2017 KSK Rollover Systems Test Plan

Version: 2016-07-22

Contents

Introduction

This document describes the actions needed to test changes to the ICANN infrastructure involved in the KSK rollover. Performance of the plan is by the IANA Functions Operator, coordinating with the Root Zone Maintainer (RZM). The tests include the interface with the Root Zone Maintainer, handling of the Key Signing Request and Signed Key Response, and generation of files containing the trust anchors to be published via HTTP(S).

Scope

The following procedures are affected and must be tested before a KSK rollover:

- **Key management -- key creation, replication and deletion**
- **KSR processing -- transfer and signing**
- **Trust Anchor publication**

Test Scheduling

- ***Key management*** must be tested and results approved no later than October 1, 2016, in order to be able to plan and execute the key creation ceremony in October 2016 and the key replication ceremony in February 2017.
- ***KSR processing*** must be tested and results approved no later than April 1, 2017, in order to be able to plan and execute the KSR signing ceremony in May 2017.
- ***Trust Anchor Publication*** must be tested and results approved no later than October 1, 2016, to be able to publish the updated TA XML after the replication ceremony in February 2017.

Key Management

Key Creation

The current key management software (*ICANN DNSSEC Key Tools*) includes a key generator (*kskgen*) that was used to generate the KSK in 2010. As none of the key parameters (e.g., algorithm and key length) has changed, it is expected that this tool can be used as is to generate additional keys.

- **T1:** The IANA Functions Operator should validate that *kskgen* works as expected and can be used to generate KSK-2017.

Key Replication

Existing procedures exist to copy keys between HSMs and were executed as part of the initial key ceremonies in 2010, as well as the HSM replacement in 2015.

- **T2:** The IANA Functions Operator should validate that a new key can be copied between HSMs in the same KMF, as well as between HSMs in different KMFs.

Key Deletion

The current key management software (*ICANN DNSSEC Key Tools*) includes a key backup tool (*keybackup*) that can be used perform various key lifecycle duties, e.g. key list, backup and delete. It is expected that this tool can be used as is to delete existing keys.

- **T3:** The IANA Functions Operator should validate that *keybackup* can be used to delete existing keys.

Key Processing

KSR Transfer

During the KSK rollover, multiple Key Signing Requests (KSRs) will be submitted from Root Zone Maintainer to the IANA Functions Operator.

- **T4.1:** The IANA Functions Operator should validate that it can accept multiple KSRs and return back multiple SKRs.

- **T4.2:** The IANA Functions Operator should validate that multiple submitted KSRs are equal (except for filename and XML identification).

KSR Signing

Note: The current KSR Signer (*ksrsigner*) has insufficient support for the key rollovers as currently envisioned, and will need updating before KSRs related to the key rollover can be processed. Requirements on the updated KSR Signer can be found in *2017 KSK Rollover Operational Implementation Plan*. The following tests can only be performed once such an update has been implemented.

For each possible key ceremony in preparation for phase D, E and F, the IANA Functions Operator should generate and sign corresponding test KSRs.

- **T5.1:** The IANA Functions Operator should develop a regression tool to validate that *ksrsigner* can sign the following SKRs:
    - □ **C-to-C:** extend phase C, do not continue to publication
    - □ **C-to-C:** prolong backout from phase D
    - □ **C-to-D:** move forward to publication
    - □ **D-to-C:** back out from publication to normal
    - □ **D-to-D:** prolong backout from phase E
    - □ **D-to-E:** move from publication to rollover
    - □ **E-to-D:** back out from rollover to publication
    - □ **E-to-E:** extend phase E, stay in rollover
    - □ **E-to-F:** move from rollover to revocation
    - □ **F-to-G:** move from rollover to normal
- **T5.2:** After a production KSR has been received, the IANA Functions Operator should perform an internal dry-run (practice) key ceremony to verify that the received KSR(s) can be processed at the next (real) key ceremony.
- **T5.3:** The IANA Functions Operator should verify back out procedures in cooperation with the RZM and that the correct back out SKR (identified by filename, XML identification and content hash) can be communicated and implemented.

Trust Anchor Publication

Trust Anchor XML Generator

- **T6.1:** The IANA Functions Operator should validate that a valid Trust Anchor XML file containing an active KSK-2010 and an active KSK-2017 can be created using data from Certificate Signing Requests resulting from key generation ceremonies.
- **T6.2:** The IANA Functions Operator should validate that a valid Trust Anchor XML file containing a revoked KSK-2010 and an active KSK-2017 can be created using data from Certificate Signing Requests resulting from key generation ceremonies.
- **T6.3:** The IANA Functions Operator should validate that a valid Trust Anchor XML file containing an active KSK-2017 can be created using data from Certificate Signing Requests resulting from key generation ceremonies.

Trust Anchor Signing

- **T7.1:** The IANA Functions Operator should validate that it can produce a detached S/MIME signature of a Trust Anchor XML file.

ICANN

One World, One Internet

ICANN.ORG