Non-Public Domain Names in Certificates

ICANN

High-Risk Strings Study

- On the potential security impacts of the applied-for new-gTLD strings in relation to namespace collisions with non-delegated TLDs that may be in use in private namespaces including their use in X.509 digital certificates.
- Expected by 21 June 2013

Internal Name Certificate Issue Questions

- How widespread is the use of internal name certificates that either do or could contain names that collide with new gTLD applications?
- What are the risks associated with delegating new gTLDs with names that could appear in internal name certificates issued to someone not related to the new gTLD?

Request for Information (1/5)

1. Are non-public domain names used in common names or subjectAlternativeNames?
2. What types of certificates are allowed with non-public domain names? (e.g., TLS/SSL, S/MIME, VPN, code signing, access control)

Request for Information (2/5)

3. Anonymous statistical data to ascertain how many certs with non-public domain names have been issued and how many are still valid in the following categories:
   1. certificate type
   2. certificate lifetimes
   3. country-of-origin
   4. organization

Request for Information (3/5)

4. Do you allow issuing CAs under your root CA?
5. Are issuing CAs allowed to issue certs with non-public domain names?
6. Are policies being revised to restrict issuing certs with non-public domain names?

Request for Information (4/5)

7. What issues are of concern from a CA operator's perspective with regard to introduction of new TLDs at the root of the public DNS?

8. Who from your CA will communicate with ICANN in discussing these issues from your perspective and that of your customers?

Request for Information (5/5)

9. What recommendations can be offered for how to introduce new TLDs at the public DNS root?

10. How can further coordination between ICANN and root CA operators occur?

Sensitive Data

- ICANN is willing to sign an NDA to protect the information provided

- Only anonymized/aggregated information will be published

Follow-up Questions & Data Submission

- Please, contact Francisco Arias: francisco.arias@icann.org

Thank You & Questions?