TRAFICOM
Finnish Transport and Communications Agency

.fi DNSSEC Practice Statement (DPS)

Document type: Documentation
Creation date: 2.8.2021
Updated: -

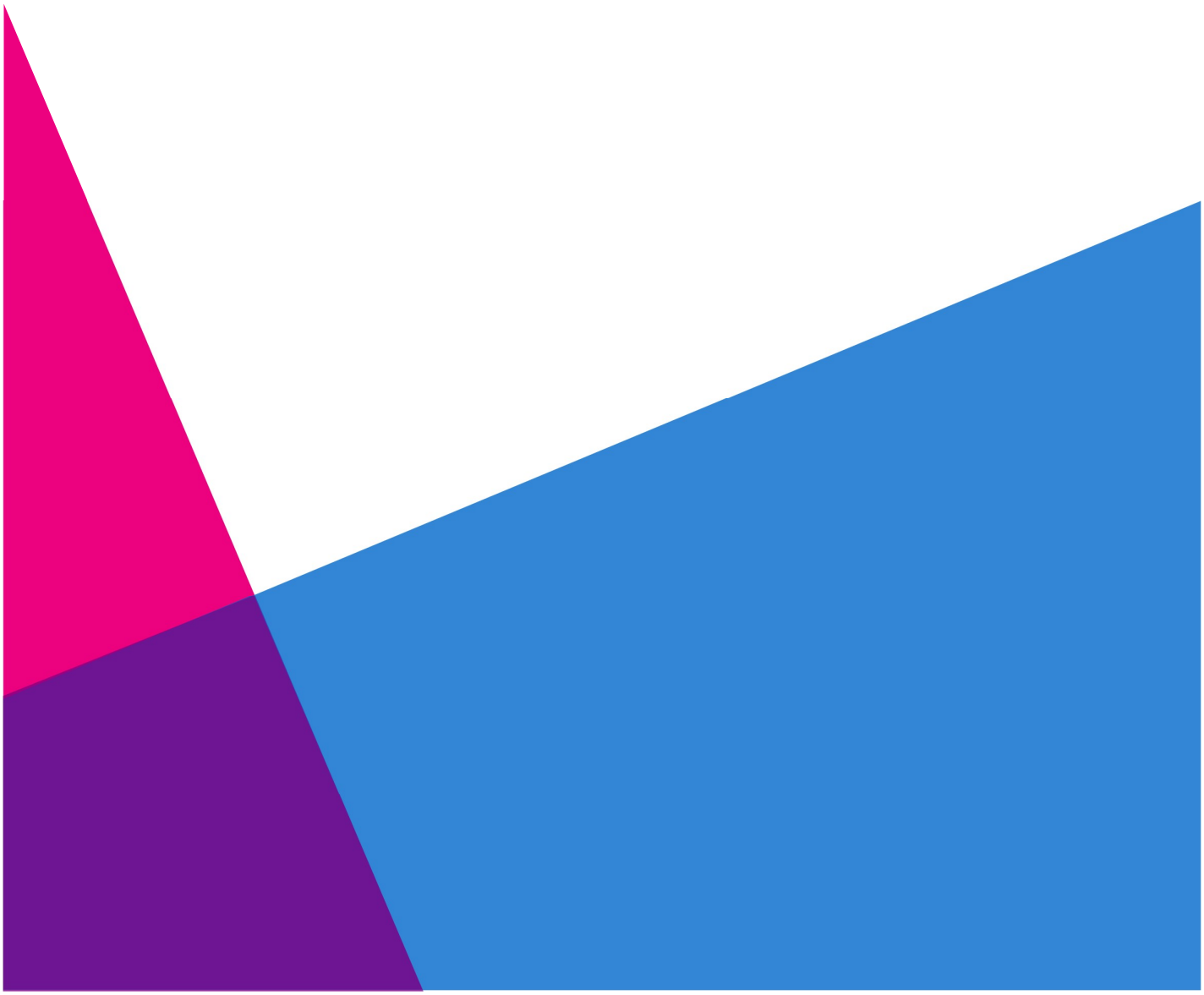

Table of Contents

1 Introduction

This document is Traficom's statement of security practices and provisions that are applied related to the operation of DNS Security Extensions (DNSSEC) for the .fi top-level domain administered by Traficom.

This document conforms mostly to RFC 6841: A Framework for DNSSEC Policies and DNSSEC Practice Statements (DPS).

1.1 Overview

The Domain Name System Security Extensions (DNSSEC) is a set of IETF specifications for adding origin authentication and data integrity to the Domain Name System (DNS). DNSSEC provides a way for software to validate that DNS-data has not been tampered with or modified during transit. This is done by incorporating digital signatures and public key encryption into the DNS hierarchy. The trust follows the same distribution as the DNS tree, meaning that the chain of trust originates from the root zone, delegated in the same manner as the responsibility for a zone.

1.2 Document name and identification

.fi DNSSEC Practice Statement (DPS)

1.3 Target group and applicability

The following parties, to which this document has applicability, have been identified.

1.3.1 Registry

Traficom is responsible for the administration and technical operation of the .fi top-level domains and consequently the registration of domain names that identify underlying zones. This also implies that Traficom manages supplements, changes and removal of all data that is associated with a domain name.

Traficom is responsible for:

- generating the cryptographic key material used in DNSSEC
- protecting the confidentiality of the private component of the key pairs
- securely signing all authoritative DNS resource records in the applicable zone using DNSSEC with the designated keys.

Finally, Traficom is responsible for the secure export, registration and maintenance of DS resource records in the root zone, which establishes the chain of trust from the root zone to the applicable zone and enables validation of DNS records using the key for the root zone.

1.3.2 Registrars

A Registrar is the party that is responsible for the administration and management of a domain name on behalf of the Registrant. The Registrar handles the registration, maintenance and management of the Registrants domain name and is a partner to Traficom. The Registrar is responsible for securely identifying the Registrant of a domain and for adding, removing or updating the specified DS records for each domain at the request of the domain's Registrant.

1.3.3 Registrants

A Registrant is the physical person or legal entity that has registered and holds a domain name. Registrants are responsible for generating and protecting their own DNSSEC keys, for signing the relevant data and for registering and maintaining corresponding DS records through a Registrar.

It is also the Registrants responsibility to perform key rollovers when keys are suspected of having been compromised or lost.

1.3.4 Relying party

The relying party is the entity that relies on DNSSEC signatures, such as validating resolver operators and parties offering other corresponding applications. The relying party is responsible for the configuration and maintenance of the appropriate Trust Anchors.

1.3.5 Applicability

Each Registrant is responsible for determining an appropriate level of security for their domain. This DPS applies exclusively to the .fi top-level domain administered by Traficom, and describes the procedures, security controls and practices employed in the management of DNSSEC in the applicable zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC for the applicable zone and based on this and other circumstances assess their own risk.

1.4 Specification administration

This DPS is updated as appropriate, such as in the event of significant modifications in systems or procedures that have significant effect on the content of this document.

Responsible for the specification administration of the DPS is Traficom's Chief Information Security Officer. The outermost responsibility for the approval and publishing lies with the Fi-domain name team within Traficom.

1.4.1 Specification administration organization.

Finnish Transport and Communications Agency Traficom

1.4.2 Contact information

Finnish Transport and Communications Agency Traficom

fi-domain-tech@traficom.fi

1.4.3 Specification change procedures

Changes to this DPS are either made in the form of amendments or with the publication of a new version of the document. This DPS and any amendments to it are published at:

https://www.traficom.fi/

Only the most recent version of this DPS is effective. Traficom reserves the right to amend this DPS without notification for amendments that are not designated as significant from a security point of view. Traficom will provide notice in case of significant revisions via the above web page.

2 Publication of keys

2.1 Publication of key signing keys (KSK)

.fi root uses as split-key signing scheme (refer to section 6.1) and publishes the relevant Key Signing Keys (KSKs) for the applicable zones as follows:

Directly in the root zone (only DS)

.fi root uses the tools for secure electronic updating of data in the root zone.

3 Operational requirements

3.1 Meaning of domain names

A domain name is a unique identifier, often associated with services such as web sites or e-mail. Applying for registration under the applicable top-level domains is open to all private individuals and legal entities with a civil or corporate registration number, or who can be identified through the registry of a public authority, or an organization with a designation similar to that of a public authority. Foreign applicants may use other methods of unique identification.

The "first come, first serve" approach applies to the registration of new domain names under applicable top-level domains, meaning that domain names are allocated in the order in which applications are received by Traficom's registry services. Terms and conditions for registering domains for .fi are published at:

- https://finlex.fi/en/laki/kaannokset/2014/en20140917.pdf
- https://www.finlex.fi/fi/viranomaiset/normi/480001/42590
-

3.2 Identification and authentication of child zone manager

It is the responsibility of the Registrar to securely identify and authenticate the Registrant through a suitable mechanism, as stipulated in national regulations by Traficom.

3.3 Registration of delegation signer (DS) records

DNSSEC is activated by publishing at least one DS record for the child zone in the applicable top-level domain. Publishing the DS records establishes the chain of trust to the child zones referred keys. The Registry presumes that any syntactically correct DS record is valid and will not perform any additional checking, such as making sure that the specified keys are part of the child zones keyset.

The Registry accepts DS records from the Registrars through the EPP interface, in the format specified in RFC 5910 (Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP). Up to six (6) DS records per domain name may be registered.

3.4 Method to prove possession of private key

Traficom does not conduct any checks with the aim of validating the Registrant as the holder of a certain private key. The Registrar is responsible for conducting both the checks that are required and those that the Registrar furthermore considers necessary.

3.5 Removal of DS resource records

A DS record is removed by sending an EPP command from the Registrar to the Registry, or via Registrar web interface. The removal of all DS records will deactivate the DNSSEC security mechanisms for the child zone in question.

3.5.1 Removal request

The registrant has the authority to request removal of DS records. If the registrar serves as the name server provider for the registrant's domain name, the registrar has the right to, without the request of the registrant, remove these DS records. Traficom retains the right to remove DS records, if Traficom is of the view that they cause, or may cause, serious operational disruption. In cases where the name server operator publishes the necessary information for DNSSEC, Traficom may remove DS records for these domain names.

3.5.2 Procedure for removal request

The registrant or a representative designated by the registrant appoints the registrar to perform the task of carrying out the removal. A registrar that is not the name server operator of these domains may only do this on behalf of the registrant. When a removal command is received by Traficom via EPP or via Registrar web interface, it will be removed by the next zone generation.

In cases where the registrar is the name server operator for the registrant's domain(s) the registrar has the right to, without a request from the registrant, add, remove or change DS records for these domains. Under normal circumstances, the zone is updated every hour. Subsequently, taking time-to-live (TTLs) and distribution time into account, the whole procedure of distributing new delegation information may take longer to complete, before being fully deployed. Registrants will have to account for this timing when calculating their signing scheme and when performing key rollovers.

3.5.3 Emergency removal request

If a Registrant finds himself in a situation where it is impossible to perform the removal request through its current Registrar, Traficom urges the Registrant to change Registrar and are thereby sending an authorization code which can be used for such change.

Traficom has the right to change, remove or reject the publishing of DS records if, and only if, they cause or might cause severe operational damages or disturbances to the applicable top-level domain administered by Traficom

4 Facility management and administrative controls

4.1 Physical controls

Based on continuous risk analysis and re-evaluation of threats, physical perimeter protection, monitoring and access controls, as well as appropriate compensating controls, are implemented to ensure that the registry and signer systems are not tampered with, stolen or sabotaged.

4.1.1 Site location and construction

.fi root servers reside in two fully operational redundant and geographically dispersed facilities, more than 5 kilometers apart. All DNS data is continuously updated through automatic replication between the facilities.

Both operations facilities implement comparable physical security controls in a multi-tiered structure, where the innermost tier is strictly controlled and monitored.

4.1.2 Physical access

All critical components are available at both operational facilities. Entry is logged, and the premises are continuously monitored.

4.1.3 Power supply and environment

The operational facilities provide a controlled, regulated and monitored operating environment. Each facility has redundant power with underground transmission from separate transformer stations. In addition, the facilities provide backup power from generators, capable of powering the facility for at least 24 hours.

4.1.4 Water exposures

The facilities are provided with detection mechanisms and protection for flooding.

4.1.5 Fire prevention and protection

The facilities are equipped with fire detection and automatic fire suppression mechanisms based on dry extinguishing agents. The facilities are provided with raised floor and each room in the facility constitutes an independent fire cell.

4.1.6 Media storage management

Traficom has implemented and enforces an information classification system, which defines the requirements imposed for storage of sensitive information. Storage devices carrying such information are stored in spaces with physical protection to the same level as the data centers.

4.1.7 Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, either by Traficom or by a contracted party. This applies where appropriate for HSM’s as well.

4.1.8 Off-site backup

Certain critical data is also securely stored off-site. Off-site back-ups are stored in encrypted form, and access to encryption keys is limited to persons with SA role.

The storage facility is geographically separated from other operational facilities. The storage facility has at a minimum the same level of physical protection as the operational facilities.

4.2 Procedural controls

4.2.1 Trusted roles

Trusted roles are held by individuals that are involved in the generation and use of private key material as well as the delivery and publication of the public key material of the applicable zones. The trusted roles are:

1.Systems Administrator, SA

2.Security Officer, SO

At any given time, there must be at minimum two individuals appointed per trusted role. A single individual may not hold more than one trusted role at a time.

4.2.2 Number of persons required per task

Separation of duties and roles are enforced for critical operations. These tasks require one individual from each role to participate in the process.

4.2.3 Identification and authorization for each role

Only people who have signed a non-disclosure agreement, and an agreement to acknowledge their responsibilities with Traficom may hold a trusted role.

4.2.4 Tasks requiring separation of duties

All critical HSM (Hardware Security Module) operations are required to be performed on-location, in one of the operational facilities. Duties are segregated by the Security Officer not having exclusive physical access to the operational facilities, while the System Administrator are not allowed access to the information required to activate the HSM. Furthermore, the responsibility for export and publishing of the public key components of the KSK is distributed in such a way that only the SO has authority to register the key material, while only the SA has the authority to initiate key generation (see Section 5.1.2

Critical operations therefore include activation of the HSM, key administration and export and publishing the public component of the KSK.

The operations may be carried out only in the presence of authorized individuals.

4.3 Audit logging procedures

Logging is automatic and involves the continuous collection of audit information related to the activities in the registry system. This log information is used in the monitoring of operations, for statistical purposes and for root-cause analysis in the event of a suspected security compromise or incident.

4.3.1 Types of events recorded

The following events are included in automatic logging:

- all types of operations involving an HSM, such as key generation, key activation, signing and exporting of keys
- attempts for remote access, successful and unsuccessful
- privileged operations
- entrance into a facility.

4.3.2 Frequency of processing log

Logs are analyzed through automated and manual processes.

4.3.3 Retention period for audit log information

Log information is stored on-line in log collecting systems for a minimum of five years.

4.3.4 Protection of audit log

The logging systems are protected against unauthorized viewing, manipulation and destruction of log data. Audit information relating to the physical access control system is stored outside of the control of the SA role.

4.3.5 Audit log backup procedures

The logs are backed up as part of normal system backups. The log collecting system consist of separate units, where no backups are taken.

4.3.6 Audit log collection system

Electronic log information is transferred in real-time to the collection system.

4.3.7 Vulnerability assessments

All anomalies discovered in the audit log information are investigated and analyzed for potential vulnerabilities.

Traficom is also a member of several organizations and communities where security-related information is collected, analyzed and confidently shared among the stakeholders. This information is continuously evaluated for new threats.

4.4 Compromise and disaster recovery

4.4.1 Incident handling procedures

Any actual or perceived event of security-critical nature that has led to or could have led to a security compromise is defined as an incident. All incidents are managed in accordance with Traficom's incident handling procedures. The incident handling procedures includes conducting a root-cause analysis, to formally identify the nature and impact of the event, in order to identify what measures are required to prevent the event from reoccurring (or to limit its consequences). The procedures also provide means of escalation and reporting of incidents to the appropriate authority within Traficom. An incident which involves the suspicion of a private key compromise, leads to the immediate rollover of keys in accordance with the procedures indicated in section 4.5.3

4.4.2 Corrupted computing resources, software, and/or data

In the event corruption of information systems or resources is detected, the incident handling procedures shall be initiated, and appropriate measures be taken. If required, the disaster recovery procedures are also enacted.

4.4.3 Entity private key compromise procedures

If the confidentiality of a private key is suspected to have been compromised, or if the key may have been misused, the following key rollover procedures will be initiated:

If a zone signing key (ZSK) is suspected of having been compromised, Traficom will immediately stop using that key. If necessary, a new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or safely been discarded from the resolvers, whichever occurs first. If a ZSK is suspected of having been completely compromised and revealed to unauthorized parties, this will be notified through the appropriate channel.

If a key signing key (KSK) is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign the key set until it can be considered sufficiently safe to remove the key, considering the risk for disruptions in relation to the risk presented by the compromised key. A KSK rollover is always announced through the appropriate channels.

If the KSKs (and possibly also the ZSKs) are lost completely, new keys will be generated at the earliest convenient occasion and included in the key set. In the meantime, it may occur that the applicable zones will be unsigned until all the systems are recovered, and new DS records have been published in the root zone. During this time all the scheduled ZSK rollovers will be postponed.

4.4.4 Crisis management and Business continuity

Traficom has prepared a contingency plan ensuring that mission-critical operations can be relocated between the operational facilities within four hours. Spare components for critical hardware are available, if needed. The contingency plan also includes capability to resume other mission-critical services and systems at any of the alternative locations. The plans are regularly tested, and the results are recorded and subsequently evaluated.

The contingency plan includes:

roles and responsibilities in the activation of crisis management procedures

how and where the crisis management shall convene

activation of backup IT operations

appointment of a Task Manager

criteria and procedures for resuming normal operations.

4.5 Discontinuation of DNSSEC

If Traficom must discontinue DNSSEC for the applicable zones for any reason, and go to an unsigned zone, this will take place in an orderly manner with public notification.

4.6 Transfer of operational responsibility

If the operation of the applicable zone is transferred to another party, Traficom will assist in the transition to make it as smooth as possible

5 Technical security controls

5.1 Key pair generation and installation

5.1.1 Key pair generation

All keys required for the continued operation of the applicable zone (in the foreseeable future) are pre-generated in advance through a formal key ceremony. The generation of the key material includes KSKs, ZSKs and all internal keys used for access control, key distribution and backup.

During the initial key ceremony, the HSM master keys are first generated. After they have been safely and securely installed in each device designated for production, the application keys (KSKs and ZSKs) are generated and securely distributed using the master key.

When new keys are required to be generated, this will take place through a scheduled key ceremony on-location at one of the operational facilities. Keys will be generated and backed-up to the backup-module (refer to section 5.2.4).

Key generation and distribution require at the minimum one SA and one SO working in unison throughout the whole process.

5.1.2 Public key delivery

The public component of a KSK is exported from the signing system as part of the key ceremony. After exporting it is verified by both SO and SA.

5.1.3 Public key parameters generation and quality checking

The usage of a validated hardware devices, HSM's (refer to section 5.2.1), provides reasonable assurance that the key generation is being performed in a secure manner with respect to among other things pseudo-random number generation and quality checking of key parameters, such as exponent size and primality testing.

5.1.4 Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside of the signing system. The signing system and HSMs are not used for any other purpose than DNSSEC.

A signature made by a DNSSEC key has a maximum validity period of 14 days for both the ZSK and KSK, with an inception time of two hours from the time when the signatures are produced.

5.2 Private Key protection and Cryptographic Module Engineering controls

All cryptographic operations involving the KSKs and ZSKs are performed in the protected memory of an HSM. No private keys are ever stored unprotected outside the HSMs.

5.2.1 Cryptographic module standards and controls

The signing system uses hardware security modules (HSMs) and backup modules validated at FIPS 140-2 level 3.

5.2.2 Private key (m-of-n) multi-person control

Traficom does not enforce multi-person control for private key operations. Refer to section 4.2.4 for compensating controls through separation of duties in the HSM activation process.

5.2.3 Private key escrow

.fi root private keys are not escrowed.

5.2.4 Private key backup

During the key ceremony, the pre-generated application keys are copied to a separate backup-module with characteristics similar to the HSM itself. The backup module is stored separately in safe accessible by the SO.

5.2.5 Private key storage on cryptographic module

Private keys, while stored in persistent memory in the HSM, are always stored in encrypted form using a key which resides in a tamper-proof and secure memory area of the HSM

5.2.6 Private key archival

Private keys that are no longer used are not archived.

5.2.7 Private key transfer into or from a cryptographic security module

During the initial key ceremony, an HSM master key is generated and distributed to the designated devices set up for production. The distribution is performed physically using a separate set of hardware token devices with necessary activation keys. After this key distribution has been completed, the tokens are stored in a safe accessible only by the SO.

5.2.8 Method of activating private key

To activate the HSM and its private keys a SA is giving a SO access to the equipment. The HSM and its private keys are activated by the SO demonstrating possession of the activation data. This data is stored by the SO.

5.2.9 Method of deactivating private key

No automatic procedure of deactivation is implemented.

5.2.10 Method of destroying private key

No efforts are made to destroy private keys after their operational period has expired and they have become invalid.

5.3 Other aspects of key management

5.3.1 Public key archival

Public keys are not archived after expiration.

Key usage period

After the operational period of a key has elapsed and the key is superseded, the key enters the expired state and becomes invalid. Keys in the expired state will not be reused and are removed as part of the standard operating procedures for maintaining the signer system.

5.4 Computer security controls

In systems related to .fi root, a role-based authorization and authentication system is in use, which enables discretionary access controls and reporting of assigned authorizations. Logging is being done at a level which enables individual accountability for all (privileged) operations in each subsystem.

All mission-critical systems are also continuously monitored for events relevant to the stability and security of the system.

5.5 Network security controls

Network infrastructure utilized in .fi root production is logically divided into various security zones. Firewalls are used for managing the communication between the different network segments and to critical components of the registry system. All information which may be of sensitive nature, and is being transferred over the communications network, is always protected using strong encryption mechanisms.

5.6 Timestamping

.fi root DNS system uses Finnish official time and other highly accurate and high-availability time sources.

5.7 Life cycle technical controls

5.7.1 Security management controls

Any parties participating in .fi root DNSSEC administration are required to comply to requirements stated in Traficom’s Information Security Policy.

5.7.2 Change management security controls

Traficom is using work models that includes selected parts from adequate standards like ISO/IEC 27001 and parts from modern work models for continuous integration and continuous delivery in order to manage and control changes in the IT environment

6 Zone signing

6.1 Key lengths, key types and algorithms

.fi root uses a split-key signing scheme in signing of the applicable zone. The splitting is made through key signing key (KSK) and zone signing key (ZSK). Key lengths and algorithms for each key shall be of sufficient strength for their designated purpose and operational period. Only IETF standardized algorithms shall be used by the applicable top-level domain.

For the .fi top level domain the RSA algorithm with a modulus size (key length) of 2048 bits for both KSK and ZSK.

6.2 Authenticated denial of existence

NSEC is used to provide authenticated denial of existence, as specified in RFC 4034.

6.3 Signature format

6.3.1 Signature format: .fi top level domain

Signatures are generated by encrypting SHA256 hashes (RSA/SHA256as specified in RFC 6594).

6.4 Key roll-over

ZSK rollover is carried out every 3 months via an automated procedure.

KSK rollover is carried out every 12 months, requiring also manual steps.

Either or both keys can also be manually roller-over in case of eg. suspected security breach.

6.5 Signature lifetime and re-signing frequency

Resource Records (RR Sets) are signed with a validity period of 14 days (randomized on 12 hours window). Signatures which expire within 10 days will be refreshed hour-by-hour.

6.6 Verification of resource records

To ensure valid signatures and integrity of the DNSKEY record, a set of checks are automatically run at each signing occasion. These controls include verification of signatures using the Delegation Signer (DS) records registered with IANA for the Root Zone, as well as verification of time and date. Zone information which does not pass the automatic checks will put the production of a new zone file on hold and become flagged for manual intervention and troubleshooting. The production of a new zone file is on hold until the troubleshooting and error-handling is completed. Furthermore, verification of the validity of all resource records are made in accordance with the current standards prior to distribution.

6.7 Resource records time-to-live

The time-to-live (TTL) for each DNSSEC Resource Record (RFC 4034) is specified as follows, in seconds:

Resource records time-to-live	
RR type	TTL
DNSKEY	900
DS	21600
NSEC/NSEC3	as SOA minimum (86400)
RRSIG	same as TTL for RR (varies)

Finnish Transport and Communications Agency
Traficom

P.O.Box 320 FI-00059 TRAFICOM, Finland
Tel. +358 295 345 000

traficom.fi

TRAFICOM
Finnish Transport and Communications Agency