is replaced by a new version.

8.4 Limitations of Liability
FAITID and its agents shall not be liable for any financial loss, or loss arising from incidental damage or impairment, resulting from its performance of its obligations hereunder. No other liability, implicit or explicit, is accepted.

8.5 Dispute Resolution Provisions
Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

8.6 Governing Law
This DPS shall be governed by the laws and applicable regulations of the Russian Federation.