CCNSO MEMBERS MEETING

IANA Names Function Update

Kim Davies
Director, Technical Services

ICANN 60: Abu Dhabi, UAE
31 October 2017
Overview

- New DNSSEC algorithm support
- New automated workflows
- Implementing the FOI recommendations
- Root Zone Management System roadmap
- Other development work
- Rolling the Root Zone Key Signing Key
- Performance reporting
- Customer Survey
New DNSSEC algorithm support

- Original suite of algorithms were those supported in 2010 with comprehensive software support.
- New algorithms, particularly associated with elliptic-curve cryptography, are now available.
- Aim is to support new algorithms and digests as mature implementations are available.
- **New algorithms supported in October 2017:**
  - GOST R 34.10-2001
  - ECDSA P-256 SHA-256
  - ECDSA P-384 SHA-384
- **New digest types supported in October 2017:**
  - GOST R 34.11-94
  - SHA-384

### Algorithm Types
- DSA/SHA-1
- RSA/SHA-1
- DSA-NSEC3-SHA1
- RSASHA1-NSEC3-SHA1
- RSA/SHA-256
- RSA/SHA-512
- GOST R 34.10-2001
- ECDSA P-256 SHA-256
- ECDSA P-384 SHA-384
- EdDSA 25519
- EdDSA 448

### Digest Types
- SHA-1
- SHA-256
- SHA-384
- GOST R 34.11-94
New automated workflows

- Routine change requests have been sent between PTI and Verisign via EPP.
- Three business processes were still manually communicated:
  - Changes to the authorities for the root zone
  - Deletion of a TLD
  - Escalation of a change request to be an “emergency”
- **New support introduced in August 2017:**
  - 100% of interactions communicated via EPP to Verisign (as the Root Zone Maintainer)
  - Meets requirements stipulated in the Root Zone Maintainer Agreement

iana.org/help/rzms-changelog
Framework of Interpretation provides guidance that informs how we should implement requests to delegate or transfer (redelegate) ccTLDs.

Key implementation impacts:
- Terminology
- Informed Consent
- Delegation Contacts
Terminology

- Guidance to replace historical term **Sponsoring Organisation** with **ccTLD Manager**
- In ccTLD-only documentation, terminology has been updated.
- In places also used by gTLDs, generic terminology such as “TLD Manager” is being used.
Terminology

- Guidance to replace historical term **redelegation** with **transfer** with accompanying rules for consent and revocation for cause.
- In documentation, terminology has been updated.
- In our early experience, the term “redelegation” is much more commonly understood in the community and we often have to explain we now must call them transfers.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-04-05</td>
<td>Delegation of the .rugby domain to World Rugby Strategic Developments Limited</td>
</tr>
<tr>
<td>2017-04-03</td>
<td>Delegation of the .hotels domain to Booking.com B.V.</td>
</tr>
<tr>
<td>2017-03-06</td>
<td>Transfer of the .versicherung domain to TLD-BOX Registrydienstleistungen GmbH</td>
</tr>
<tr>
<td>2017-03-01</td>
<td>Transfer of the .irish domain to Tin Mill LLC</td>
</tr>
<tr>
<td>2017-02-21</td>
<td>Transfer of the .homedeapot domain to Home Depot Product Authority, LLC</td>
</tr>
<tr>
<td>2017-02-21</td>
<td>Transfer of the .thd domain to Home Depot Product Authority, LLC</td>
</tr>
<tr>
<td>2017-02-14</td>
<td>Delegation of the .africa domain to ZA Central Registry NPC trading as Registry.Africa</td>
</tr>
<tr>
<td>2017-01-17</td>
<td>Delegation of the .پاکستان (“Pakistan”) domain representing Pakistan in Arabic Script to National Telecommunication Corporation</td>
</tr>
</tbody>
</table>
3.2. The FOIWG further interprets section 3.6 of RFC1591 regarding agreement to the Transfer as requiring that the communication from the IANA Operator requesting a party’s consent should clearly state (a) what the party is being asked to agree to and (b) what steps the IANA Operator will or may take in response to the party’s (i) affirmative consent, (ii) affirmative refusal to consent, or (iii) failure to respond to the communication requesting consent. The IANA Operator should also advise the Manager to seek legal advice prior to granting consent. The requirement to secure informed consent does not obligate the IANA Operator to ensure that the party from whom consent is sought is informed about consequences not within ICANN or the IANA Operator’s control.

- Providing a pro-forma consent form for execution by the current manager.
- Explicitly spells out the requirements derived from the FOI recommendations.
Delegation Contact

3.1. The FOIWG interprets section 3.6 of RFC1591 to require that the IANA Operator only seek consent for a Transfer request from the incumbent manager and the proposed manager. The IANA Operator should not seek consent from the Administrative or Technical contacts.

- Implemented in today’s manual processes.
- Intend to implement explicitly in next generation RZMS is to allow authorization contacts in the new model to be configured as “delegation contacts” or not. The ccTLD manager is empowered to nominate which of their contacts are allowed to approve transfers.
- Expect to retain additional out-of-band mechanisms to be conducted throughout due diligence process. Transfer approval electronically would be only a component. (See auth model discussion)
Open Issues

- IANA has implemented the recommendations from the ccNSO that has clear guidance
- Waiting on pending implementation issues from the ccNSO:
  - Procedure for how to revoke a ccTLD for cause and keep it operational
  - Appeal mechanism
RZMS Roadmap

**Completed**

- New automated workflows
- New DNSSEC algorithm support
- FOI implementation

**Next: Next-generation re-architecture**

- New authorization model
- New technical check implementation
- New customer API
- New security options
New Authorization Model

- Flexible mechanism for TLD managers to choose who can authorize changes, separated from the contacts that are published in the WHOIS.

New Flexible Model

Administrative Contact
1. Listed in public WHOIS
2. Approves change requests
3. Must be in country (ccTLDs)

Technical Contact
1. Listed in public WHOIS
2. Approves change requests

Authorising Contacts
1. Not published (managed via RZMS)
2. Approves change requests

- One or more (no fixed number)
- Must be persons (no role accounts)
- Stronger identity controls
- Flexible threshold approval options
- In-country requirements?
Authorization model design considerations

• Migration of existing contacts
  • Role accounts to be replaced with persons
• Granularity of control by contacts
  • How detailed should each contact’s access be configured?
  • Balancing complexity against meeting most/all needs
  • API-only accounts?
• In-country requirements from RFC 1591
• Protocol for adding special processing/handling on file
Other development work

- **Other elements of the next-generation RZMS**
  - **New technical check implementation.** Separate technical check logic into a standalone application that provides richer feedback and debugging.
  - **New customer API.** Provide a modern API to allow TLD managers to build systems to interact directly with RZMS, providing new possibilities to reduce error and in particular perform bulk operations.
  - **New security options.** Provide mechanisms for multi-factor authentication, mandatory authentication for authorizing change requests, audit logging and other improvements.

- **Instrumenting our LGR (IDN table) management process**
  In cooperation with the customer standing committee, modeling the process for publishing LGR changes and instrumenting our current systems to collect statistics that will ultimately augment the existing Root Zone change request SLAs.
KSK Rollover

- Multi-year process to replace the trust anchor for the DNS for the first time
- Considered sensitive as how software copes with updating the anchor is untested in the real world.
- Our team has generated the new trust anchor and published it.
- Cut-over was planned for 11 October 2017 but has been delayed to study late-breaking telemetry data.
- New cut-over target date to be decided.

iana.org/dnssec
PTI produces monthly reports on its performance for the Customer Standing Committee (CSC).

iana.org/performance/csc-reports

The SLE Dashboard provides real-time reporting of performance metrics defined by the naming community for root zone management performance.

sle-dashboard.iana.org
Lastly...

- **We are starting our annual customer survey**
- Invitations were send out last week to people who have transacted with us in the past 12 months
- Historically we have had a low response rate from ccTLD managers.
- Please take a moment to respond to the invitations (they will come from a company called Ebiquity)
- Responses due by 17 November
- Questions about the process? Email iana@iana.org
Feedback welcome.

kim.davies@iana.org