IANA: Who, what, why?
(or, Why the IANA functions are less interesting than you thought)

Elise Gerich, Michelle Cotton, Naela Sarras, Kim Davies
IANA Department
IANA Department — Who are we?

Elise  
Kim  
Naela  
Michelle  
Leo  
Pearl  
Amanda  
Selina  
Paula  
Dalini  
Andres  
Punky  
Marilia
What are the IANA functions?

- In 1998, ICANN was established as the steward and operator of the IANA functions
- The IANA Department within ICANN maintains the registries of the Internet’s unique identifiers
- The unique identifiers include protocol parameters, Internet numbers and domain names
- The IANA Department maintains these lists according to policies adopted by Internet names, numbers and protocol standards communities
Why does the IANA Department exist?

• The IANA Department within ICANN coordinates the Internet unique identifier systems needed to ensure the Internet interoperates globally.

• If computers did not use the same system of identifiers and numbers to talk to one another, the system would not interoperate.

• The authoritative registries are used by vendors, service providers, businesses, application developers and others to innovate and expand the use of the Internet.
Protocol Parameters

Number Resources

Domain Names
Protocol Parameters

Number Resources

Domain Names

Michelle Cotton
Comprehensive index of protocol parameter registries at [iana.org/protocols](http://iana.org/protocols)
Where do protocol parameter registries come from?

- The Internet Engineering Task Force (IETF) community writes Internet Drafts (I-Ds)
- When approved by the leadership of the IETF, these I-Ds become official Requests for Comments (RFCs)
- Many RFCs contain guidance to the IANA Department:
  - Instructions on the creation of a unique registry for protocol parameters
  - Registration policy
  - Initial registrations and reserved values
What is the IANA Department’s role with protocol parameter registries?

- **Before RFC approval:**
  - Review

- **After RFC approval:**
  - Implementation
  - Maintenance
Reviewing Internet Drafts before RFC approval

7. IANA Considerations

7.1. Registry for the fedfsAnnotation Key Namespace

This document defines the fedfsAnnotation key in Section 4.2.1.6. The fedfsAnnotation key namespace is to be managed by IANA. IANA is to create and maintain a new registry entitled "FedFS Annotation Keys". The location of this registry should be under a new heading called "Federated File System (FedFS) Parameters". The URL address can be based off of the new heading name, for example: http://www.iana.org/assignments/fedfs-parameters/...

Future registrations are to be administered by IANA using the "First Come First Served" policy defined in [RFC5226]. Registration requests MUST include the key (a valid UTF-8 string of any length), a brief description of the key’s purpose, and an email contact for the registration. For viewing, the registry should be sorted lexicographically by key. There are no initial assignments for this registry.

Work closely with the IETF community to make sure the “IANA Considerations” section of I-Ds is clear
Implementation and Maintenance for protocol parameter registries

• After RFC approval:
  • **Creation** of new registries and/or **updates** to existing registries
  • **Maintain** through accepting registration requests from the Internet community
  • Follow the registration policy for new registrations and modification to existing registrations
  • Update references
How many registries does the IANA Department maintain?

Over 2,800 protocol parameter registries and sub-registries.
Processing Protocol Parameter Requests

Request
What type of protocol parameter is being requested?

Registration Policy
Look at the named registry to determine which registration policy to follow. Defining RFC determines the policy.

Processing and Evaluation
- Follow the appropriate process according to registration policy
- Consult with experts if required
- Gather more information from requester if needed

Update Registry
- Make protocol parameter assignment in registry
- Notify the requester the registration is complete
Processing Protocol Parameter Requests

1. Request for a new Media Type
2. Review request: Are all the fields complete?
3. Send to technical expert for review
4. Add media type to the registry
5. Confirm request is complete with the requester
6. My media type registration is complete!
Requests per month
(Excludes Private Enterprise Numbers)

- Sep 2013: 175
- Oct: 148
- Nov: 129
- Dec: 133
- Jan 2014: 175
- Feb: 164
- Mar: 139
- Apr: 185
- May: 169
- Jun: 158
- Jul: 146
- Aug: 139
Performance Targets

- Performance standards were developed collaboratively with the IETF to supplement the existing MoU between ICANN and the IETF.
- Began reporting in 2007 on the Service Level Agreement deliverables.
- SLA is reviewed, modified and approved annually.

<table>
<thead>
<tr>
<th>Year</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLA Met</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>KPIs Met</td>
<td>99%</td>
<td>98%</td>
<td>99%</td>
<td>99%</td>
<td>100%</td>
<td>99%</td>
<td>100%</td>
<td>99%</td>
</tr>
</tbody>
</table>
Unique Identifiers

Internet Protocol

IPv4 Addresses

IPv6 Addresses

IP Header Flags

Border Gateway Protocol

AS Numbers

Path Attributes

...
Deterministic Decision Making

- The policies have deterministic formulas governing when an RIR can get more and how much they can get.
- IPv4 is allocated on a schedule and not by request.
- IPv6 and AS Numbers are allocated on receipt of a justified request.
- Staff validate what an RIR reports against what it publishes via its daily stats reports.
Allocation Types

• Formula + Request
  (IPv6 and ASN allocations)

• Formula + Schedule
  (IPv4 allocations)

• IETF Allocation Procedures
  (Non-Unicast Addresses)
**Formula + Request**
(IPv6)

**Request**
- ✓ Comes from an RIR

**Do they qualify?**
- ✓ Less than half of a /12 in reserve
- ✓ Not enough to last 9 months

**What do they get?**

\[ n = (6\text{mo usage}) \times 18 \]

\[
\begin{align*}
  n \leq 1 & \rightarrow 1 \times /12 \text{ block} \\
  n > 1 & \rightarrow n \times /12 \text{ block}
\end{align*}
\]
RIPE NCC IPv6 Pool as at 2014-10-02
(Millions of /48 addresses)

- Available (54642)
- Allocated (3670)
- Reserved (12620)
- Assigned (0)
Allocate and Communicate (1)

<table>
<thead>
<tr>
<th>PREFIX</th>
<th>DESIGNATION</th>
<th>DATE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5F00::/8</td>
<td>IANA</td>
<td>2008-04</td>
<td>Reserved</td>
</tr>
<tr>
<td>3FFE::/16</td>
<td>IANA</td>
<td>2008-04</td>
<td>Reserved</td>
</tr>
<tr>
<td>2C00::0000::/12</td>
<td>AFRINIC</td>
<td>2006-10</td>
<td>Allocated</td>
</tr>
<tr>
<td>2A00::0000::/12</td>
<td>RIPE NCC</td>
<td>2006-10</td>
<td>Allocated</td>
</tr>
<tr>
<td>2800::0000::/12</td>
<td>LACNIC</td>
<td>2006-10</td>
<td>Allocated</td>
</tr>
<tr>
<td>2600::0000::/12</td>
<td>ARIN</td>
<td>2006-10</td>
<td>Allocated</td>
</tr>
<tr>
<td>2400::0000::/12</td>
<td>APNIC</td>
<td>2006-10</td>
<td>Allocated</td>
</tr>
<tr>
<td>2620::0000::/23</td>
<td>ARIN</td>
<td>2006-09</td>
<td>Allocated</td>
</tr>
<tr>
<td>2001:B000::/20</td>
<td>APNIC</td>
<td>2006-03</td>
<td>Allocated</td>
</tr>
</tbody>
</table>
Allocate and Communicate (2)

Communicate allocation to the RIR

Communicate allocation to the operations community
Communicate results
After the formula is applied per the schedule, the results are communicated to the RIRs and operations community, and the IANA registry is updated.
[iana.org/assignments/ipv4-recovered-address-space](http://iana.org/assignments/ipv4-recovered-address-space)
Allocations per year

- 2011: 4
- 2012: 2
- 2013: 5
- 2014: 5
Performance Targets

• Formal performance standards consultation in 2012
• Have met or exceeded all targets since public reporting began in 2013

<table>
<thead>
<tr>
<th>Key Performance Indicators</th>
<th>Target</th>
<th>Actual</th>
<th>Target Met</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy (1)</strong> — Policy is correctly implemented.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Accuracy (2)</strong> — Registry is updated before notifying requestor of allocation.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Timeliness and Process Quality (1)</strong> — For a specific request, ICANN does not need to seek more than two iterations of clarification from the requesting Regional Internet Registry in order to correctly apply the registration policy.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Timeliness and Process Quality (2)</strong> — Requests are to be completed within 7 days.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Transparency (1)</strong> — Public announcement of an allocation is made on the same day as the allocation being recorded in the IANA registry.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Transparency (2)</strong> — An implementation schedule for a new global policies under C.2.9.3 will be posted following ratifications within 14 days for simple policies, and 30 days for complex policies.</td>
<td>100%</td>
<td>100%</td>
<td>✔</td>
</tr>
</tbody>
</table>
Unique Identifiers

Domain Name System

Domain Name Space

Domain Resource Record Types

DNS Security Algorithm Types

DNS Header Flags
Unique Identifiers

Domain Name System

Domain Name Space

- root
  - .org
    - wikipedia.org
  - .us
    - icann.org
  - .бел
    - дамена.бел
    - someco.us
1 Event Triggers Request

An event such as a change in TLD operator, routine maintenance (technical or staffing change) or a natural disaster triggers the need for a change request.
<table>
<thead>
<tr>
<th><strong>Operator</strong></th>
<th><strong>Recognized Company or Organization</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Formal Legal Name, Physical Address</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Contacts</strong></th>
<th><strong>Administrative Contact</strong></th>
<th><strong>Technical Contact</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Name, Job Title,</strong></td>
<td><strong>Name, Job Title,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Company, Address,</strong></td>
<td><strong>Company, Address,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Phone, Fax, Email</strong></td>
<td><strong>Phone, Fax, Email</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Technical configuration</strong></th>
<th><strong>Data that goes in the root zone</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Authoritative name servers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IP addresses of name servers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>DNSSEC (DS) records</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Metadata</strong></th>
<th><strong>Courtesy information not tied to operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>URL to Operator’s website, location of WHOIS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>service, domain converted to A-label, language etc.</strong></td>
</tr>
</tbody>
</table>
### Operator

Hamburg Top-Level Domain GmbH  
Gertigstrasse 28, Hamburg, 22303  
Germany

### Contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Address</th>
<th>City</th>
<th>Country</th>
<th>Email</th>
<th>Voice</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oliver Joachim Sueme</td>
<td>Hamburg Top-Level Domain GmbH</td>
<td>Gertigstrasse 28, Hamburg, 22303</td>
<td>Hamburg</td>
<td>Germany</td>
<td><a href="mailto:os@dothamburg.de">os@dothamburg.de</a></td>
<td>+49 40 27806736</td>
<td>+49 40 380 89 810</td>
</tr>
<tr>
<td>Martin Schlicksbier</td>
<td>TLD-BOX Registrydienstleistungen</td>
<td>Jakob-Haringer-Strasse 8</td>
<td>Salzburg</td>
<td>Austria</td>
<td><a href="mailto:iana@tld-box.at">iana@tld-box.at</a></td>
<td>+43 662 2345 48730</td>
<td></td>
</tr>
</tbody>
</table>

### Technical configuration

| NS A                | 194.0.25.21 2001:678:20:0:0:0:0:21 |
| NS C                | 193.170.187.10 2001:62a:a:3000:0:0:0:10 |
| DS                  |                                       |
| DS 53866 8 2 AF2F53F6B523F31C04A741B3826D27CBAE16F4BA6F... |
| DS 26479 8 1 1C9F5D68C413E8A9A2C8E1C1637B8A4DA2CA6827 |
| DS 26479 8 2 4A48334EF87D7FC156E886E5A2B2682FCF0679ED6FC... |
| DS 53866 8 1 D26808AE1E19086BCF5FC88D59066C3AD22F2E56 |

### Metadata

http://www.dothamburg.de  
whois.nic.hamburg
**Change Request**

A TLD operator submits a change request to IANA Department within ICANN. This is typically done through an automated web service ICANN provides called the Root Zone Management System (RZMS).
3 Policy Check

ICANN checks that the change request meets policy and technical requirements and confirms consent from the appropriate parties. If issues are found, ICANN clarifies with the TLD operator. Then, ICANN forwards the request to NTIA for authorization to proceed.
Technical
- Name Servers are responding
- Name Servers return correct data that matches the request
- DNS data can be verified using the supplied DNSSEC DS records
- Supplied email addresses work

Consent
- Existing contacts agree to change
- New contacts agree to their new responsibilities
- Other impacts TLDs agree

Regulatory
- Request meets legal requirements

Well-formedness
- Supplied data is clear, well-formed and consistent

Transfer of responsibility
- Meets policy requirements for transfers (differs between ccTLDs and gTLDs)
gTLDs
Change request reflects outcome of an evaluation and contracting process conducted elsewhere in ICANN according to GNSO policies.

ccTLDs
Change request reflects outcome of a consensus building process that happened **within the country**.
Implement changes

After authorization to proceed, any technical changes to the root zone are implemented. This includes applying a tamper-evident seal using DNSSEC, and distributing the updated root zone file to root server operators. The Root Zone Database is updated with the changes.

Verification

Changes that satisfy the policy requirements are transmitted to NTIA for verification. NTIA reviews the change and then gives authorization to proceed with publishing the change.
The Root Key Signing Key

- As part of its root zone related functions, the IANA Department manages the key signing key, used to secure the DNS with the DNSSEC protocol.

- An auditable process of performing key signing ceremonies to use this key is conducted using members of the community as key participants.
The DNSSEC root key is stored in a device known as a **hardware security module (HSM)** whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper proof. If there is an attempt to open it, the contents will self-destruct.
Seven smart cards exist that can turn on each device. The device is configured such that **3 of the 7** smart cards must be present to make it useable.
Each smart card is given to a different ICANN community member, known as a trusted community representative. To access the key signing key, therefore, at least three of these TCRs need to be present.
The HSM is stored inside a high-security safe, which can only be opened by a designated person, the safe security controller. The safe is monitored with seismic and other sensors.
The safes are stored in a secure room which can only be opened jointly by two designated persons, the *ceremony administrator* and the *internal witness*. The room is monitored with intrusion and motion sensors.
The safe room is located within a larger room where ceremonies are performed involving the TCRs and other persons. Ceremonies are recorded on video, witnessed by the participants and others, and audited by a third party audit firm. Access to the room needs to be granted by another designated person, the **physical access control manager**, who is not on site.
The ceremony rooms, known as **key management facilities**, are located within two guarded facilities, one each on the US West and East coasts.
The ceremonies

- Approximately four times a year, the TCRs and others meet to use the HSMs to sign keys to be used for the root zone.

- The process is streamed and recorded, with external witnesses watching every step. All materials (videos, code, scripts, etc.) are posted online at iana.org/dnssec.

- The purpose is to ensure trust in the process. DNSSEC only provides security if the community is confident the HSMs have not been compromised.
Watch short documentaries:

The Guardian
http://goo.gl/JvPu62

BBC Horizon
http://goo.gl/WAz1iV
Performance

Comprehensive service level performance reporting at  
iana.org/performance
How big is the job?

- **4** Key signing ceremonies
- **726** Top Level Domain Delegations
- **1,115** Domain-related requests
- **5** Number-related requests
- **13** Number Resource Registries
- **3,871** Protocol-related requests
- **2,800+** Protocol Parameter Registries
- **2** Third party audits
- **1,106** General enquiries

**Request count:** Period 30 September 2013 — 30 September 2014

**TLD count:** As at 7 October 2014

Domain related requests include processing .int, .arpa and other non-root related requests.
Satisfaction by customer group

- Trusted Community Representatives: 100%
- Requesters of routine root zone changes: 93%
- Regional Internet Registries: 100%
- Requesters of protocol parameter assignments: 93%
- Requesters of .int zone changes: 87%
- IESG members: 92%

IANA Functions Customer Survey 2013
## Root Processing Times

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of requests</th>
<th>Average processing time (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nameserver (NS) records</td>
<td>19</td>
<td>6.0</td>
</tr>
<tr>
<td>DNSSEC (DS) records</td>
<td>2</td>
<td>0.0</td>
</tr>
<tr>
<td>Admin contact change</td>
<td>12</td>
<td>16.3</td>
</tr>
<tr>
<td>Tech contact change</td>
<td>9</td>
<td>13.8</td>
</tr>
<tr>
<td>Metadata change</td>
<td>6</td>
<td>6.2</td>
</tr>
<tr>
<td>Delegation/redelegation</td>
<td>34</td>
<td>6.3</td>
</tr>
<tr>
<td>Root server update</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Measurement period: 2014-08-16 to 2014-09-15
The IANA Department does

- Create registries based on policies from the community
- Maintain existing registries
- Allocate number resources
- Publish all registries for general public use

The IANA Department doesn’t

- Create nor interpret policy
- Determine what can be a domain name
- Choose TLD managers
Summary

• IANA Department maintains the registries of unique numbering systems that keep the Internet interoperating.

• Most IANA registries are straightforward, and are not generally known to the end-user.

• High profile, hierarchically-delegated registries are used for the Domain Name System and Number Resources. IANA Dept. maintains the global “root” for these.
Thank you!

Website: iana.org
Service level reporting: iana.org/performance
Functional areas: iana.org/protocols, iana.org/numbers, iana.org/domains
More background: iana.org/about