

# TH DNSSEC Implementation



Krit Witwiyaruj  
Thai Name Server Co., Ltd  
TH Registry

# TH Domains

- One Registry & One Registrar
  - Many Resellers
- 33,800 ASCII domains delegated on 3<sup>rd</sup> level domain name.
- 11,900 IDN domains under .th
- DNSSEC enable since April, 2009
  - 1 TLD and 2 SLD zones signed.



# Name Servers

- 1 Primary Name Server
  - Running ISC Bind 9.6.1-P1
- 5 Secondary Name Servers
  - 2 Servers in Thailand
    - Self manage, Thai Name Server Co., Ltd.
  - 3 Servers outside the country
    - RIPE NCC
    - ISC (SNS) <https://www.isc.org/solutions/sns>



# DNSSEC System Architecture

- **Key Store**
  - Store key information for signing zone
- **DS & DNSKEY Database**
  - Store DNSKEY and DS of delegated zone.
- **Key Admin Tools**
  - Create keys and rollover keys
- **DS Admin Tools**
  - Convert DNSKEY to DS
- **Zone Signer**
  - Create and Sign zones from registry DB



# TH zone keys

- Key algorithm

- RSA-SHA1 fixed

- Key size

- Adjustable per zone
  - Currently 2048 bits for KSK, 1024 bits for ZSK
  - Bigger ZSK size mean more memory require
    - For every parties, not only TLD



# Zone Signing

- Sign zone using BIND's dnssec-signzone
- Sign zone from newly created unsigned zone
- Takes about 45 sec. to sign the biggest zone
- Signed zone grow approx. 5 times in size
- Signature lifetime is one month
  - May be a little too long for production environment



# TH zone KSK Publication

- **ITAR (Interim Trust Anchor Repository)**
  - <https://itar.iana.org/anchors/>
- **ISC DLV (DNSSEC Look-aside Validation)**
  - <https://dlv.isc.org/>
- **THNIC Foundation**
  - On going development to provide public key of all delegated domain



# TH zone KSK Rollover

- Two KSKs with 1 year rollover period
  - An Active KSK (signing the key)
  - A pre-publish KSK
    - Published 1 year before becoming active
    - Published in ITAR so that trust anchor can be configure accordingly
    - If the root is signed this may be not needed
  - Start signing with the new key 1 month before rollover
    - Signing key with both KSKs



# TH zone ZSK Rollover

- Two ZSKs with 2 months rollover period
  - An Active ZSK (signing the zone)
  - A pre-publish ZSK
    - Published 2 months before becoming active
    - For using in case of emergency rollover
  - Only one ZSK will be used to sign the zone when rollover
    - Post-publish old ZSK for 3 day after the rollover
    - Then start introducing a new pre-publish ZSK



# Registration

- Delegated zone need to send in their public key
  - Keyset format only one key accepted
  - Registrar verify the key before submit data to the Registry
- Roll over key
  - Same process as register new key
- Cancel or remove the key
  - In case of key lost or changing provider
  - Send in request with a document to verify the ownership



# Registration Policies

- DNSKEY ready in the zone prior to registration
  - Also rollover the key
- Register the DNSKEY in keyset format
  - accept one key only
- Must use reliable DNSSEC signing nameserver
  - Resign zone before signature expire time
- Minimum KSK size 2048 bits



# Experience

- BIND 9 running smoothly so far
- Zone Signer stop once due to incorrect format RR miss taken input
- Resign zone is important RRSIG has expire time
  - Otherwise SERVFAIL



# Issues

- Very low number on interested parties
  - Introduce new costs
  - A lot of works to be learn and to be done
  - No hosting tools available
  - No support applications just yet
- Expectations of security
  - Keys are important thing to manage
- Not all provider or reseller support DNSSEC
  - Few properly understand DNSSEC
- Changing provider need to start over DNSSEC registration again



Thank You

