ITL BULLETIN FOR SEPTEMBER 2017

UPDATING THE KEYS FOR DNS SECURITY

Scott Rose, Larry Feldman,[1] and Greg Witte,[1] Editors
Advanced Network Technologies Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

The Internet's Domain Name System (DNS) uses the DNS Security Extensions (DNSSEC) to help maintain the authenticity and integrity of its services. DNSSEC adds digital signatures and supporting keying material to the DNS, enabling users to authenticate domains and detect attempts to spoof or modify DNS responses transmitted over the Internet. In October 2017, the DNSSEC key for the root of the DNS will be updated (or "rolled") for the first time.

NIST's Information Technology Laboratory has been working with DNS experts from around the world to help plan and test the procedures to be used in this important DNSSEC maintenance procedure. This article explains how DNSSEC works, describes the validation keys that are being used to improve DNS reliability, presents a timeline of the key change (or "rollover"), and explains what DNS administrators need to know if DNSSEC validation is used.

An Introduction to DNSSEC

DNS is a foundational component of the Internet. While each of the millions of hosts on the Internet has one or more unique network addresses, DNS is what makes it possible for a user to address it by a more meaningful name. For example, the network address: 2406:da00:ff00::36f3:d44e is actually the more familiar "www.nist.gov."

Although DNS is critical to today's Internet system, we have known about serious security issues with it for at least 30 years. To help address these issues, a set of protocols - DNSSEC - was developed to digitally sign DNS information, thus introducing public key infrastructure (PKI) into the DNS.

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, partnering with NIST, has helped for many years to lead the DNSSEC Deployment Initiative, which works to encourage all sectors to voluntarily adopt security measures that will improve security of the Internet's naming

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

infrastructure as part of a global, cooperative effort that involves many nations and organizations in the public and private sectors.

DNSSEC helps to confirm the authenticity of DNS source information, and helps to ensure that responses haven't been spoofed or tampered with. DNS is based on a hierarchical tree-like structure, where a parent zone (e.g., .gov) maintains links to its branches (e.g., nist.gov, time.gov, science.gov). In a similar way, with DNSSEC, each parent top-level domain (TLD) can vouch for the security of its child delegations. These TLDs, in turn, are authenticated by the DNS Root Zone – the top node of the entire DNS tree.

Clients must pre-configure one or more validation keys to validate DNSSEC responses. Keys higher in the DNS hierarchy are preferred, because they can be used to establish trust for all delegations under that node in the DNS. For example, the key for ".gov" can be used to build trust in any DNSSEC-signed domain under ".gov." Since the DNS Root Zone (".") is the top node of the entire DNS tree, clients configured to use the Root Zone key for DNSSEC will be able to validate any response from a fully DNSSEC signed zone.

DNSSEC participation is optional for private sector organizations, and clients must signal that they want DNSSEC information included in responses. DNSSEC validation is mandatory for federal agencies and is included in the requirements of the Federal Information Security Management Act (FISMA), the U.S. legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.

Securing the Keys

To deploy DNSSEC in the DNS root zone – and as part of the process of improving DNS reliability – the group of Root Zone Management (RZM) Partners initiated a collaboration in 2009 and, in July 2010, released the first publication of a signed root zone that could be validated. The RZM Partners at the time were:

- Internet Corporation for Assigned Names and Numbers (ICANN);
- Verisign, as the Root Zone Maintainer; and
- U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA), as the Root Zone Administrator.

The public key that is used to authenticate DNS data occurs through a master key signing key (KSK). The current Root Zone KSK was generated in 2010 at a ceremony held in an ICANN facility in Culpeper, Virginia. The key materials were subsequently transported to a second ICANN facility in El Segundo, California, and once it was verified that they had been securely transported, the public component of the KSK key pair was published. The requirements for generating and maintaining the Root Zone KSK, as well as the respective responsibilities of each of the RZM Partners, were specified by NTIA.

The Internet Assigned Numbers Authority (IANA), a set of functions operated by ICANN, was originally contracted by the NTIA to include numerous coordination and administration functions that are critical for DNS. The IANA Functions Contract between NTIA and ICANN was modified in July 2010 to include responsibilities associated with Root Zone KSK management, and those requirements have been carried forward in subsequent revisions of that contract.

The contract expired in 2016 without renewal, with ICANN continuing to perform the IANA functions as part of a multistakeholder model. NTIA and NIST continue to interact with ICANN, but no longer as the IANA contract holder. Instead, NTIA (with NIST as technical advisors) is the designated U.S. Government agency responsible for Internet Governance.

To ensure ongoing security, in a process similar to how many of us update our own passphrases periodically, those Root Zone keys need to be updated. The previous IANA contract required that: "[the] RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation."[2] While this is no longer required, ICANN continues to follow recommended sound security operations and is moving forward in updating the DNSSEC Root Zone KSK.

Root Zone DNSSEC Key Rollover

For the first time since the Root Zone KSK was initially generated, ICANN (in its role as the IANA Functions Operator, and in cooperation with the other RZM Partners) is planning to perform a Root Zone DNSSEC KSK rollover in October 2017. Changing the key means generating a new cryptographic key pair and distributing the new public component.

In December 2014, ICANN solicited volunteers from the community to participate with the RZM Partners in a Design Team to develop the Root Zone KSK Rollover Plan. The deliverables for this work were a comprehensive set of technical and operational recommendations and a detailed implementation plan for executing the first Root Zone KSK rollover.

The ICANN plan for the Root Zone key rollover is documented on their website, https://www.icann.org/resources/pages/ksk-rollover. The major milestones are:

- **October 27, 2016:** KSK rollover process begins, as the new KSK is generated.
- **July 11, 2017:** Publication of new KSK in DNS.
- **September 19, 2017:** Size increase for DNSKEY response from root name servers.
- **October 11, 2017:** New KSK begins to sign the root zone key set. **(This is the actual rollover event.)**
- **January 11, 2018:** Revocation of old KSK.

[2] This requirement is stipulated in the DNSSEC Policy and Practice Statements (DPS), Root Zone KSK Operator DPS, Section 6.5.

- **March 22, 2018:** Last day the old KSK appears in the root zone.
- **August 2018:** Old key deleted from both ICANN Key Management Facilities.

ICANN is executing an extensive outreach campaign to ensure that those who currently use the KSK know about the change. The ICANN Communications Plan has been in place for nearly a year, and draws on a broad array of communications tools and social media. Even the U.S. Computer Emergency Readiness Team (US-CERT), an organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) that analyzes and reduces cyber threats, disseminates cyber threat warning information, and coordinates incident response activities, recently issued a notice about the pending event.

As the coordination progresses, the following plans linked on the ICANN KSK rollover page will support the update:

- **2017 KSK Rollover Operational Implementation Plan** - Describes the operational steps to accomplish the 2017 KSK Roll project, including the timeline of the eight-phase process.
- **2017 KSK Rollover Back Out Plan** - Describes anticipated deviations from the Operational Implementation Plan based on anomalies occurring while executing the operational plan.
- **2017 KSK Rollover External Test Plan** - Covers the preparation of operational test environments, accessed by the general Internet public, to evaluate whether external systems are prepared to participate in the KSK roll.
- **2017 KSK Rollover Monitoring Plan** - Describes the plan to monitor the effects of changing the trust anchor for the root zone in the traffic toward root servers.
- **2017 KSK Rollover Systems Test Plan** - Describes the actions needed to test changes to ICANN's infrastructure involved in the KSK roll.

It is important to note that if the KSK rollover goes smoothly, as anticipated, there will be no noticeable impact to Internet users. That said, with any change to something as critical as the Root Zone of the DNS, there is a small chance that some systems will not be able to gracefully handle the rollover. If there are major complications, the plans describe the process for the Root Zone Managers to address and recover from complications.

What DNS Administrators Need to Know

First, the KSK rollover only affects DNS recursive resolvers that have been configured to use DNSSEC. If DNSSEC is not configured, then the Root Zone rollover will not impact current operation.

If DNSSEC validation is used, the administrator has two options:

1. **Configure automated key rollover**: Most DNS implementations now support the automated key rollover protocol specified in RFC 5011. This protocol enables a DNSSEC client to automatically update its trusted keys when the trusted DNS zone signals that it is changing its key. How this configuration is done is specific to implementation, so administrators should consult their implementation's documentation. Automated key rollover can be tested using the ICANN KSK Rollover Testbed. This requires the use of a test system, as production systems should not use the testbed (it is not a full root zone). Administrators should monitor their systems during major operations in the rollover time frame (see above). If a large number of errors are seen on the day of or immediately after an event, this could mean that the automated rollover did not work or encountered an error. Administrators may have to manually update the Root Zone key (see #2 below).

2. **Manual key rollover**: If the given DNS client uses DNSSEC but does not support the automated key rollover protocol, administrators must update the key manually. How this is done is specific to the implementation in question, so administrators should consult their implementation's documentation. The new Root Zone key can be added to the set of trusted keys at any time but should be added before the old key is revoked to ensure continued operation. From the posted roadmap, this date is **October 11, 2017**. Therefore, the new Root Zone key (that is already published) **must be added before October 11, 2017**.

ICANN, working with industry experts, provided detailed recommendations in the above-referenced plans on how to implement the Root Zone KSK rollover. The recommendations include references to appropriate procedures, coordination with Root Server System Advisory Committee (RSSAC), and schedule of operations.

Afterwards, stakeholders will review lessons learned and will identify opportunities for improvement of subsequent instances. The next planned RZ KSK roll is years away but may include additional activities such as an update to the security algorithm used by the key management systems. Such an algorithm rollover might provide improved security with shorter keys.

Conclusion

As with passphrases and PKI certificates, the cryptographic keys used to sign the DNS root zone need to be changed periodically to help maintain integrity and ensure the continued security of the DNS. The Root Zone Management Partners are working to implement a seamless and transparent update, but since this type of root-level change has never occurred before, the rollover must be widely and carefully coordinated.

No action is required of typical Internet end-users, who should not notice any impact at all. Internet service providers, enterprise network operators, and DNS administrators who operate DNSSEC validating resolvers must ensure that their systems obtain (or are configured with) the public part of the new KSK. Managers of federal DNS systems can stay up to date through the NIST website: https://rollready.dnsops.gov.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov