SSAC
ICANN Security and Stability
Advisory Committee

28 January 2008

SAC 026: SSAC Statement to ICANN and Community on Deployment of DNSSEC

SSAC notes the DNSSEC deployment efforts of ICANN and the community at large and encourages continued efforts to improve the security of the domain name system. We recognize that any technology deployment on a global scale is apt to reveal issues not considered in protocol design and development and in controlled (test) environments. SSAC notes that several such issues have been exposed with respect to DNSSEC[1] and recommends the following actions.

1. As manager of the IANA function, ICANN should continue its efforts to support and facilitate deployment of DNSSEC. ICANN should place initial emphasis on IANA function activities required for achieving DNSSEC signed zone operation in zones for which the IANA function has full operational responsibility, e.g., ARPA and INT, as well as zones where they have shared operational responsibility, e.g., root zone. ICANN should identify and resolve any issues associated with achieving signed operation of these zones, such as handling signed delegations and key distribution processes. ICANN should ensure that the appropriate community is involved with testing of systems prior to the operational deployment of each signed zone. As soon as practical, ICANN should define, coordinate and publish schedules for the dates of testing and operational deployment of each of these zones.

2. GTLD registries should study business, technical and financial issues regarding DNSSEC deployment with ICANN. During these studies, GTLD registries should identify policy and operational issues with ICANN/IANA, establish a time line for DNSSEC deployment with ICANN and discuss DNSSEC as an element of GTLD registry agreements.

3. DNSSEC will be most effective if it is a global service. Thus, ccTLD registries should also study business, technical and financial issues regarding DNSSEC deployment with ICANN. During these studies, registries identify any policy and operational issues to IANA/ICANN and establish a time line for DNSSEC deployment.

[1] During September 2007, engineers working with the .SE DNSSEC deployment determined that certain broadband access routers were unable to correctly process the Authentic Data (AD) bit and dropped DNS messages when the bit was set. This discovery stimulated further and more comprehensive testing of a broadband access products provided by a large set of vendors. The event also identified a software error in BIND, which was patched.

4. Registrars should study business and technical issues related to (a) accepting keys on behalf of registrants with ICANN and registries, and (b) providing DNSSEC service for customers who use registrar's name services. Registrars should identify any policy and operational issues with ICANN, establish time lines for DNSSEC deployment, and discuss DNSSEC as an element of registrar accreditation agreements.

In parallel with these activities, SSAC intends to review the readiness and completeness of DNSSEC, evaluating the following issues:

a) Protocol completeness.

b) The key rollover process.

c) Proposals for trust anchor repositories, including evaluation of DLV and other specific proposals.

d) Implementation and deployment testing, including dedicated test servers with signed (root and TLD) zones, trouble and performance reporting operation.

e) Performance and error analysis, establishing metrics for success.

f) End User Application development.

g) Availability of DNSSEC on commonly used DNS server platforms.

SSAC believes that these combined efforts are necessary to assure a widespread deployment and adoption of DNSSEC and looks forward to cooperating with all parties on this initiative.