.JP: DNSSEC key signing ceremony and the role of TCR

APTLD77 Members’ Updates
20 February 2020
Satsuki Hori @ Japan Registry Services (JPRS)
About me: Satsuki Hori (堀 五月)

• Working for JPRS as an engineer since 2012
  – Develop and Operate
    ➢ JP DNS server, M-Root server,
      JP domain name registry system
  – Plan and Participate
    ➢ JP DNSSEC key signing ceremony
• And will contribute to ICANN…
  – Selected as a Backup TCR
    (Trusted Community Representatives)

Please call me “Satsuki” :)

Copyright © 2020 Japan Registry Services Co., Ltd.
JP DNSSEC Practice Statement (JP DPS)

- It states ideas of policies and practices at JP zone

- JP DPS defines that the KSK (Key Signing Key) must be changed on an annual basis

JPRS holds “the key ceremony” every year
The “.jp DNSSEC Key Ceremony”

- Held in every October (per-year basis)
- Inviting two external witnesses
  - Witness A: selected from JP DNS joint operation organization
  - Witness B: selected from JP domain registrar
- The result is published on JPRS website (see below)

[Held in every October (per-year basis)]

[Holding in every October (per-year basis)]

[Inviting two external witnesses]

- Witness A: selected from JP DNS joint operation organization
- Witness B: selected from JP domain registrar

[The result is published on JPRS website (see below)]

### Our materials

[TEB (Tamper Evident Bag)]
- Sealed perfectly, and can be detected when opened

TEB has the unique ID

- [Smart card]
  - To store KSK
- [USB memory]
  - To store ZSK
  - It has physical authentication key

Store these materials into TEB

### Physical security in our ceremony

<table>
<thead>
<tr>
<th>Tier</th>
<th>Security Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1: Data center</td>
<td>Vein authentication, Baggage inspection</td>
</tr>
<tr>
<td>Tier 2: Server room</td>
<td>Vein authentication</td>
</tr>
<tr>
<td>Tier 3: Rack</td>
<td>Physical Key, Video monitoring</td>
</tr>
<tr>
<td>Tier 4: Safety box</td>
<td>Two keys (managed by two departments) required, Monitoring open/close</td>
</tr>
<tr>
<td>Tier 5: TEB</td>
<td>Ensure uniqueness and confidentiality</td>
</tr>
</tbody>
</table>
The role of TCR

• Composition and Roles
  – Active TCR
    ➢ Crypto Officers (COs): 14 people
      【Role of COs】
      • Store the key to open the safety box
      • Participate in the key signing ceremonies
    ➢ Recovery Key Share Holders (RKSHs): 7 people
      【Role of RKSHs】
      • Store the key to Decrypt a backup data of the KSK
      • Participate in the event of a catastrophe
  – Backup TCR
    ➢ Backup TCR: about 10 people (currently 8)
      【Role of Backup TCR】
      • Prepare to become an Active TCR
      • I don't know which role to play

I'm here now!
FYI: A proposal about future root zone KSK rollovers

- IANA is now working about future root zone KSK rollovers
  - Based on knowledge and experience of the first root zone KSK rollover (completed in 2019)

- Public comments invited from November 1 2019 to January 31 2020

Proposal for Future Root Zone KSK Rollovers

- I sent a public comment with Yoshiro YONEYA, my senior colleague of JPRS
  - Commented about the KSK life cycle and material appearance
Discussion / Comments

• How does your TLD operate DNSSEC?
  – Here are a few things to keep in mind..
    ➢ Key lifecycle
    ➢ Have a ceremony (or not)
    ➢ Invite external witnesses
    ➢ Publishing the result
    ➢ Materials (TEB, Smart card, USB memory, HSM..)
    ➢ Physical security

Any comments / input are welcome!