



Increasing the Root Zone ZSK Size

Friday, 1 April 2016 12:00 (30)

Verisign, in its role as Root Zone Maintainer, plans to increase the size of the root zone Zone Signing Key (ZSK) in 2016. The ZSK has been a 1024-bit RSASHA256 key since the initial deployment of DNSSEC to the root zone in 2010. In the latter half of 2016, the ZSK size will be increased to 2048-bits.

In this presentation we will outline the schedule for the change, describe various technical and non-technical details for implementing the change, describe how the change will affect root zone response sizes, and our plans for emergency fallback to a 1024-bit in the unlikely event it should be necessary.

Summary

Primary author(s) : WESSELS, Duane (Verisign)

Presenter(s) : WESSELS, Duane (Verisign)

Session Classification : Public Workshop: Research

Track Classification : Public Workshop