MAY 28, 2016

NOMINET

DNSSEC PRACTICE STATEMENT FOR TOP-LEVEL DOMAINS

ABSTRACT

THIS DOCUMENT IS A STATEMENT OF SECURITY PRACTICES AND PROVISIONS WHICH ARE APPLIED TO THE ADMINISTRATION AND OPERATION OF DNS SECURITY EXTENSIONS (DNSSEC) IN THE TLD.

TABLE OF CONTENTS

1. INTRODUCTION

This document is the DNSSEC Practice Statement (DPS) for the TLD zone. It states the practices and provisions that are employed in providing TLD Zone Signing.

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 Domain Name System data have not been modified during transit. This is accomplished by adding digital signatures into the DNS hierarchy to form a chain of trust between the internet root and domain names.

This DPS is specifically applicable to all DNSSEC related operations performed by Nominet for the TLD zone.

1.2. Document name and identification

Document title: Nominet DNSSEC Practice Statement for TLD zones

Version: 1.0

Date: Thu, 26 May 2016

1.3. Community and Applicability

This DPS is applicable to the DNSSEC operations of the Nominet operated TLDs.

1.4. Specification Administration

1.4.1. Specification administration organization

Nominet
Minerva House
Edmund Halley Road
Oxford Science Park
Oxford
OX4 4DQ
United Kingdom

1.4.2. Contact Information

For questions regarding this DPS or the operations of DNSSEC in the TLD:

Telephone:	+44(0)1865 332481 (Lines open 8am - 6pm)
Email:	nominet@nominet.uk

1.4.3. Specification change procedures

Nominet reserves the right to change, amend or revoke this DPS without prior notice. Material changes will be announced on the Nominet website.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

Information relating to the DNSSEC operations of the TLD are published at:
http://registrars.nominet.org.uk/gtlds/gtld-registrar-systems/dnssec

2.2. Publication of key signing keys

A cryptographic hash of the public portion of the TLD KSK will be published in the root zone. This hash will be updated in advance when the associated key is about to be rolled.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

DNSSEC provides mechanisms for adding origin authentication and data integrity to the Domain Name System (DNS). DNSSEC provides a way for software to validate that Domain Name System data have not been modified during transit. It does NOT provide any way of determining the legal entity behind the domain name, nor the relevance of the domain name.

3.2. Activation of DNSSEC for child zone

DNSSEC for a child zone is activated when a DS record is published in the TLD zone.

3.3. Identification and authentication of child zone manager

Nominet does not perform any verification of the identity and authority of the child zone manager as it only applies changes received from Registrars.

3.4. Registration of delegation signer (DS) resource records

Nominet applies changes to the TLD zone file based on requests from Registrars.

3.5. Method to prove possession of private key

Registrars are not required to present proof of possession of private keys.

3.6. Removal of DS resource records

3.6.1. Who can request removal

The removal of DS records can only be requested by the Registrar.

3.6.2. Procedure for removal request

All requests including removals are received, validated and processed automatically.

3.6.3. Emergency removal request

Nominet offers Registrars out of hours emergency support, should any requests fail to process automatically. Contact details can be found at **http://registrars.nominet.org.uk/contact**

4. FACILITY, MANAGEMENT & OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction
Operations centres used for TLD operations, including the DNSSEC key management, have at least 4 tiers of physical security, each tier with progressively more restrictive access policy. The two main operation centres are currently separated by at least 14 miles.

4.1.2. Physical access
Dual-access control is mandated for all personnel to gain entry to the innermost tier.

4.1.3. Power and air conditioning
Each operation centre has air conditioning, UPS based backup power and a diesel generator.

4.1.4. Water exposures
Nominet has taken reasonable precautions to minimize the impact of water exposure to our systems.

4.1.5. Fire prevention and protection
Nominet has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

4.1.6. Media storage
Media containing production software, as well as media containing data, audit, archive, and backup information is stored within the main Nominet facility and in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel. All offsite backups use data at rest encryption.

4.1.7. Waste disposal
All information-carrying media which may contain internal or confidential information are destroyed following a Standard Operating Procedure. This includes hard-drives, flash storage devices, etc.

4.1.8. Off-site backup
Audit information is routinely and regularly replicated between and stored at both operation facilities.

4.2. Procedural Controls

4.2.1. Trusted roles
There are four trusted roles;

(1) System Administrator (SA).
(2) Security Officer (SO).
(3) Auditor (AU).
(4) Safe Keeper (SK).

All roles are tightly bound to the Nominet Hierarchy. The Security Officer (SO) role is performed by a member of the Senior Management Team. The Auditor (AU) role is performed by an employee that is appointed by the Senior Management Team. The Safe keeper is the CEO, or someone delegated by the CEO.

Procedures requiring management of secure key storage require credentials held by the Security Officer. Access to the systems containing private keys require credentials held by the System Administrators. When access to the safe is required, the safe keeper becomes involved.

4.2.2. Identification and authentication for each role
Personnel in trusted roles are prior to the assignment of their credentials (for logical access) identified to another trusted person.

4.2.3. Tasks requiring separation of duties
Physical access to the safe and secure key storage requires one person from each trusted role (SO/SA).

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements
All personnel participating in the operation of DNSSEC systems have demonstrated proficiency in their assigned role and have undergone training.

4.3.2. Background check procedures
New employees will go through appropriate security vetting procedures.

4.3.3. Training requirements
Nominet provides employees and contractors with on-the-job training on the procedures, processes and administration of the DNSSEC system.

4.3.4. Job rotation frequency and sequence
All personnel assigned to trusted roles will be exercised in their roles by rotating all planned operational activities among the trusted persons.

4.3.5. Sanctions for unauthorized actions
In the event that Nominet suspects unauthorized actions by a trusted person, this persons credentials will immediately be suspended awaiting an investigation.

4.3.6. Contracting personnel requirements
All contracted personnel adhere to the same requirements as employees.

4.3.7. Documentation supplied to personnel
All Standard Operating Procedures (SOP's) are documented and supplied to the personnel responsible for executing them.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded
Events to be recorded in the audit log includes, but are not limited to:

- Physical entry into the operations facility,
- Changes in physical and logical authorisations,
- Key management activities.

4.4.2. Frequency of processing log
Events listed before are processed continuously and automatically.

4.4.3. Retention period for audit log information
Audit log information are retained for at least as long as it is needed to fulfil the audit requirements of section 7.

4.4.4. Protection of audit log
Off-line audit log information are physically protected in a secure offsite facility.

4.4.5. Audit log backup procedures
Audit logs are backed up to off-line storage on a weekly basis.

4.4.6. Audit collection system
Audit logs are replicated in real time to at least two physically and logically separate log collection systems. Only authorised system administrators (SA) have access to these systems.

4.4.7. Notification to event-causing subject
Personnel responsible for operations and personnel in trusted roles are informed that event logging is enabled.

4.4.8. Vulnerability assessments
Nominet monitors and evaluates information sources relating to cryptographic and mathematical achievements, security and vulnerability reports from vendors and community groups, and collaborates with other TLD operators in evaluating the domain name system environment. In addition, all systems are monitored on a 24/7 basis for disruptions and unexpected events.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures
If Nominet detects an event that has or could have caused a security compromise of any of the security mechanisms, the incident handling procedures are activated. These procedures includes how incidents are to be investigated, acted upon, reported to the stakeholders and actions to avoid the incident from reoccurring.

4.5.2. Corrupted computing resources, software, and/or data
Where corrupted resources, and/or data causes (or could have caused) a disruption of operations that event will be viewed upon as an incident, and the incident handing procedures will be activated.

4.5.3. Entity private key compromise procedures

4.5.3.1. Key Signing Key compromise
If a KSK is suspected to be compromised, an investigation will commence determining the severity of the event. In the event the confidentiality of the KSK cannot be guaranteed, the KSK roll-over procedure will be enacted. Depending on the severity of the situation, the emergency KSK roll-over procedure may be enacted, which will complete within 96 hours. In other cases, the roll-over procedure will aim to be completed within 5 working days.

4.5.3.2. Key Signing Key loss
If a KSK is lost the standard KSK roll-over procedure will be enacted.

4.5.3.3. Zone Signing Key Compromise
If a ZSK is suspected to be compromised an investigation will commence determining the severity of the event. In the event the confidentiality of the ZSK cannot be guaranteed, the ZSK roll-over procedure will be initiated and completed within 3 working days.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities
Nominet maintains business continuity and disaster recovery capabilities, where normal operations can be moved to the alternative site. Critical administrative functions can be re-established in arbitrary office spaces using remote access technology and internally publsihed procedures.

4.6. Entity termination

In the event the responsibilities of the TLD are transferred to another party, Nominet will co-operate to facilitate a KSK roll-over to the new party.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation
Key generation will occur in pre-planned form using Standard Operating Procedures.

5.1.2. Public key delivery
The hash of the public key will be delivered to IANA using the method mandated whenever it is updated. No other publication of public keys will be made.

5.1.3. Public key parameters generation and quality checking
Key generation is performed on secure hardware according to a standard operating procedure. The standard operating procedure is updated on a yearly basis to ensure the parameters used are still appropiate

5.1.4. Key usage purposes
The keys used for signing the TLD will not be used for any other purpose, or outside of the signer system.

5.2. Private key protection and Hardware Engineering Controls

5.2.1. Hardware standards and controls
Nominet uses secure hardware to generate and protect keys.

5.2.2. Private key (m-of-n) multi-person control
M-of-N multiperson control of private keys are not implemented.

5.2.3. Private key escrow
Private keys are not escrowed.

5.2.4. Private key backup
The key storage files are distributed between the two operations centres using an encrypted connection.

5.2.5. Private key storage
Keys are stored on the secure hardware.

5.2.6. Private key archival
Private keys which have reached the expired state will be deleted/destroyed and are not archived.

5.2.7. Method of activating private key
Private keys are activated automatically using the policy configured by the System Administrator.

5.2.8. Method of deactivating private key
Private keys will be deactivated when the secure hardware is shut down or loses power.

5.2.9. Method of destroying private key
Keys that have entered the expired state will be removed from the secure hardware automatically based on the configured policy.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival
Public keys are not archived after their operational period has expired.

5.3.2. Key usage periods
When a key has been rolled over and superseded with a new key, it enters its expired state. A key moved into the expired state will never be re-used to sign resource records or for any other purpose.

5.4. Activation data

5.4.1. Activation data generation and installation
The key storage hardware is activated by the Systems Administrator, using individual passwords, selected by the System Administrator according to the following complexity requirements:

(1) At least 6 characters,
(2) containing at least 3 alphabetic and 1 nonalphabetic character.

5.4.2. Activation data protection
Activation data is stored in an encrypted format only available to assigned System Administrators.

5.4.3. Other aspects of activation data
The secure key storage hardware implements mechanisms to counter password guessing attacks.

5.5. Computer Security Controls

Nominet uses a standardised server platform for all critical components. Systems are continuously monitored for security and stability issues. Accounts and authorisations are centrally managed.

5.6. Network Security Controls

Nominet's production servers are logically separated into security zones using filtering devices. Filters are configured according to the least-privilege principle allowing only the necessary communication paths to flow over the filtering device. During master key management operations, systems are always disconnected from any communications network.

5.7. Timestamping

All systems synchronises time from a trusted internal source using NTP.

5.8. Life Cycle Technical Controls

5.8.1. System development controls
No software components critical to the operations of the TLD zone are internally developed by Nominet.

5.8.2. Security management controls
Configuration of all systems are centrally managed and revision controlled. The authenticity and integrity of software components are verified using digital signatures before being installed onto the server platform.

5.8.3. Life cycle security controls
Critical software components are either sourced from suppliers using a procurement process, or based on open-source products. For each of these categories of products there is a Quality Assurance (QA) process which includes rigorous testing and continuous follow-up of any stability or security issues uncovered during the products life-cycle.

6. ZONE SIGNING

6.1. Key lengths and algorithms

The TLD KSK key pair(s) is a RSA key pair, with a minimum modulus size of 2048 bits.
The TLD ZSK key pair(s) is a RSA key pair, with a minimum modulus size of 1024 bits.

6.2. Authenticated denial of existence

Authenticated denial of existence will be provided through the use of NSEC3 resource records as specified in [RFC5155].

6.3. Signature format

The KSK signatures will be generated by encrypting SHA-256 hashes using RSA [RFC5702].

6.4. Key roll-over

The ZSK will be rolled over to a new key when considered operationally neccesary. No standby keys are used.
The KSK will be rolled over to a new key when considered operationally neccesary. No standby keys are used, and the roll-over process will not take into account the timings specified in [RFC5011].

6.5. Signature life-time and re-signing frequency

All signatures will have a 35 days validity, with 2 hour inception and no jitter applied to the signature life-time.

6.6. Verification of zone signing key set

Zone signing keys are generated, signed and maintained within the same signer system.

6.7. Verification of resource records

The resource records to be signed are authenticated to be from a trusted source using cryptographic signatures.

6.8. Resource records time-to-live

RRtype	TTL
DNSKEY NSEC3 DS RRSIG	1 Hour 3 Hours 1 Hour as covered RR

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

Internal compliance audits are performed when major changes are undergone and at least every 3 years.

7.2. Identity/qualifications of auditor

The assessor will be proficient in DNS and DNSSEC technology, as well as information security management and auditing practices.

7.3. Auditor's relationship to audited party

Auditors can be selected from internal resources which do not currently hold a part as a trusted person in the DNSSEC operations, or may be sourced as a contractor from an external party.

7.4. Topics covered by audit

Assessments will be made using the current version of the DPS as the basis.

7.5. Actions taken as a result of deficiency

If discrepancies are discovered during audit, these are communicated directly to the management of operations and the security co-ordinator of Nominet, which will determine the severity of the discrepancy and form an action plan for correcting the cause.

7.6. Communication of results

The results of any audits will kept internal to Nominet. No further communication of any auditing reports will be made

8. LEGAL MATTERS

The Registry operates within the jurisdiction of England and Wales.

9. REFERENCES

9.1. Normative References

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <http://www.rfc-editor.org/info/rfc5011>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <http://www.rfc-editor.org/info/rfc5155>.

[RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5702, DOI 10.17487/RFC5702, October 2009, <http://www.rfc-editor.org/info/rfc5702>.

9.2. Informative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements”, RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions”, RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

APPENDIX A. TABLE OF ACRONYMS AND DEFINITIONS

A.1. Acronyms

Term	Definitition
AD	Authenticated Data Flag
BIND	Berkley Internet Name Domain
CC	Common Criteria
CD	Checking Disabled
DNS	Domain Name System
DNSKEY	Domain Name System Key
DNSSEC	Domain Name System Security Extensions
DO	DNSSEC OK
DPS	DNSSEC Practices Statement
DS	Delegation Signer
EAL	Evaluation Assurance Level (pursuant to the Common Criteria)
FIPS	Federal Information Processing Standards
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NS	Name Server
NSEC	NextSecure
NSEC3	Hashed NextSecure
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RFC	Request for Comments
RRSIG	Resource Record Signature
SEP	Secure Entry Point
SHA	Secure Hash Algorithm
SOA	Start of Authority
TA	Trust Anchor
TLD	Top Level Domain
TSIG	Transaction Signature
TTL	Time To Live

A.2. Definitions

Term	Definitition
Chain of Trust	DNS keys, signatures, and delegation signer records that, when validated in a series, can provide proof of authenticity of the last element in the chain using the first element in the chain. Usually, the first element is a trust anchor.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Compliance Audit	A periodic review that an entity undergoes to determine its conformance with standards that apply to it.
Delegation Signer (DS)	Delegation Signer is one of the resource records indicating that the delegated zone is digitally signed. It also assures that the parent zone recognizes the indicated key for the delegated zone. Refer to [RFC4034] for the formal definition.
Key Signing Key (KSK)	A key that signs the key set.
Management Review	Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Parent Zone	The zone that is one level higher in the DNS hierarchy.
Policy Management Authority	The office within NOMINET responsible for promulgating the DPS.
Public Key Infrastructure	The architecture, organization, techniques, Infrastructure practices, and procedures that collectively support the implementation and operation of a public key cryptographic system.
Repository	DNSSEC-related information made accessible online.
Resource Record Signature (RRSIG)	Signature data in a zone. Refer to [RFC4035] for the formal definition.
RSA	A public key cryptographic system invented by Ron Rivest, Adi Shamir, and Leonard Adleman.
Root Zone Management System (RZMS)	A system used to automate the Root Zone update process.
Secret Share	A portion of a private key or a portion of the activation data needed to operate a private key under a Secret Sharing arrangement.
Trust Anchor	A trust anchor is an authoritative entity represented via a public key. A validating security-aware resolver uses this public key as a starting point for building the authentication chain to a signed DNS response. Refer to [RFC4033] for the formal definition of a trust anchor in the context of DNSSEC.
Trusted Role	A role within the DNSSEC operations that must be held by a Trusted Person.
Trusted Person	Personnel assigned to a Trusted Role.
Trusted Status	Trusted Status is achieved by a person who has successfully completed the screening requirements for Trusted Roles set out in this DPS.
Trustworthy system	Computer system in which hardware, software, and System operational procedures provide a reasonable (1) security against intrusion, misuse, unauthorized access, (2) degree of availability, and (3) adherence to accepted security practices.
Zone	A boundary of responsibility for each domain.

APPENDIX B. HISTORY OF CHANGES

Section	Description
Creation of first Edition	N/A

AUTHOR'S ADDRESS

Nominet
Minerva House
Edmund Halley Road
Oxford Science Park
Oxford
OX4 4DQ
United Kingdom


NOMINET