

# Update on DNSSEC implementation in .lk .இலங்கை and .இலங்கை domains



**Chamara Disanayake**

Manager Engineering

LK Domain Registry

[www.nic.lk](http://www.nic.lk)

# TLDS

- LK Domain Registry operates 3 top level domains
  - CCTLD
    - .lk
  - IDN ccTLD
    - ශ්‍රී ලංකා - (.lanka) .xn--fzc2c9e2c
    - இலங்கை - (.ilangai) .xn--xkc2al3hye2a



# Security in DNS

---

- Use TSIG for reliable zone transfer between DNS servers
- Enable DNSSEC and sign all zones



# Zone Signing Ceremony

- LK Domain Registry generated its KSKs and ZSK for all 3 domains
  - On 22<sup>nd</sup> June at LankaCom systems



# Zone Signing Ceremony

- Generated KSK and ZSK
- KSK public keys
  - Directors signed and the official embossed seal placed in the printed KSK
- Private keys of KSK encrypted and stored in external storage
  - Passwords are sealed and kept securely



# Used Parameters

---

- Key generation command `dnssec-keygen`
- Algorithm
  - RSASHA1
- `keysize`
  - 2048 for KSK
  - 1024 for ZSK



# KSK Public Keys

.lk KSK Public Key

.lanka KSK Public Key

```
; This is a key-signing key, keyid 64636, for xn--fzc2c9a2c
```

.ilankai KSK Public Key

```
; ; This is a key-signing key, keyid 41176, for xn--xkc2a13hye2a.
```

```
; ; Created: 20100622123546 (Tue Jun 22 18:05:46 2010)
```

```
; ; Publish: 20100622123546 (Tue Jun 22 18:05:46 2010)
```

```
; ; Activate: 20100622123546 (Tue Jun 22 18:05:46 2010)
```

```
/ xn--xkc2a13hye2a. IN DNSKEY 257 3 5
```

```
( AwEAAa4stTv1ZxVaYt2/ldrnz2iU6bZ1qVU8BYPqDqJy0YuH79nVSWA7
```

```
( 9TYLyqknYAnZF7A4tGtBI7INRKQmN+WrH1SZz05dtpHmzb6G8Z4KEOS1
```

```
c hDc4Cu7RHixJI/dozR8cMshS9ECOIH25uFWS7axjlgWWrItQA2329G7+
```

```
2 SCEJSUG8Q9yhtMWJEL9GaWUqbOD8NC5kWds6an/qXuirtgicUSm23B+6
```

```
D+vNqbxmojvqaIYTIPes1ejPrHcpAvV1CPxh9A1ZxC1q7EvawDsJnKEv
```

```
6rqurLCfp810i1T02OD7M11Qnu9ZuM4QzhSO6CkdpTrR4EA7VO885M/L 65+25AaKTwk=
```



# DS Records

- lk. IN DS 25545 5 1  
CB63D4EF5402447E2056972E436E771E745F7264
- lk. IN DS 25545 5 2  
AE81C6B6DD92E8C63EE1F4F6E3166AB0AE19BD3442029FA4B  
BC29614 2EBB3C7B
- xn--fzc2c9e2c. IN DS 883 5 1  
0D0DF43A6D818EFB1E9E7430712367BE4F6E0310
- xn--fzc2c9e2c. IN DS 883 5 2  
2367F554950F82CB1069E935406DF3B809C6F0CA2F560BB8C2  
8FC82B EF054DBD
- xn--xkc2al3hyc2a. IN DS 17356 5 1  
33E53FAD537B7C4AF2374DDC3A671F8FA7005653
- xn--xkc2al3hyc2a. IN DS 17356 5 2  
662ABF8F2E2CB223E0625C8A8D69AAB67B7916D8021290DC18  
79B1BF 125721A8



# Issues with DNSSEC

- Zone file size and bandwidth
  - 8~10 times of unsigned zone file
  - Since zone file is generated using backend DB entire zone has to be resigned
  - Can not use IXFR
- NSEC record
  - Anyone can get the entire zone



# DNSSEC Future at LK

- Submit DS records of .lk and IDN cctlds to ICANN
- Enable customers to submit their DS records securely
- Use NSEC3 and its features
- Public awareness programs, workshops



# Thank You

---

**chamara@nic.lk**

