Key Management in JP

ICANN47 Durban
DNSSEC Workshop
17 July 2013
Shinta Sato <shinta@jprs.co.jp>
Outline

JPRS’s activities in DNSSEC Key management

- DPS
  - JP DPS
- Key management
  - KSK Ceremony in JP
  - ZSK Ceremony in JP

- Photos
DPS

DNSSEC Policy & Practice Statement

- Comparable to
  - Certification Practice Statement (CPS) from X.509 Certification Authority (CA)

- Established by KSK / ZSK Manager

- DNSSEC Key Ceremony
  - Generate key pairs (KSK / ZSK)
DPS - Overview -

1. Introduction
2. Publication and Repositories
3. Requirements for DNSSEC Practice
4. Facility, Management and Operational Controls
5. Technical Security Controls
6. Zone Signing
7. Compliance Audit
8. Legal Matters
JP DPS

Published on Jan 14, 2011
✓ https://jprs.jp/doc/dnssec/jp-dps-eng.html

Adopted then current DPS framework
✓ DNSSEC Policy & Practice Statement Framework
  • draft-ietf-dnsop-dnssec-dps-framework-05 (RFC 6841)

Key Management in JP
✓ KSK and ZSK Ceremony in accordance with JP DPS
KSK Ceremony in JP

- Once per year in Tokyo
  - held 3 times (2010, 2011, 2012)

- Operated by Trusted Persons
  - Key Activation Observers → JPRS x 2
  - Signing Key Operators → JPRS x 2
  - External Witnesses → Outside x 2

- Approx 5 hours
  - number of steps: 219
How to make KSK?

- HSM not used
  - originally designed software by JPRS

- KSK generated on RAMdisk of offline PC
  - generated KSK copied to 6 Smart Cards
    - 3 Cards per Locations
  - procedure
    - Generate × 1, Copy × 6, Remove × 1
Location of KSK

- In Safety-boxes
  - two geographically diverse locations

- Safety-box Specification
  - 2 physical keys
    - each key managed by different dept. in JPRS
      - Customer Services Dept. and Systems Dept.
  - Security Monitoring
    - door sensor
    - video monitoring / recording
ZSK Ceremony in JP

- Every 3 months in Tokyo
  - held 21 times

- Operated by Trusted Persons
  - Signing Key Operators → JRPS x 2
  - Key Activation Observers → JPRS x 2
  - Internal Witnesses → JPRS x 2

- Approx 4 hours
  - number of steps: 190
Sign & Transport DNSKEY RRset

- Sign DNSKEY RRset in Smart Card
  - KSK Private key NOT revealed outside

- Transport DNSKEYs and RRSIGs
  - using Encrypted USB Storage
Location of ZSK

- In Safety-boxes
  - two geographically diverse locations

- In JP Zone Management Server(s)
  - used to sign JP Zone for every 15 minutes
Key Management in JP - Overview -

{USB Storage(2), Smart Card (3), PC} × 2

JP Zone Management Server

Encrypts Storage

Transport

External/Internal Witnesses

Key Ceremony Check-Sheet

Operate KSK & ZSK on offline PC

Key Ceremonies

2 different SKO to access KSK

Signing Key Operator

+Key Activation Observer

2 different keys

Signing Key Operator

12Copyright © 2013 Japan Registry Services Co., Ltd.
Photos
Smart Cards & Reader

Encrypted USB Storages
Video Camera

Safety-box (custom-made)
KSK Ceremony Scripts on Oct 2012

Smart Card Size: 85.5 × 54.0 × 0.76mm