Agenda

- KSK Rollover
- RDAP
- Next generation authorisation model
- Customer API
- Technical Checks
- Prioritisation Questions
KSK Rollover
## KSK Rollover High Level Project Plan

| Milestone                                      | Stat | Target  | 4Q14 | 1Q15 | 2Q15 | 3Q15 | 4Q15 | 1Q16 | 2Q16 | 3Q16 | 4Q16 | 1Q17 | 2Q17 | 3Q17 | 4Q17 | 1Q18 | 2Q18 |
|------------------------------------------------|------|---------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|      |
| Vendor Rollover Testbed Meeting                | ✔    | 10/2014 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Design Team Convened                          | ✔    | 12/2014 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| DT Draft Development                          | ✔    | 8/2015  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| DT Recommendation Public Comment             | ✔    | 8/2015  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| DT Final Report Development                   | ✔    | 1/2016  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| DT Recommendations Published                  | ✔    | 2/2016  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Communication Plan Development Initiated      | ✔    | 11/2015 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Communication Plan Development                |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Communications Plan Execution                 |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| External Testing Sites Developed              | ✔    | 10/2014 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| External Testing Sites Published              | ✔    | 10/2014 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| External Testing                              |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| CPE Testbed Development Initiated             | ✔    | 10/2015 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| CPE KSK Rollover Tests                        |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Systems Testing Plan Development Initiated    | ✔    | 10/2015 |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Systems Testing Plan Development              |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Systems Testing Plan Initiated                |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Systems Testing Plan Execution                |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Monitoring Plan Development Initiated         | ✔    | 3/2016  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Monitoring Plan Complete                      |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Monitoring Infrastructure Buildout Initiated   |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Monitoring Infrastructure Buildout            |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Monitoring                                    |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Backout Plan Development Initiated            | ✔    | 3/2016  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Backout Plan Development                      |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Operational Plan Development Initiated        | ✔    | 3/2016  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Operational Plan Development                  |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Generation of New KSK                         |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Insertion of New KSK                          |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Withdrawal of Old KSK                         |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Revocation of Old KSK                         |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| Removal of Old KSK                            |      |         |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |

Legend:
- **Not Yet Initiated**
- **Completed**
- **On Target**
- **Behind Schedule**
- **Intervention Required**
RDAP Support

What is RDAP?
Registry Data Access Protocol (RDAP) is a newly developed technical standard from the IETF that provides next generation access to registration data. It is intended to be a successor to the WHOIS protocol, but can run in parallel with existing WHOIS servers.

IANA’s Role
One of the features RDAP has over WHOIS is automatic discovery of RDAP servers. You no longer have to manually find where the right server is for the data you are looking up, the protocol will do this automatically. It does this by using “bootstrap registries” that are published as an IANA service.

What’s new
We have implemented bootstrap registries for IPv4, IPv6, AS numbers and Top-Level Domains. TLD Managers are now able to log into our Root Zone Management System to list their RDAP servers to appear in the bootstrap registry for the DNS.
RDAP Support

RDAP clients fetch bootstrap registry which lists known top-level RDAP servers

```
"services": [
  [[ "fou", "bar" ], [ "rdap.registrycorp" ]],
  [[ "baz", "rdap.baz.boop" ]], ...
]
```

Queries are fulfilled by connecting to RDAP servers listed in bootstrap registry

RDAP Bootstrap Registry

TLD’s RDAP Server
RDAP Support

`$ cdn-statistics --path /rdap --month 2016-03
/rdap/dns.json 1041
/rdap/ipv4.json 523
/rdap/asn.json 492
/rdap/ipv6.json 483
...
`
Stand up an RDAP server for the resources we maintain
- TLDs
- .INT and .ARPA domains
- High-level IPv4 and IPv6 allocations
- Multicast addresses
- Reserved allocations
Authorisation Model Evolution
Improving Authorisation – Why?

- Currently, each TLD has an administrative and technical contact; listed in WHOIS and both must cross-authorise change requests.
- Feedback and experience shows model is anachronistic.
  - Authorising function is preferrably by performed by people who are separate from “customer service” contacts TLD registries like to publish.
  - Increase in role accounts means IANA has trouble identifying people for purposes of out-of-band authentication.
  - Does not provide flexibility for different kinds of authorisation (m-of-n, etc.).
  - Does not provide for disabling less secure facets of model.
- Wish to implement multi-factor authentication.
  - Need recovery mechanisms. With many role accounts today it is hard to know who is behind them and who to allow to recover.
Proposed New Model

Current

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

Future?

Administrative Contact
1. Listed in public WHOIS
2. Public information only, not used for authorisation
3. Must be in country (ccTLDs)

Technical Contact
1. Listed in public WHOIS
2. Public information only, not used for authorisation

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?

Transition process
Improving Authorisation – Some Challenges

- Implementing technical changes behind a feature flag
- Need induction and migration process
  - "v1" (legacy) and "v2" (new) domains/contacts
- Strong identity controls (no role accounts)
- Are changes to authorisers/settings meta-changes or root zone changes?
- Clear rules for process of recovering credentials (store biographical data?)

Thanks. Timothy, can you confirm to me your complete first name on the account?

TIMOTHY
Timothy

Thank you for confirming the details. I got your account now.
Root Zone API Access
API access is a recurring request
Bulk operations is another recurring request
API access may solve both problems, giving a reasonable solution to bulk operations
Root Zone Change API

- REST-based API to perform same functions as web interface:
  - Lodge change requests
  - Review status
  - Submit authorizations
- Sandbox
- Bulk Updates
- Token-based Auth
Root Zone Change API — Some Issues

- Multiple changes in single CR?
  - How do you process changes that span multiple domains?
- RSP access?
Enable automated access to this account
This allows access to your account by software tools, to perform functions like bulk operations and checking status of requests without needing to manually view the website. Also known as API access.

Access Tokens

**Full Rights Access Token**
This token has the ability to perform all actions this account is empowered for. It is recommended this be used sparingly, as it will allow tools to both lodge and authorize change requests by this account.

9ae24762-164e-4f2e-b956-a5deb6628742

**Limited Access Access Token**
This token is able to lodge change requests and read status, but is not able to authorize change requests on behalf of this account. This is recommended for bulk update submissions.

fe118226-71eb-48f7-98a7-9812e78ad6f4

**Read-Only Access Token**
This token is able to see status of current and historical change requests, but cannot create requests, approve change requests, or otherwise make changes. This is recommended for tools that check request status.

@fead65f-6156-47d9-8007-9761081c0ba6

For instructions on how to use these tokens with automated tools, please read our Root Zone Management API documentation

- Requests for registry service provider access
- Graduated access control tokens?
Technical Check Evolution
Technical checks

- Revise technical checks
  - See last Jamboree!
- Allow for customer to opt-out of certain changes
- Provide improved communication of issues
  - Better error message reporting
  - Debug logging captures and visible via self-service
- Improved backend implementation (parallelism)
Other RZMS Work
Backend Improvements

- Automatic user provisioning
- Increased automation
- Technical check opt-outs
- Capture verbose logs for customer inspection
- Audit logging of all events for all accounts/domain for later review
Prioritisation

- Which of these are most/least valuable to you?
  - API for root zone change management
  - New authorisation model
  - Bulk update mechanism via web site
  - Technical check opt-outs
  - Multi-factor authentication for account
  - Audit logging
  - Others?

- Any recommendations/preferences on implementation details?
- Which implementation details do you want to review in detail?
Thank you!

Root Key Signing Ceremony 24
February 2016