Root Zone DNSSEC Key Signing Key Rollover

Champika Wijayatunga - ICANN | SANOG29 - Pakistan | Jan 2017

Motivation for the Talk

- ICANN is about to change an important configuration parameter in DNSSEC
- For a network DNS operator, this may create a need for action
- This discussion is meant to inform: What is happening, when, and what to do if troubleshooting is needed

Who Will Be Impacted?

DNS Software Developers & Distributors

System Integrators

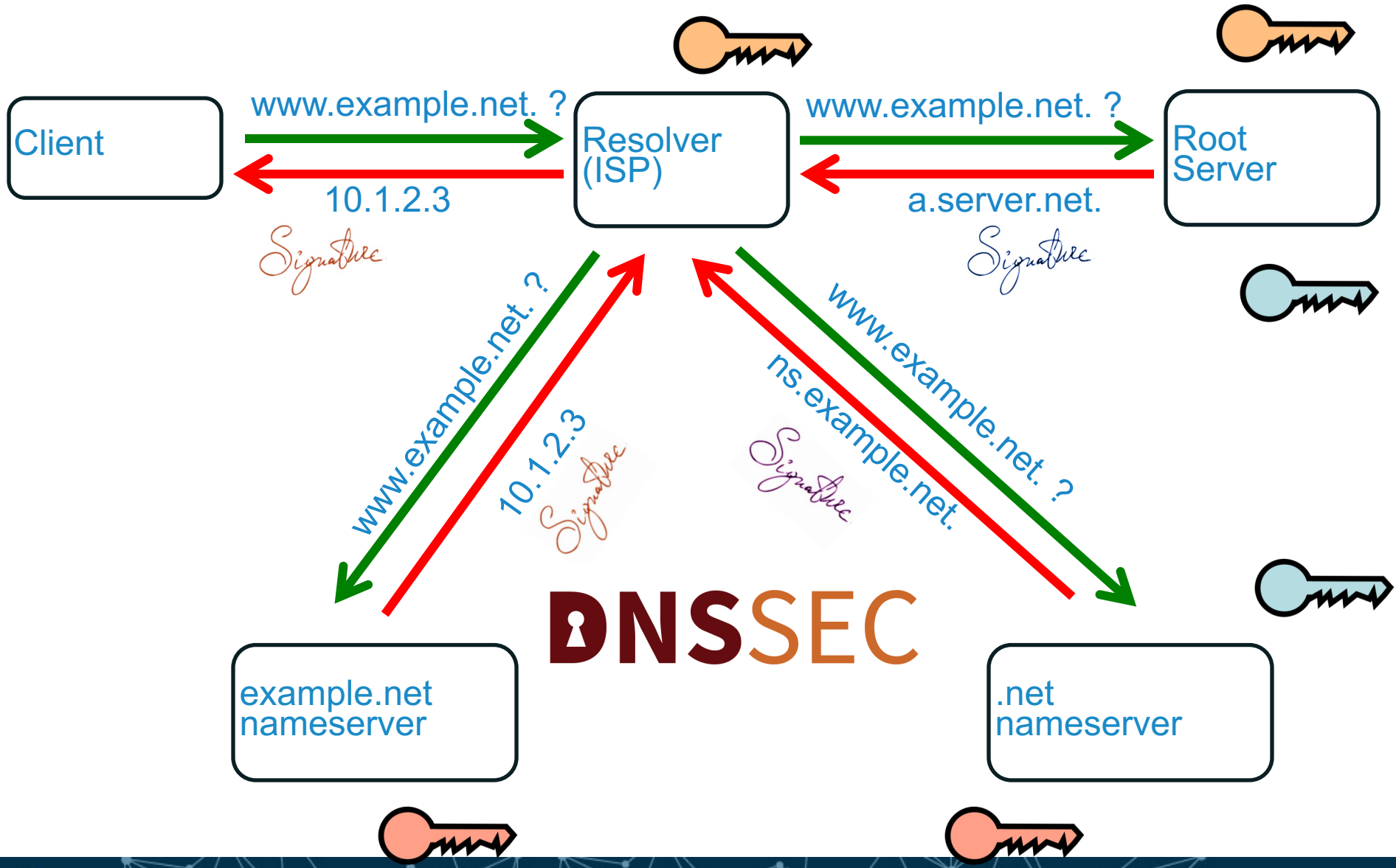
Network Operators

Root Server Operators

Internet Service Providers

End Users
(if no action taken by resolver operators)

How DNSSEC Works

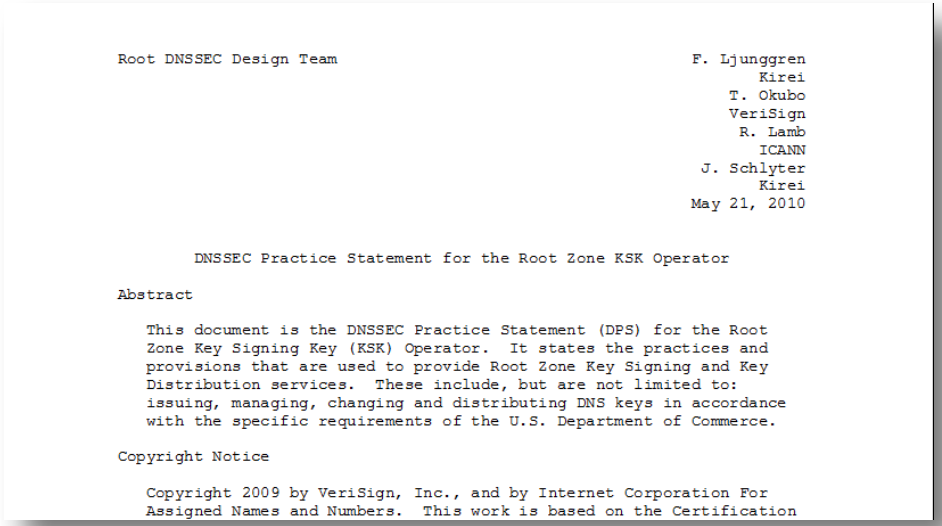


DNSSEC Key Management in the Root Zone

- DNSSEC key management is divided into
  - Key Signing Key (KSK), self-signs the key set
  - Zone Signing Key (ZSK), signs other zone data
- These roles are meaningful to the operators of signed zones
  - The significance is that the roles are separated
- ICANN manages the KSK
  - Same KSK since operations began in 2010
  - The KSK signs the ZSK quarterly in a ceremony
- Verisign, as Root Zone Maintainer, manages the ZSK
  - ZSK is changed quarterly

DNSSEC Key Management in the Root Zone

- Multi-stakeholder, bottom-up trust model* /w 21 crypto officers from around the world
- Broadcast Key Ceremonies and public docs
- SysTrust audited
- FIPS 140-2 level 4 HSMs



Root Root DNSSEC Design Team

F. Ljunggren
Kirei
T. Okubo
VeriSign
R. Lamb
ICANN
J. Schlyter
Kirei
May 21, 2010

DNSSEC Practice Statement for the Root Zone KSK Operator

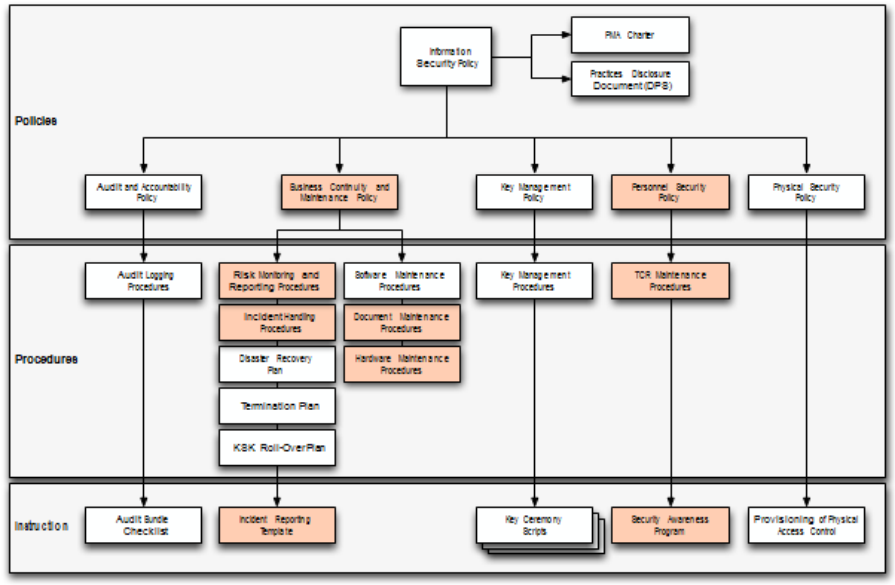
Abstract

This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, but are not limited to: issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. Department of Commerce.

Copyright Notice

Copyright 2009 by VeriSign, Inc., and by Internet Corporation For Assigned Names and Numbers. This work is based on the Certification

Root DPS
DNSSEC Practice Statement



*Managed by technical community+ICANN

Photos: Kim Davies

Why Change the KSK?

- Primary reason – Operational Preparedness
  - KSK has no expiration date, currently no weakness
  - No key should live forever: bad crypto practice
  - DNSSEC Practice Statement states the key will be rolled
  - Prefer to exercise process in normal conditions
    - As opposed to abnormal, such as key compromise
- Big challenge
  - Involves countless/uncountable participants
  - No test environment can cover all possibilities

The KSK Roll Plan Documents

- The plan consists of five documents
  - 2017 KSK Roll Operational Implementation Plan
  - 2017 KSK Roll Systems Test Plan
  - 2017 KSK Roll Monitoring Plan
  - 2017 KSK Roll External Test Plan
  - 2017 KSK Roll Back Out Plan

- The documents are available at https://www.icann.org/kskroll

Bottom Line

- Changing the root KSK will impact just about all DNSSEC validations (15% worldwide)
- If the trust anchor is "misconfigured" (i.e., the wrong key) DNSSEC will reject legitimate responses
- To anyone or any process relying on DNS, it will appear that the desired data is unavailable, website is unreachable, "the Internet is down"

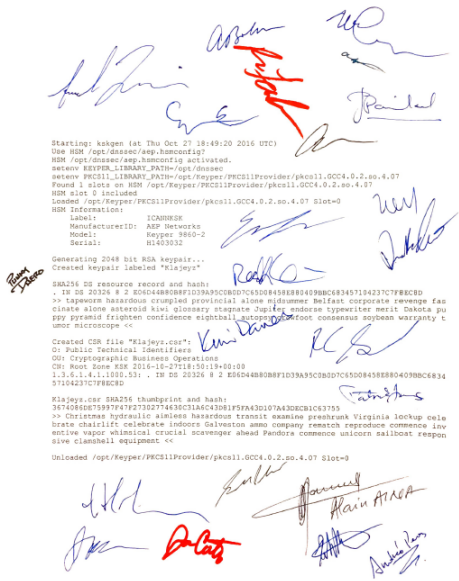
What You Need to Know

- Manage Your Trust Anchors
  - Be aware of your software tools for managing trust anchors
  - Be aware of the new KSK
- When Events Happen
  - Keep an eye on dates
  - Be mindful of when changes are scheduled and monitor appropriately

Planned KSK Roll Dates

- Plans publically available from July 22, 2016

- Key ceremonies
  - Q4 2016 ceremony (October 27): generate new KSK
  - Q1 2017 ceremony (February): KSK operationally ready



Don’t Get Locked Out!

- To help ensure trouble-free Internet access for their users, Internet service providers, enterprise network operators and others who have enabled DNSSEC validation must update their systems with the public part of the new KSK (the root “trust anchor”)
  - Available from https://www.iana.org/dnssec/files

- Key dates of the process when end users may experience interruption in Internet services:
  - 19 September, 2017

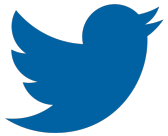
    Size increase for DNSKEY response from root name servers
  - 11 October, 2017 – Most important date

    New KSK used for signing for the first time
  - 11 January, 2018

    The old KSK is revoked

For More Information

- Join the ksk-rollover@icann.org mailing list:
  - https://mm.icann.org/listinfo/ksk-rollover



- Follow on Twitter
  - @ICANN
  - Hashtag: #KeyRoll

- Visit the web page:
  - https://www.icann.org/kskroll

Engage with ICANN

Thank You and Questions

Reach me at:
Email: champika@icann.org
Website: icann.org/kskroll


twitter.com/icann


gplus.to/icann


facebook.com/icannorg


weibo.com/ICANNorg


linkedin.com/company/icann


flickr.com/photos/icann


youtube.com/user/icannnews


slideshare.net/icannpresentations