DNSSEC Policy & Practice Statement (DPS)

Introduction

The purpose of this DPS is to document the policies and procedures for operating DNSSEC in .versicherung. This document conforms to the Internet-Draft DNSSEC Policy & Practice Statement Framework (draft-ietf-dnsop-dnssec-dps-framework).

Overview

DNSSEC is an extension to the existing DNS-System that enables the authentication of DNS data and makes it possible to verify that the content of a DNS response has not been modified.

Resource record sets secured with DNSSEC are cryptographically signed and use asymmetric cryptography to establish a so-called “chain of trust” that traverses the public DNS tree. This trust originates at the root zone and follows the same delegation process as that of domain name registrations.

Document Name and Identification

Document title: DNSSEC policy statement for .versicherung
Version: 1.0
Created: Oct 10, 2011

Community and Applicability

The .versicherung-Registry supports the registry-registrar model, it deals only through registrars and registrants have no direct contact with the registry.

Registry

The .versicherung-Registry is responsible for the TLD .versicherung. This means that this organisation is responsible for the managmenent of all data related to registration, modification and deletion of (2^{nd}-level)-domain names under .versicherung.
The registry is also responsible for generating the relevant cryptographic keys, ensuring protection for those keys, signing the actual zonefile and the registration and maintenance of DS records in the root zone.

Registrar

The Registrar is responsible for the administration and management of domain names on behalf of the Registrant. They are also responsible for the registration and maintenance of the corresponding DS-Records within the Registry.

Registrant

The Registrant is a physical or legal entity that controls a domain name. They are responsible for the proper signing of child zones and the registration and maintenance of DS records through the Registrar. If necessary the process of zone signing can be delegated to the Registrar.

Dependent entities

Dependent entities are those users of that DNSSEC data, for example ISPs using validating resolvers or other applications. The dependent entities are responsible for maintaining the appropriate DNSSEC trust anchors and configurations.

Specification Administration

This DPS will be periodically reviewed and updated as appropriate.

Specification Administration Organization

TLD-BOX Registrydienstleistungen GmbH

Contact

TLD-BOX Registrydienstleistungen GmbH
Jakob-Haringer-Straße 8
5020 Salzburg
Austria
Telefon: +43/662/234548-38
Fax: +43/662/234548-938
E-Mail: office@tld-box.at

Specification Change Procedures

Any changes to this document need to be signed off by the Chief Technical Officer of TLD-BOX.
The most recent version of this DPS will be published on the website of the .versicherung-Registry.

Publication and Repositories

Publication Site

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

Publication of Key Signing Keys (KSK)

The deployed KSKs are published in the form of DS-Records directly in the root zone.

Access Control

DNSSEC-relevant information published on the specific website is accessible by the general public.

Operational Requirements

Meaning of Domain Names

The purpose and meaning of domain names can be found in domain registration policies of the .versicherung-Registry.

Activation of DNSSEC for Child Zone

A minimum of one DS Record must be provisioned by a registrar in the registry and subsequently published in the DNS for DNSSEC to be enabled for the relevant child zone. The published DS Record establishes the chain of trust to the child zone.

The registry presumes that provisioned DS records are of the correct form and will not perform any specific validation checks on these records except some basic syntax checking This means, in essence, that the registry will not verify if a DNSSEC enabled child-zone can be validated by the relevant DS record.

Identification and Authentication of Child Zone Manager

Reponsibility for the identification and authentication of a child zone manager rests with the registrar.

Registration of Delegation Signer (DS) Records

The registry accepts DS records through its EPP interface from any registrar. The registrar is identified and authenticated as described in Question 25(EPP). The DS record must be valid and sent in the format indicated in RFC 5910. Up to six DS records can be registered per child domain. The registrar can also remove all or selected DS records for a child domain.

Method to Prove Possession of Private Key

The registry does not perform any validation checks for authenticating the Registrant as the manager or holder of a specific private key.

Removal of DS Record

DS records can be removed via the EPP interface by the respective registrar. If all DS records of a child zone are removed, DNSSEC-validation for that zone is disabled.

Facility, Management and Operational Controls

Physical Controls

Site Location and Construction

The .versicherung-Registry is operated from two fully operational and geographically dispersed data centers, more than 300 kilometers apart. One data center houses the primary systems; the other data center houses the backup systems. In case of emergency a switchover to the 2nd data center is performed.

Physical Access

Physical access to the data center is limited to authorized personnel. All entry activity is recorded and the environment is continuously monitored.

Power and Air Conditioning

Power is supplied via separate and independent feeds. In case of power failure, power is provided by UPS and backup power generator units.

All air conditioning systems are also fully redundant.

Flood protection

Both data centers implement flood protection and detection mechanisms.

Fire Protection and Prevention

The data centers are equipped with fire detection and suppression systems.

Media Storage

Sensitive media is stored in a fireproof safe which is only accessible by authorized personnel.

Waste Disposal

All confidential documents and media are shredded or destroyed before disposal.

Off-site Backup

All systems are backed up to an external tape-library in a separate datacenter.

Procedural Controls

Trusted Roles

So-called “trusted roles” are staffed with highly trained and experienced personnel who will perform all relevant DNSSEC tasks such as the generation and deployment of keys, the management of trust anchors etc. These trusted roles are:

- System Administrator, SA
- Security Officer, SO

Task Requiring Separation of Duties

Any task performed on the zone-signer system requires at least one System Administrator and one Security Officer to be present.

Personnel Controls

Qualification, Experience and Clearance Requirements

Engineers taking part in a trusted DNSSEC role must have been working for the company for more than one year and must have all necessary qualifications.

Background Checks

Background checks are performed as part of the hiring process for all personnel .

Training Requirement

New trust role members must be present for and observe at least two regular key roll-overs with existing trust role members.

Contracting Personnel Requirements

Only personnel in specified trusted roles are permitted access to DNSSEC systems. If needed, a team member can perform tasks with the guidance of an external contractor. At no time, however, are external contractors or third parties permitted access to perform tasks directly on these systems.

Documents Supplied to Personnel

The registry supplies the necessary documentation to employees to support their work in a secure and satisfactory manner.

Audit Logging Procedures

Types of Events Recorded

The following events are logged to detect illegal/incorrect operations:

- Entry to all data center facilities
- Remote access attempts (successful and unsuccessful) to all DNSSEC Systems
- Any type of DNSSEC operation (such as key generation, key rollovers etc)

Frequency of Log Processing

All logs are checked by a number of automatic and manual methods.

Retention Period for Audit Log Information

Logfiles are stored for at least 30 days on the logging system. Thereafter, log files are archived on the backup system for at least 3 months.

Protection of Audit Log

Access to audit logs is permitted only for authorised personnel.

Audit Log Backup Procedures

Audit logs are backed up on external tape media periodically. This tape library is located in an external data center.

Audit Collection System

Electronic log information is transferred in real-time to audit collection systems. Physical audit logs are archived in a fireproof safe.

Notification to Event-causing Subject

Any persons that trigger an event to be logged are not also notified of this action or that such logging is taking place.

Vulnerability Assessments

All anomalies in logging information are investigated to analyze potential vulnerabilities.

Compromise and Disaster Recovery

Incident and Compromise Handling Procedures

If the private part of an active KSK is (likely to be) compromised, an emergency key rollover will be performed.

If the DNSSEC systems become unavailable due to accidents or disasters, the personnel will attempt to get systems back online as soon as possible.

Corrupted Equipment, Software or Information

In the event of a hardware fault the faulty element(s) will be replaced as soon as possible (Full service contracts are maintained with all hardware vendors).

In the event of a software or data issue, the registry will perform recovery actions in accordance with pre-defined recovery plans.

Business Continuity and IT Disaster Recovery Capabilities

In the event of a disruption to DNSSEC services due, for example, to a disaster at a data center facility, the registry will recover the service(s) as soon as possible at the backup data center.

Entity Termination

If it becomes necessary to discontinue DNSSEC services for any reason, the registry will invoke a pre-defined set of procedures. The general public will also be informed in such an event.

If operations are to be transferred to another party, the registry will participate in the transition to ensure it as seamless as possible.

Technical Security Controls

Key Pair Generation and Installation

Key Pair Generation

The generation of key pairs is performed by hardware security modules (HSM) which are managed by trained and specifically appointed personnel in trusted roles. Key generation actions take place when necessary (e.g. before a planned key rollover) and must be performed by a minimum of two authorised personnel. These personnel must be present during the entire operation.

The entire key-generation procedure is logged electronically and documented manually by the security officer.

Public Key Distribution

The public part of the KSKs are exported and verified by the system administrator and security officer. The security officer is responsible for publishing the DS record in the root zone.

Newly generated keys will be synced automatically with the backup DNSSEC systems. The system administrator and the security officer are responsible for verifying synchronisation.

Public Key Parameters Generation and Quality Checking

Key parameters are defined in the Zone Signing Policy (see below) and quality control measures include verification of the key lengths.

Key Usage Purposes

A key generated for DNSSEC purposes must only be used for DNSSEC activities and should never by used outside of the signing systems. A key must only be used for one zone and cannot be reused.

Private Key Protection and Cryptographic Modules Engineering Controls

All cryptographic operations are performed within the HSMs.

Cryptographic Module Standards and Controls

The systems use HSMs which are FIPS 140-2 Level 2 certified.

Private Key (m-of-n) Multi-person Control

A minimum of 2 out of 5 persons are required to active a HSM module.

Key Escrow

Private keys are not escrowed.

Private Key Backup

Private keys are stored on at least 2 HSMs. As the HSMs store these keys which are encrypted with a HSM master key on the local file system of the signer, these private keys are also included in the normal file-system backup.

Private Key Storage on Cryptographic Module

The HSM master key is shared by all HSMs used for .versicherung. This master key is used to decrypt the private keys stored on the local file systems on the signer.

Private Key Archival

Private keys which are no longer in use are not archived in any particular form except that of normal backup copies.

Private Key Transfer into or from a Cryptographic Module

All private keys will be generated directly on the HSMs. They will be synced periodically and automatically to the backup system, which is initialized with the same HSM master key.

Method of Activating a Private Key

A new private key is activated be a team consisting of the system administrator and security officer.

Method of Destroying a Private Key

Private keys will not be destroyed. Once they have reached end of life, they are removed from the DNSSEC system.

Other Aspects of Key Pair Management

Public Key Archival

Obsolete public keys are not archived

Key Usage Period

KSKs will be rolled over when needed; ZSKs will be rolled over every 90 days.

Activation Data

Activation Data Generation and Installation

Each security officer is responsible for creating their own activation data.

Activation Data Protection

Each security officer is responsible for protecting their activation data. If a compromise of this activation data is suspected, the responsibility rests with the security officer to immediately change it.

Other Aspects of Activation Data

As part of emergency planning, a copy of all activation data is sealed in envelopes and stored in a secure location.

Computer Security Controls

Access to all computing components and registry systems is logged and traceable. All critical operations performed on these systems will also be logged. All personnel with access to these systems must use individual access credentials. The use of shared credentials is not permitted.

Network Security Controls

The registry systems are split into a number of different VLANs and security zones depending on security classification. All network traffic between these security zones is filtered by a number of firewall layers.

Time Stamping

Registry systems synchronise all system clocks with trusted time sources from the University of Vienna. All timestamps generated by the registry system are in UTC.

Life Cycle Technical Controls

System Development Controls

An open source product is used to implement DNSSEC. Any new versions of this software are tested in a lab environment and are subjected to a pre-defined testing framework. Only when all tests have completed successfully can the software be rolled out to production environments and in accordance with pre-defined procedures.

System Management Controls

A security audit of the registry system was performed before initialising the service and will be repeated at regular intervals.

Zone Signing

Key Lengths and Algorithms

The RSA algorithm with a key length of 2048 bits is used for generating KSKs and a key length of 1024 bits used for generating ZSKs.

Authenticated Denial of Existence

The registry uses NSEC3 with Opt-OUT as defined in RFC 5155.

Signature Format

The digital signature algorithm used to sign the TLD zone file is RSA/ SHA-2 as defined in RFC 5702.

Zone Signing Key Roll-over

The expected lifetime of the ZSK is 90 days.

Key Signing Key Roll-over

A KSK roll-over will be performed as needed.

Signature Life-time and Resigning Frequency

The KSK signatures of the TLD zone DNSKEY RRset will have a validity period of 15 days. The ZSK signatures of the TLD zone authoritative data will have a validity period between 12 and 14 days.

Verification of Zone Signing Key Set

Before publishing a signed zone on the name server, the zone must pass a number of checks

- Verification of the chain of trust from the DS-Record in the parent zone to the signature of the SOA record in the child zone
- Verification that the validity period of the signature of the SOA-Record is at least 2 days in the future
- Pass a number of predefined queries (with DNSSEC enabled) for special records in the zone

Verification of Resource Records

The Registry verifies that all resource records are conformant with the current standards before publishing the zone.

Resource Records Time-to-live (TTL)

The TTL for DS records will be set to 10800 seconds (3 hours) and the TTL for DNSKEY and NSEC3 records to 3600 seconds. RRSIG records inherit TTLs from the corresponding signed RRset.

Compliance Audit

A regular audit for DNSSEC systems and services will be performed. Audit reports are subsequently provided to the registry and any operational recommendations will be applied as necessary.

Legal Matters

Jurisdiction resides within the operators country of residence. Respective contracts such as Registrar contracts as well as the Terms and Conditions of end customer contracts (if applicable) will be closed.

The registry also complies with the national data protection acts and only releases customer data without consent if legally obliged.