.POST DNSSEC implementation policy

Document history

Date	Comments	Version
1 October 2014	Replaced interim DNSSEC guidelines	1.0
15 March 2018	General updates	1.1
11 May 2021	General updates	1.2

Contacts:

Questions or concerns regarding this document should be sent to
UPU .POST Team:
secretariat (at) info.post
Tel. +41 31 350 3111

Table of contents

1 Introduction

The domain name system (DNS) was not originally designed with strong security mechanisms to provide integrity and authenticity of its data. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system.

The DNS security extension (DNSSEC) (RFC4033, RFC4034, RFC4035) addresses these vulnerabilities by using public key cryptography to add data origin authentication, data integrity verification and authenticated denial-of-existence capabilities to the DNS. In short, the DNSSEC provides a way for software to verify the origin of DNS data and check that it has not been modified in transit or by intermediaries.

To provide a means for stakeholders to evaluate the strength and security of the DNSSEC chain of trust, an entity operating a DNSSEC-enabled zone may publish a DNSSEC policy and practice statement (DPS) describing critical security controls and procedures relevant for scrutinizing the system's trustworthiness. The DPS may also identify any of the DNSSEC policies (DPs) it supports, and explain how it meets their requirements.

The DP and DPS are not primarily aimed at users relying on signed responses from the DNS (relying parties); instead, their audience is other stakeholders of the DNS infrastructure, a group that may include bodies such as regulatory authorities.

Even though this document is heavily inspired by the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647), with large parts being drawn from that document, the properties and structure of the DNSSEC trust model are fundamentally different from those of the X.509 Public Key Infrastructure (PKI) (1).

2 Objectives

To have a reference for DNSSEC implementation for .POST sTLD and for registrants implementing DNSSEC by themselves, in compliance with section 8 of this document.

A DPS defines the policy and practices and summarizes procedures an entity uses to sign and manage a DNS zone.

This document is intended to provide information on how the Universal Postal Union (UPU) will implement and manage the .POST key signing keys (KSKs) and zone signing keys (ZSKs) for the .POST top-level domain.

The information contained in this document is intended to assist stakeholders in determining the level of confidence and trust they wish to confer in the UPU and the .POST top-level domain.

This DPS is based on IETF RFC 6841, *A Framework for DNSSEC Policies and DNSSEC Practice Statements*.

To provide a means for stakeholders to evaluate the strength and security of the DNSSEC chain of trust, an entity operating a DNSSEC-enabled zone may publish a DPS comprising statements describing critical security controls and procedures relevant for scrutinizing the trustworthiness of the system. The DPS may also identify any of the DNSSEC policies (DPs) it supports and explain how it meets their requirements.

The DP and DPS are not primarily aimed at users relying on signed responses from the DNS ("relying parties"); instead, their audience is other stakeholders of the DNS infrastructure, a group that may include bodies such as regulatory authorities.

3 Background

The DNSSEC provides a mechanism to validate DNS data to prove that it has not been modified during transit over the Internet. This is achieved by incorporating public key cryptography into the DNS hierarchy, forming a chain of trust originating at the root zone.

A DNSSEC Policy and Practice Statement (DPS) defines the policy and practices, and summarizes procedures an entity uses to sign and manage a DNS zone.

The UPU's interim DPS is intended to provide information on how the UPU will implement and manage the .POST key signing keys (KSKs) and zone signing keys (ZSKs) for the .POST top-level domain.

The interim DPS is based on IETF RFC 6841, *A Framework for DNSSEC Policies and DNSSEC Practice Statements*.

The implementation is based on the combination of OpenDNSSEC, SoftHSM and NSD software packages developed by NLnet Labs (https://www.nlnetlabs.nl).

4 Overview

The DNS is described in RFC 1034 and RFC 1035.

The DNSSEC is described in RFC 4033, RFC 4034 and RFC 4035 and is a set of specifications that add security to the DNS.

The DNSSEC provides a mechanism to validate DNS data to prove that it has not been modified during transit over the Internet. This is achieved by incorporating public key cryptography into the DNS hierarchy, forming a chain of trust originating at the root zone.

5 Community and applicability

This DPS applies exclusively to the .POST zone. It describes the procedures and security controls applicable when managing and employing keys and signatures for the signing of the .POST zone.

The UPU is responsible for top-level domain .POST direct registrations at the second and third levels, which are permitted in accordance with the .POST DMP published at www.info.post:

Zone	*2LD registry operator*	*Status of zone*
.com.post	Afilias	Restricted to commercial organizations
.edu.post	Afilias	Restricted to education sector
.gov.post	Afilias	Restricted to government sector
.org.post	Afilias	Restricted to community groups
.<cc>.post	Afilias or UPU member	Restricted to UPU members

The UPU is responsible for:

– generating KSK and ZSK key pairs for signing the .POST zone;

– protecting the confidentiality of the KSK and ZSK private components used to sign the .POST zone;

– signing all authoritative DNS resource records in the .POST zone;

– providing and maintaining the DS resource record in the root zone;

– facilitating necessary additions, updates and removals of entries within the .POST zone file with respect to the above-listed zones;

– providing a process for 2LD registry operators to submit their respective DS resource records;

– validating 2LD registry operators' DS records prior to their publication in the .POST zone;

– providing a policy for emergency key rollovers for 2LD registry operators;

– performing emergency key rollovers at the request of 2LD registry operators.

5.1 Registry operator

In the case of <cc>.post, the registry operator is responsible for:

– generating KSK and ZSK key pairs for signing their delegated zone;
– protecting the confidentiality of the KSK and ZSK private components used to sign their delegated zone;
– signing all authoritative DNS resource records within their delegated zone;
– providing the applicable DS resource record to the .POST zone manager;
– facilitating necessary additions, updates and removals for entries within their delegated zone;
– providing a mechanism for registrars to submit registrants' DS resource records into the applicable zone;
– providing a policy for emergency key rollovers;
– performing emergency key rollovers at the request of a registrar.

5.2 Registrars

A registrar acts as an agent for a registrant. Only a registrar has direct access to a registry operator's database and all change requests made by a registrant must be made via a registrar.

The registrar is responsible for:

– administering and managing domain names on behalf of the registrant;
– identifying registrants prior to accepting change requests;
– enabling registrants to submit DS resource records into the applicable registry;
– providing a policy for emergency key rollovers;
– performing emergency key rollovers at the request of a registrant.

5.3 Registrants

The registrant is a physical or legal entity that controls a domain name. Once a .POST domain name application has been approved, registrants enter into a binding and enforceable agreement with the registrar and the UPU.

Registrants are responsible for:

– generating KSK and ZSK key pairs for signing their delegated zone;
– protecting the confidentiality of the KSK and ZSK private components used to sign their delegated zone;
– signing all authoritative DNS resource records within their delegated zone;
– registering and maintaining DS resource records through their registrar.

Registrants may choose to delegate the responsibility of key management and signing to a registrar or third party zone operator like the UPU (through the Postal Technology Centre).

– Registrants are responsible for ensuring that their second-level zones are properly signed and maintained. They must also generate and upload DS records for their signed zones to their registrar (who, in turn, sends these into Afilias).
– Only the sponsoring registrar for a domain name can add, change or delete DS records for that domain name. Registrars must provide an auth-info code to verify any change for this domain name to prove possession of a private key.
– All key life cycle events, including but not limited to generation, activation, rollover, destruction and use, whether successful or unsuccessful, are logged with a system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion or other tampering.

5.4 Relying party

A relying party is the entity that makes use of DNSSEC signatures, such as DNSSEC validators and other applications. The UPU will publish DS resource records only in the root zone and recommends that the relying party should not configure static trust anchors. Any relying party that creates a trust anchor from the DS resource record does so at its own risk and the UPU takes no responsibility for any failures resulting from static trust anchor configurations. The UPU does not comply with or utilize RFC 5011.

5.5 Specification administration

This DPS is a living document and will be periodically reviewed and updated as appropriate.

5.6 Specification administration organization

Universal Postal Union (UPU)
Weltpoststrasse 4
3000 Berne, 15
SWITZERLAND

Tel: +41 (0) 31 350 3111
E-mail: secretariat (a) info.post
Website: www.info.post

5.7 Specification change procedures

Changes to the DPS that are approved by UPU will result in a new version of the document being released. New versions of the DPS will be available at the repositories listed below.

Only the most recent version of the DPS will be applicable. All changes identified in a review will be implemented within three months of the date of publication of the latest version.

6 Publication and repositories

The UPU will make this DPS and other related DNSSEC information available on its website at www.info.post.

6.1 Publication of public keys

The UPU publishes the KSK public key in single format, delegation signer (DS) records. The DS record for the .POST zone is provided to IANA for publication in the root zone. No other repositories will be used.

6.2 Registration, modification and deletion of DS resource records

Registration, modification and deletion of DS records must be limited to changes based on the .POST Domain Management Policy.

6.3 Emergency removal request

Operators may request an emergency removal or update of the DS resource record. This request must be in the same format as described above but must clearly be marked as an emergency change. All emergency requests will be treated with the highest priority and actioned as soon as possible.

6.4 Method to prove possession of private key

During pre-delegation checks, the UPU will ensure that:

– the DS records provided are available as DNSKEY records at the apex of the child zone;
– DNSKEYs are signed and verified against at least one of the DS records supplied;
– the DNSKEY has its SEP bit set;

– the signature validity period is not due to expire.

6.5 Risk

Unauthorized disclosure of a key means that another unauthorized entity may be able to use the key to sign unauthorized domain names, thereby compromising the UPU. In this case, the registrar should be informed immediately to allow it to take the necessary action.

7 Facility, management and operational controls

7.1 Site location and construction

The UPU operates two data centers, provided by Swisscom and Bedag service providers. Both data centers are located in Bern, Switzerland.

7.2 Physical access

Physical access is restricted and limited to authorized personnel. Third parties, including co-location staff, are not permitted access to racks containing UPU equipment without the authorization or accompaniment of UPU authorized personnel.

7.3 Power and air conditioning

The UPU office server room has separate air conditioning and UPS capabilities. All data centres must have:

– a redundant power feed;

– an uninterruptible power supply (UPS);

– a backup power source (generators);

– a robust cooling system (HVAC);

– each of these systems must be a minimum of N+1 for redundancy purposes.

7.4 Water exposure

The UPU has taken reasonable precautions to minimize the impact of water exposure at all sites.

7.5 Fire prevention and protection

All facilities are equipped with fire detection devices and all data centres are fitted with fire suppression systems. Detection measures are designed to comply with local safety regulations.

7.6 Media storage

Media considered sensitive is encrypted and stored in a safe accessible only to UPU management personnel.

7.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Where cryptographic devices are used, they are physically destroyed or zeroized in accordance with the manufacturer's guidance prior to disposal.

7.8 Off-site backup

The UPU performs regular backups of critical data, audit logging data and other sensitive information for the purpose of disaster recovery. All data is encrypted and stored off-site in a secure storage facility with appropriate physical and logical access controls.

The UPU has a recovery plan in case of compromising the DNS keys:

1 Identification of the personnel to notify;

2 Identification of the personnel to perform the recovery actions;

3 The re-key method;

4 An inventory of all cryptographic keys (e.g., the location of all certificates in a system);

5 Education of all appropriate personnel on recovery procedures;

6 Identification of all personnel needed to support the recovery procedures.

8 Procedural controls

8.1 Trusted roles

Trusted persons include UPU management and IT personnel that have access to the .POST zone to perform their day-to-day responsibilities. Access to signer systems requires a PIN code.

A trusted person may hold multiple roles within a signing procedure but no single trusted person can effect change to the security module (SoftHSM). All changes will be authorized, documented and signed off by a minimum of two trusted staff.

8.2 Personnel controls

Qualifications, experience and clearance requirements: Trusted persons who fulfil trusted roles must have demonstrated appropriate background, qualifications and experience relative to their prospective job responsibilities and have been employed with the UPU for a minimum of one year.

8.3 Background check procedures

All trusted persons must have been employed at the UPU for a minimum of one year and be in a senior role. Applicants must disclose their previous employment for the last five years and provide references for validation. Trusted persons will be re-checked every five years.

8.4 Training requirements

Training for a trusted role will be conducted by the UPU and will be specific to the role and responsibility of each trusted person. All trusted persons will be required to have an understanding of how the DNS works, the UPU's role in the DNS and the role of DNSSEC in the DNS.

8.5 Job rotation, frequency and sequence

The UPU will provide refresher training and updates for persons in trusted roles to the extent and frequency required to ensure that such persons maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

Trusted persons are rotated and replaced as and when required.

8.6 Sanctions for unauthorized actions

Disciplinary actions will be undertaken for unauthorized actions with respect to this DPS and/or other violations of UPU policies and procedures. Disciplinary actions may include:

– measures up to and including termination;

– damage liability;

– prosecution.

Disciplinary action will be assessed with the frequency and severity of the unauthorized actions:

– Computer security controls: The UPU ensures that the systems maintaining key software and data files are trustworthy and secure from unauthorized access. In addition, the UPU limits access to production servers to individuals with a valid business reason for such access.

– Network security controls: The signing systems are placed in separate UPU production systems, which are logically separated from all other systems. Use of normal network security mechanisms, such as firewalls, mitigate intrusion threats; only restricted role users are allowed access to production systems, and their work is logged.

– Key signing key: The UPU uses a ZSK key length of 1024 and a KSK key length of 2048 bits with algorithm 13 (Elliptic Curve Digital Signing Algorithm (ECDSA)) as the generation algorithm. Algorithm 8 (RSA/SHA-256) is also supported although being gradually phased out.

– Rollover keys: The UPU will automatically roll the ZSK with a pre-publishing scheme, as described in RFC 4641, section 4.2.1.1. ZSK rollover is carried out automatically every 90 days.

  For all domains hosted in UPU premises KSK rollover is performed once per year.

8.7 Contracting personnel requirements

Contractors are not permitted logical access to the SoftHSM. They may be used in an advisory role but will not perform any actions in relation to key generation or activation.

8.8 Documentation supplied to personnel

Trusted personnel will be provided with SoftHSM procedural documentation and a check list for use during interaction with the SoftHSM that will be signed and dated upon completion.

9 Audit logging procedures

9.1 Types of events recorded

Machine-generated logs are securely stored in a central monitoring system. These logs will be reviewed with greater scrutiny during and after key signing and key rollovers.

Zone edits and comments for the .POST zone file are versioned using a repository which includes a description of the change, the requester of the change, the authorizer of the change and the performer of the change. This information is backed up in accordance with the UPU backup procedures.

9.2 Protection of audit log

All logs are encrypted, backed up, and stored in a secure location. Logs are only available to UPU management and do not contain any private key or other sensitive information that may lead to compromise. Paper logs are scanned and stored electronically, and the paper logs themselves are then stored in a fireproof safe.

9.3 Audit log backup procedures

Audit logs are encrypted and backed up to external storage as part of the UPU backup procedure. Access to safes containing paper log material is accessible only to authorized UPU management.

9.4 Audit collection system

Automated audit data is generated and stored offsite. Data is recorded at the application, network, and operating system levels. Manually generated audit data is recorded by UPU staff and stored using current methods for physical and fire protection.

9.5 Vulnerability assessments

Anomalies or discrepancies in log data are investigated to analyze any potential vulnerabilities.

9.6 Compromise and disaster recovery

In the event that an incident compromises, or has the potential to compromise, security, the UPU will conduct an investigation to determine and identify the potential threats. If the incident leads to, or could lead to, a private key compromise of an active key, the emergency key rollover procedure will be performed.

9.7 Corrupted computing resources, software and/or data

All signing-related hardware will be covered by vendor maintenance contracts. In the event of a hardware fault, the equipment will be replaced in accordance with the contractual agreement with the vendor. In addition, the UPU maintains redundancy on all equipment at all sites. Failures will be investigated immediately and systems restored to full operation as soon as possible.

In the event of software corruption or failure, UPU trusted personnel will investigate the cause and restore systems from the most recent unaffected backup.

9.8 Business continuity and IT disaster recovery capabilities

The UPU has business continuity and IT disaster recovery plans in place to address the restoration of information system services and key business functions. These plans address:

– roles and responsibilities in the event of a disaster;

– fallback procedures for restoring business-critical processes within appropriate time frames;

– resumption procedures for restoring normal operations;

– criteria for activating the plan;

– communication with the public.

9.9 Entity termination

If the UPU were removed as the administrator of the .POST zone, the UPU trusted personnel will cooperate with the new party/parties to ensure a smooth transition. The new administrator would be responsible for maintaining the current state of the .POST zone.

If the UPU were to discontinue DNSSEC, a plan would be implemented and all notifications regarding the return to an unsigned zone would be provided via the UPU website at www.info.post.

10 Technical security controls

10.1 Key pair generation and installation

– Key pair generation: Key pair generation takes place in an OpenDNSSEC software with SoftHSM as a HSM repository that is managed by trained and specifically authorized personnel in trusted roles.

– Public key delivery: The public component of each generated KSK is exported from OpenDNSSEC as a DS record and published in accordance with the publication and repositories section.

The DS is delivered to the parent zone in accordance with the IANA procedures listed at http://www.iana.org/procedures/root-dnssec-records.html.

10.2 Key usage purposes

Keys are generated solely for the purpose of signing the .POST zone. No extraction of the keys is possible – only generation and deletion.

10.3 Private key protection and cryptographic module engineering controls

All cryptographic operations are performed in an SoftHSM and no private keys are made available, unprotected, outside of the SoftHSM.

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

Access to the signer system is documented in the trusted roles section.

10.5 Private key escrow

Private key components used for zones are not escrowed.

10.6 Private key backup

The UPU performs routine backups of the .POST ZSK and KSK private keys after each new key pair is generated. All backups are encrypted and only accessible by UPU trusted persons. Both the backup and restoration of the private keys requires dual authorization.

10.7 Private key storage on cryptographic module

Private components of keys used for the zone are stored on an SoftHSM in an encrypted format.

10.8 Private key archival

Private keys are not archived on the SoftHSM after rollover, but can be restored from backups as listed above.

10.9 Private key transfer into or from a cryptographic module

Keys are transferred to and from an SoftHSM in an encrypted format using hardware-specific operator cards that are encrypted and passcode protected.

10.10 Method of activating private key

Private keys are activated by configuring an activation and publication date when generating the relevant key pair.

10.11 Method of deactivating private key

Private keys are deactivated by specifying a delete date during generation of the relevant key pair.

10.12 Method of destroying private key

Where required, the UPU will utilize the zeroization function of its SoftHSM and other appropriate means to ensure the complete destruction of the .POST KSK and ZSK. The UPU will take all reasonable precautions to ensure that there are no residual remains of the keys that could lead to the reconstruction of the keys.

10.13 Other aspects of key pair management

The UPU will only publish the public keys that are current to the operation of the .POST zone. Public keys will not be archived past their deletion date.

10.14 Activation data

Trusted persons will hold credentials to be able to activate the SoftHSM. Activation data is stored on a hardware-specific card, which is encrypted and protected by a PIN. Trusted persons are required to safeguard their PIN in accordance with the UPU password policy.

10.15 Computer security controls

All production computer systems are housed in secure facilities. Physical and remote access to signing systems is limited to trusted persons. All physical and remote access to computer and signing systems is logged, regardless of whether it is successful or unsuccessful.

10.16 Network security controls

The SoftHSM repository resides on the signing server which is not exposed to the outside. The server is protected by two layers of firewalls.

10.17 Timestamping

The UPU uses trusted time sources within the signing system network to synchronize system clocks. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

10.18 Life cycle technical controls

The UPU tests all new sources of software in a lab environment prior to deploying to production servers. Systems are evaluated prior to their deployments, in order to maintain the quality and security of the DNS in .POST.

The UPU has technologies and policies in place to control and monitor the configuration of its systems; this includes monitoring of access to all systems, configuration changes and package installations or updates.

The SoftHSM is designed to require minimum maintenance. Updates critical to the security and operations of the signer system will be applied after formal testing and approval. The origin of all software and firmware will be securely authenticated by available means.

10.19 DNSSEC signing

DNSSEC should be deployed in each zone of the subdomains for consistency and validation of all .POST domains.

10.20 Rate limits

It is mandatory to use rate limits RRL2 in case DDoS is observed (advisable as a preventive measure) for all authoritative servers.

Note. – Implementation of rate limits will help to avoid answering requests in case of a DDoS attack (in addition to existing measures taken at the registry side).

11 Zone signing

11.1 Key lengths, key types and algorithms

The UPU uses Elliptic Curve Digital Signing Algorithm (ECDSA) algorithm with a key length of 2048 bits for the KSK and 1024 bits for the ZSK.

11.2 Authenticated denial of existence

The UPU uses NSEC3 as specified in RFC 4034.

11.3 Signature format

Signatures are generated using ECDSA algorithm (ECDSA Curve P-256 with SHA-256, RFC 8624).

11.4 Key rollover

Due to the size and algorithm used for the KSK, the UPU has decided the KSK will be rolled over annually using the double-signing method.

The ZSK, being smaller in size, is automatically rolled over every 90 days using the pre-publish method.

11.5 Signature life-time and re-signing frequency

RRsets are signed with the ZSK and have a validity period of 90 days. Automatic resigning takes place daily and all signatures are regenerated.

11.6 Verification of resource records

The UPU verifies that all resource records are in conformity with the current standards before publishing the zone. This is achieved using available tools and custom scripts.

11.7 Resource records (time-to-live)

RRtype	*TTL*
DNS key	86,400 seconds (24 hours) (same as the SOA)
Delegation signer (DS)	Inherit TTL from the corresponding delegation (NS-Set)
RRSIG	Inherit TTL from the corresponding signed RRset
NSEC	43,200 seconds (12 hours) (same as the negative TTL)

12 Legal matters

The UPU reserves the right to disable DNSSEC if the protocol introduces, or contributes to, increased instability or risk to the .POST zone. Notifications of intention to remove DNSSEC from the .POST zone will be provided via the website www.info.post.

12.1 Fees

The UPU does not charge fees for any function related to DNSSEC in the .POST zone file.

12.2 Term and termination

This DPS remains valid until it is replaced by a new version or if UPU ceases to be the .POST registry sponsor.

13 References

1 https://www.afilias.info/dps (DNSSEC policy from .POST registry)

2 https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

3 https://tools.ietf.org/html/rfc4641#section-4.2.1.1

4 https://tools.ietf.org/html/rfc6841

5 https://tools.ietf.org/html/rfc8624

6 .POST Domain Management Policy - https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services/-POST-Domain/Domain-Management-Policy