Roll of the Root Zone KSK

Edward Lewis, OCTO staff

This program note describes a project to change the Root Zone KSK.

The "Root Zone KSK" refers to a cryptographic key managed by ICANN as the IANA Functions Operator. In support of DNSSEC, which adds security to the DNS and falls under the banner of a more secure Identifier ecosystem, the Root Zone KSK is a critical element in the processing of verified DNS traffic.

The Root Zone KSK consists of a cryptographic key with two components being a private component held secret by ICANN and a public component held by each member of the anonymous audience that benefits from the security. With the private component ICANN produces digital signatures needed to verify the authenticity and integrity of data received. With the public component operators of DNS clients and caches can verify the data as it is received.

ICANN has been using the same Root Zone KSK since June 2010 when DNSSEC began to enhance the security of the Root Zone. Cryptographic keys have unpredictable useful lifetimes, as nothing remains secret forever. After 5 years of operation ICANN was assigned to prepare to change the Root Zone KSK and that process has begun.

Changing the private component is a simple task. Changing the public component is a task that has few parallels in the history of technology. The reason is that there is no known roster of those who have and rely upon copies of the public component of the Root Zone KSK.

There are technical preparations needed to minimize the risk of disruption. With the change being motivated by proper maintenance and not from an imminent threat, continuity of service is paramount. With that, there is a need to surround the technical preparations with adequate communications.

There is a need to reach anyone relying on a secure Internet that they first need to make use of DNSSEC validation from the Root Zone KSK and that the Root Zone KSK is about to change. Already engaged are the developers of the technology to ensure proper software is available, with much work to go. Operators will then need to be educated on the new software and on the timing of the events of the change to the Root Zone KSK, or key roll.

The preparations have already begun. The timing of the change is unknown, dependent on the IANA transition.