CCNSO MEMBERS MEETING
IANA Names Function Update

ICANN 58: Copenhagen, Denmark
15 March 2017

PTI | An ICANN Affiliate
Agenda

• PTI Board Update
  Lise Fuhr

• Performance Reporting
  Naela Sarras

• PTI FY18 Budget
  Elise Gerich

• Technical Development and Policy Implementation Update
  Kim Davies
PTI Board Update

Lise Fuhr
Lise Fuhr
PTI Board of Directors
Performance Reporting

Naela Sarras
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
FY18 PTI Budget

Elise Gerich
FY18 PTI Budget

- At a special meeting on 18 January 2017, the PTI Board approved the FY18 PTI budget

- The ICANN Bylaws call for a Caretaker IANA Budget, and the PTI Board proposed the FY18 PTI Operating Plan and Budget be adopted as the "Caretaker IANA Budget" described in Annex F to ICANN’s Bylaws. This Caretaker Budget will be replaced by the most recently adopted PTI Operating Plan and Budget.

- The PTI Board submitted it’s the FY18 adopted budget to ICANN, and the PTI FY18 budget will be rolled into ICANN’s FY18 budget
The Operating and Capital Expenses budget table shows a summary of all expenses other than the $0.4 million allocated for the Root Zone Maintainer Agreement.

<table>
<thead>
<tr>
<th></th>
<th>FY18</th>
<th>FY17</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating Expenses</strong></td>
<td>$9.5</td>
<td>$8.9</td>
</tr>
<tr>
<td>(including depreciation)</td>
<td>$0.1</td>
<td>$0.1</td>
</tr>
<tr>
<td><strong>Capital</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>$9.6</td>
<td>$9.0</td>
</tr>
</tbody>
</table>

US Dollars, millions

Technical Development & Policy Implementation

Kim Davies
Technical Development & Policy Implementation

- Root Zone Management System roadmap
- New authorization model
- Implementing the FOI recommendations
- Rolling the Root Zone Key Signing Key
Root Zone Management System

Planned updates to existing system

- New automated workflows
- New DNSSEC algorithm support

Next-generation rearchitecture

- New authorization model
- New technical check implementation
- New customer API
- New security options
- FOI implementation
Routine change requests are currently sent between PTI and Verisign via EPP.

Three business processes are still manually communicated:

- Changes to the authorities for the root zone
- Deletion of a TLD
- Escalation of a change request to be an “emergency”

Aim is to have 100% of interactions communicated via EPP later this year.

- Stipulated in the Root Zone Maintainer Agreement
New DNSSEC algorithm support

- Current 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.
- Deprecating algorithm and digest types to be left for future consultation on technical checks.
- Under active evaluation by development teams.
- Should we consider whether to allow untestable algorithm types in the root zone?

### 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
- GOST R 34.11-94
- SHA-384
New authorization model

- New mechanism to address pain points our customers see with the current method of submitting and approving root zone change requests.
- Find a mechanism that is flexible to allow for different configurations.
- Key foundation is decoupling the “authorization” and “published contacts” pieces of being a TLD contact.
- Seeking feedback as we commence development.
New authorization 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
New authorization 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
3. One or more (no fixed number)
4. Must be persons (no role accounts)
5. Stronger identity controls
6. Flexible threshold approval options
7. In-country requirements?

**New Flexible Model**

Transition process
• Separating the technical check processes into a separate system.
• Can be maintained independently of the RZMS.
• Published openly.
• Richer reporting and analysis.
• Comprehensive debugging logs kept for each test run, customers can view using self-service mechanisms.
• Better parallelism to address potential delays in current approach.
• Provide a mechanism for customers to interact with RZMS programmatically (using tools rather than manually interacting with website).
• Removes error-prone steps for customers with large portfolios
• Provides easy mechanism to perform bulk operations (submissions, status checking, etc.)
New security options

- Add two-factor authentication capability
- Migrate from role accounts to person based accounts
- Eliminate email-based submission
- Comprehensive audit trail available to customers to see who did exactly what, when.
• Implement terminology changes associated with FOI recommendations (e.g. phase out “redelegation”, “sponsoring organization”, etc.)
• Implement process changes associated with redelegation process.
  • “delegation contact”
Framework of Interpretation

• Framework of Interpretation provides guidance that informs how we should implement future requests to delegate or transfer (redelegate) ccTLDs.
• Key implementation requirements that require new approaches that pose questions:
  • Informed Consent
  • Delegation Contact
  • Administrative Contact residency requirement
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.

- Use a pro-forma consent form that must be executed by the current manager.
- Spells out the requirements derived from the FOI recommendations.
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.

Our proposed implementation 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.
Questions

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.

- **Is this requirement satisfied by the new authorization model?**
  - Admin and Tech contacts are separated from authorization responsibilities.
  - Authorization contacts can be configured to be for transfer or non-transfer requests only.
- **Is it sufficient for this pro-forma to be electronically accepted via the RZMS interface, or should something else be required?**
Questions

7. The FOIWG interprets the requirement that there be an administrative and technical contact for each domain including, for ccTLDs, an administrative contact residing in the country (section 3.1 of RFC1591) to mean, as a general rule, that the manager must confirm, and the IANA Operator must be able to validate, that the administrative contact resides in the country or territory associated with the ccTLD. This establishes a clear intention from RFC1591 that there be local (in the country or territory associated with the ccTLD) presence.

• **Is this requirement satisfied by the new authorization model?**
  • Administrative Contacts can continue to be required to be “in” the country, but may just be roles like a generic helpdesk.
  • All authorizers, and all substantive operations, could potentially be out of the country.
  • Does there need to be some test of materiality for being based in the country?
KSK Rollover

- Replacing the Root Trust Anchor for the first time
- Becomes operational in late 2017
- Before then, DNSSEC implementors must update their trust anchor with the new one we published in February
- ICANN in middle of awareness campaign.

iana.org/dnssec
Feedback welcome.