.hk DNSSEC deployment experience & ICANN Root key (KSK) rollover

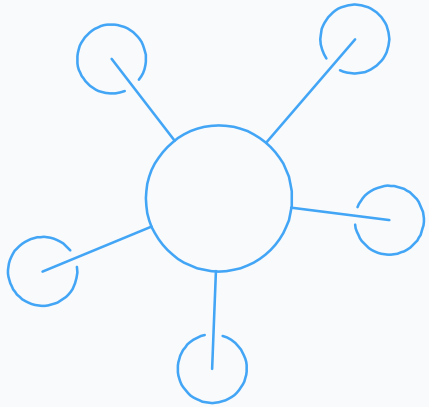
Ben Lee – Head of IT

15 Sep 2017

Background

- HKIRC is a not-for-profit company limited by guarantee set up in December 2001, and designated by the Government of the HKSAR to manage and administer all Internet domain names under .hk and .香港 country-code top level domain names
- As of 1 Sep 2017, the total registration of .hk and .香港 domain names

279,263



About me

- **Ben Lee**, Head of IT, HKIRC
  - also has the role of Information Security Officer
  - manages the technical and security of .hk and .香港 country code top level domain name (ccTLD)
  - has 15 years of experience in the domain name industry
  - actively participates in the Internet community of the region, e.g. CDNC and APTLD

What is DNSSEC ?

- DNS was designed and implemented for more than a decade ago. However, there have been concerns about the trustworthiness of data in the DNS
- With DNSSEC, it can conduct data origin authentication and ensure data integrity through the Key Pairs and Digital Signatures technologies.

Who need DNSSEC ?

DNSSEC affects every component within the Internet infrastructure ecosystem:

- Registries, registrars, domain name registrants, hardware and software vendors, ISPs, government departments and related parties
- Typical industries with higher risk of being attacked and spoofed by cyber criminals , including financials, e-commerce, Internet infrastructure providers, or for those who collect login credentials, or privacy data, or websites with high traffic

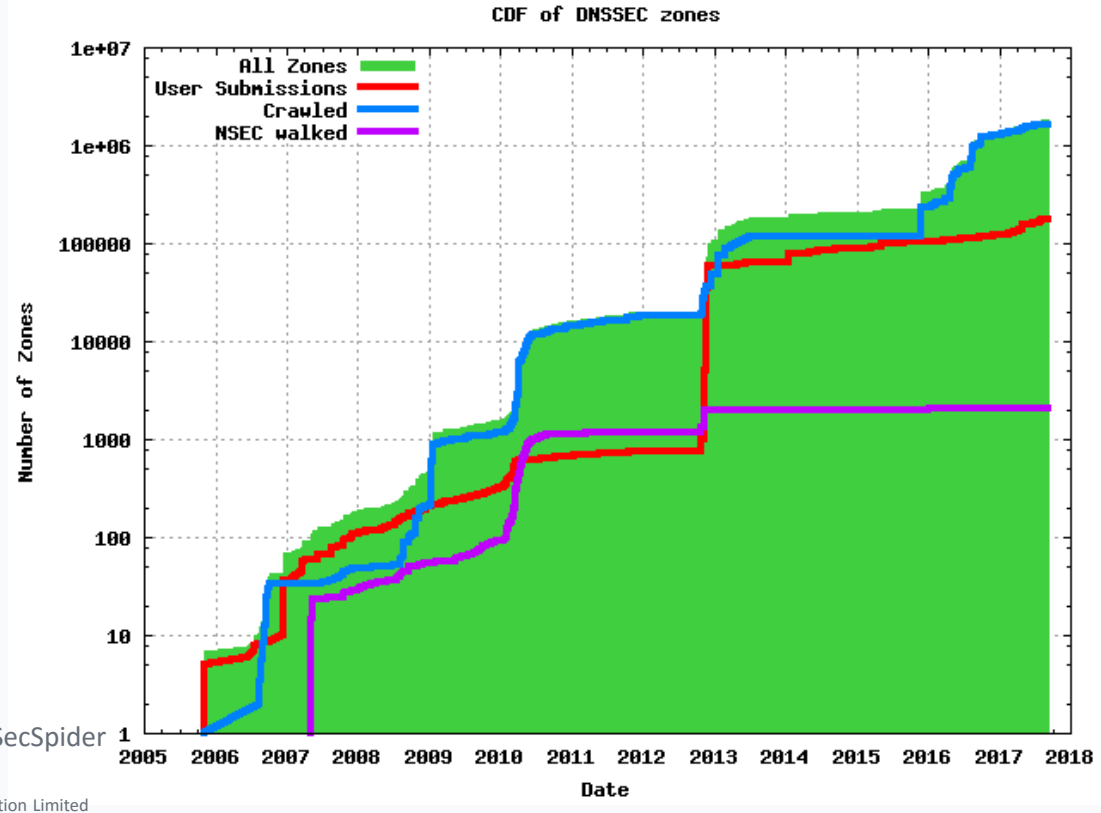
Key Benefits of using DNSSEC ?

1. Provide an extra level of security to improve **reliability**, **trustworthy** and **quality** of the DNS
2. Help ensure Internet users will be directed to the website or service they expect when entering a domain name into their browser
3. Safeguard the Internet environment and strengthen trust in the Internet as a whole

Benefits to Stakeholders

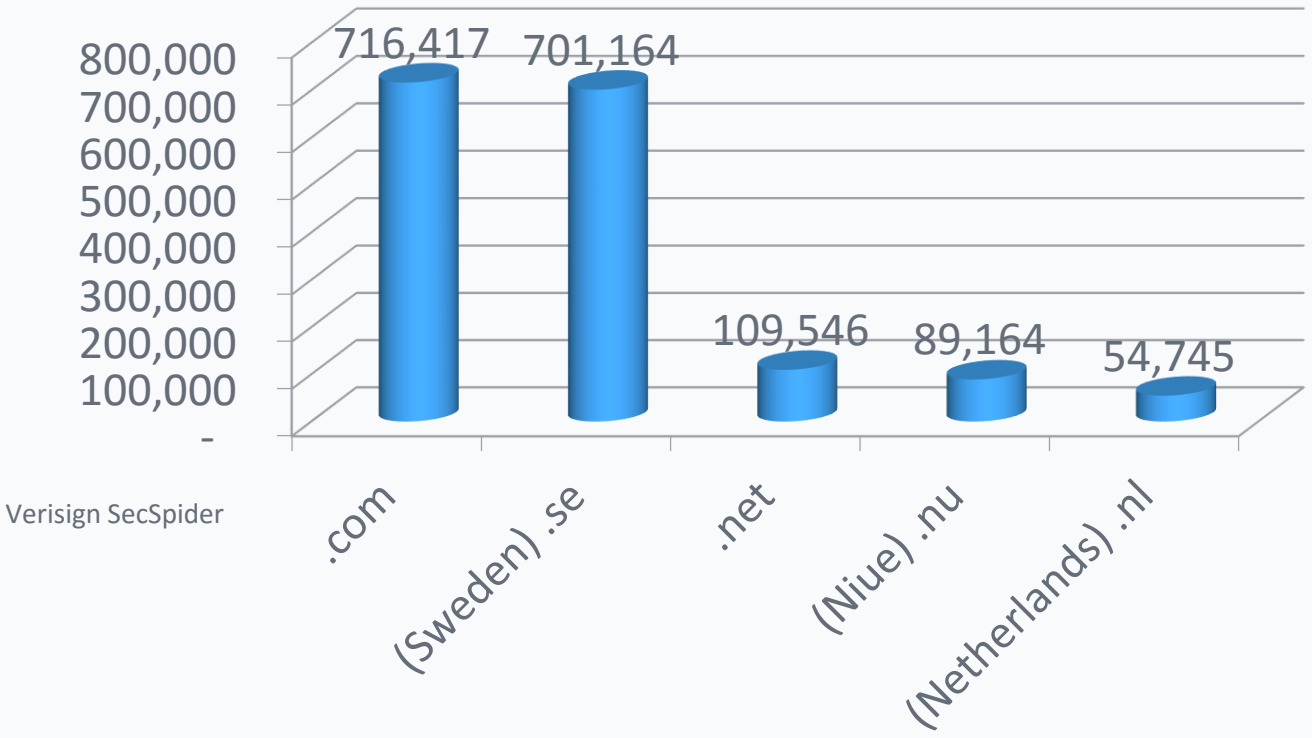
The Internet community	Registrars, DNS hosting providers	Website owners	ISPs
• Enjoying improved security in the zones that are signed, reducing cyber crimes by fake websites.	• Allowing party to offer domain signing services to their customers.	• Increasing the security of the data returned to their customers.	• Allowing their customers to verify domain names and corresponding IP addresses, reducing the security concerns generated from cyber attacks (e.g. man-in-the-middle)

Internet DNSSEC Signed Zones: 1,808,293



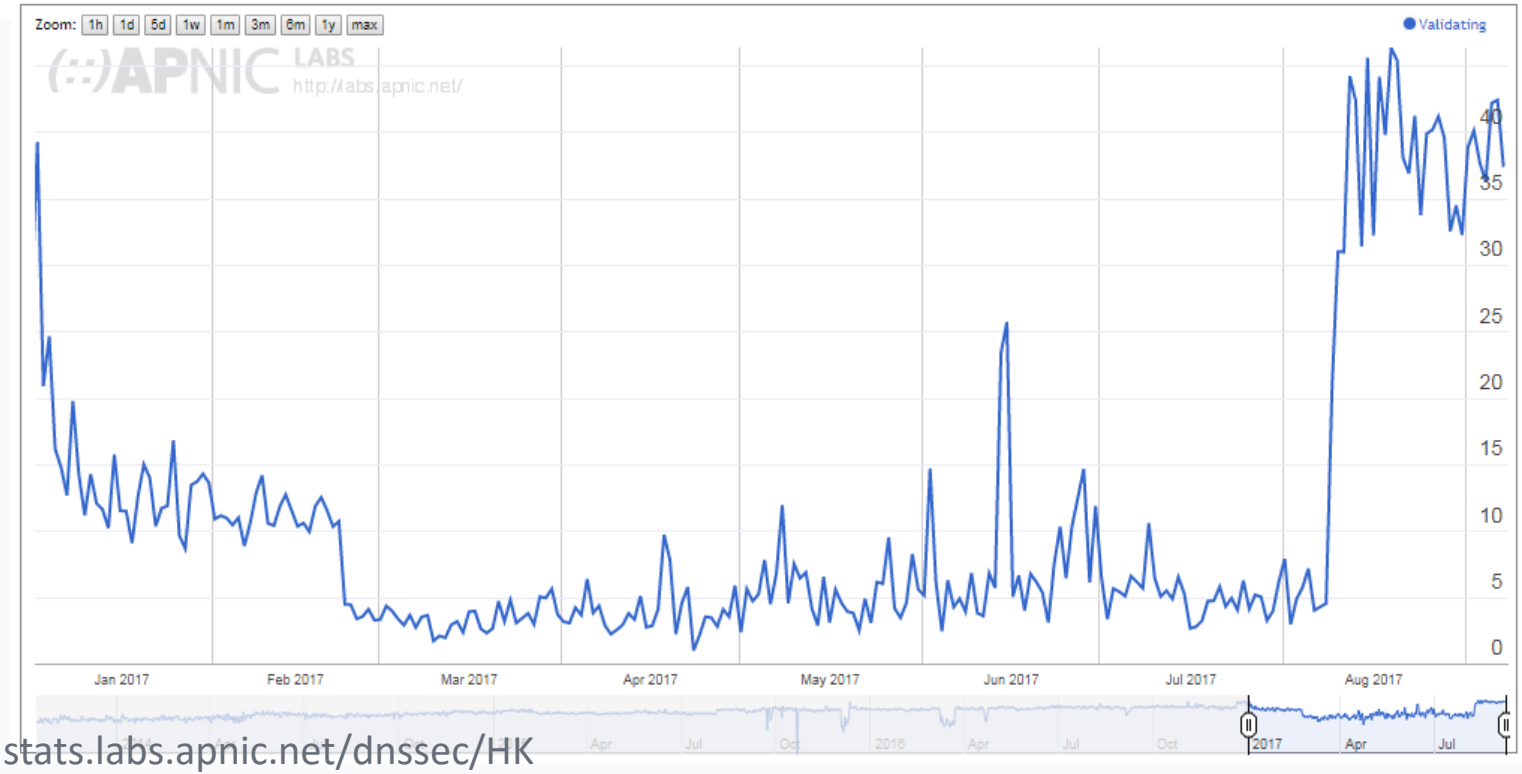
Verisign SecSpider

DNSSEC
Signed Zones



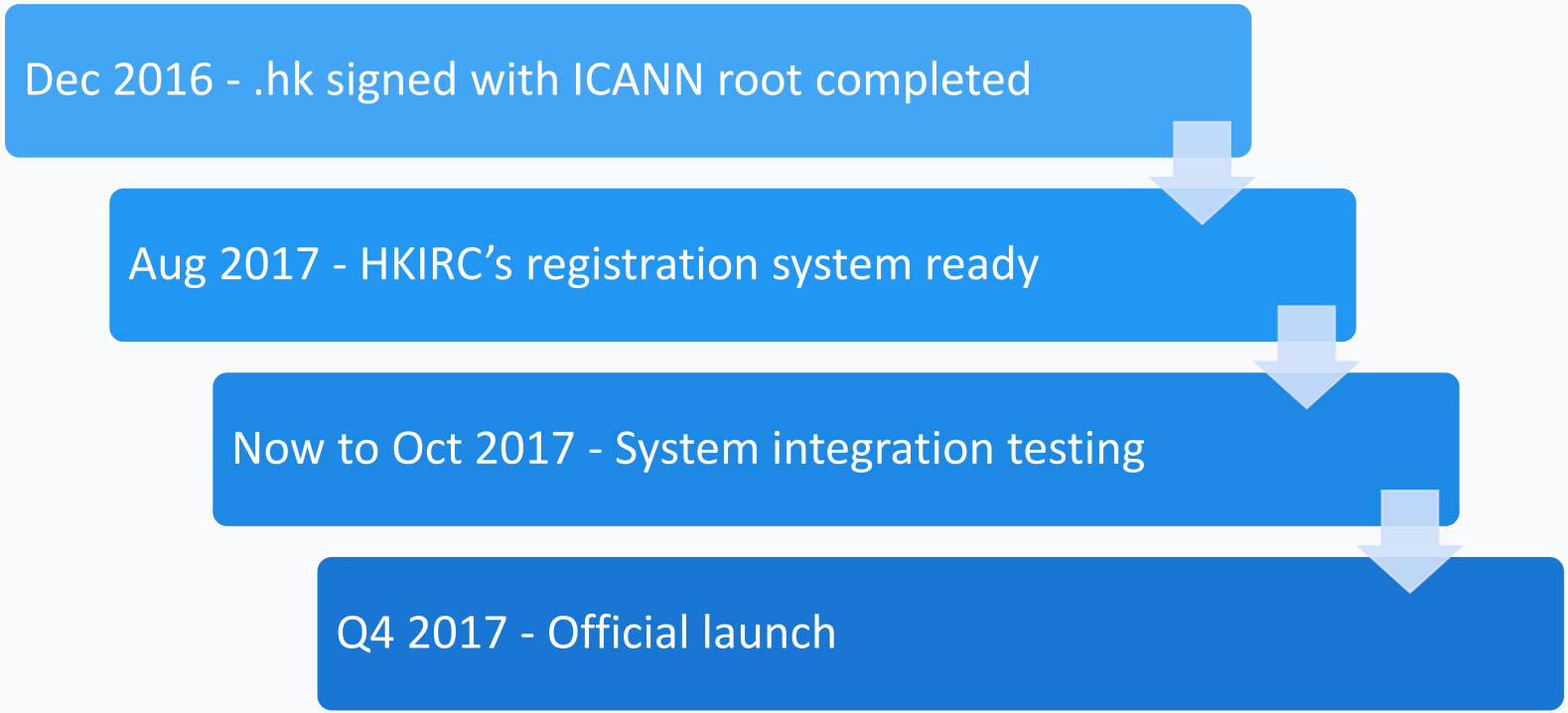
Verisign SecSpider

DNSSEC Validating Traffic in HK (average 17.27%)



stats.labs.apnic.net/dnssec/HK

HKIRC DNSSEC Deployment Timeline



What need to be done to enable DNSSEC?

DNS Hosting

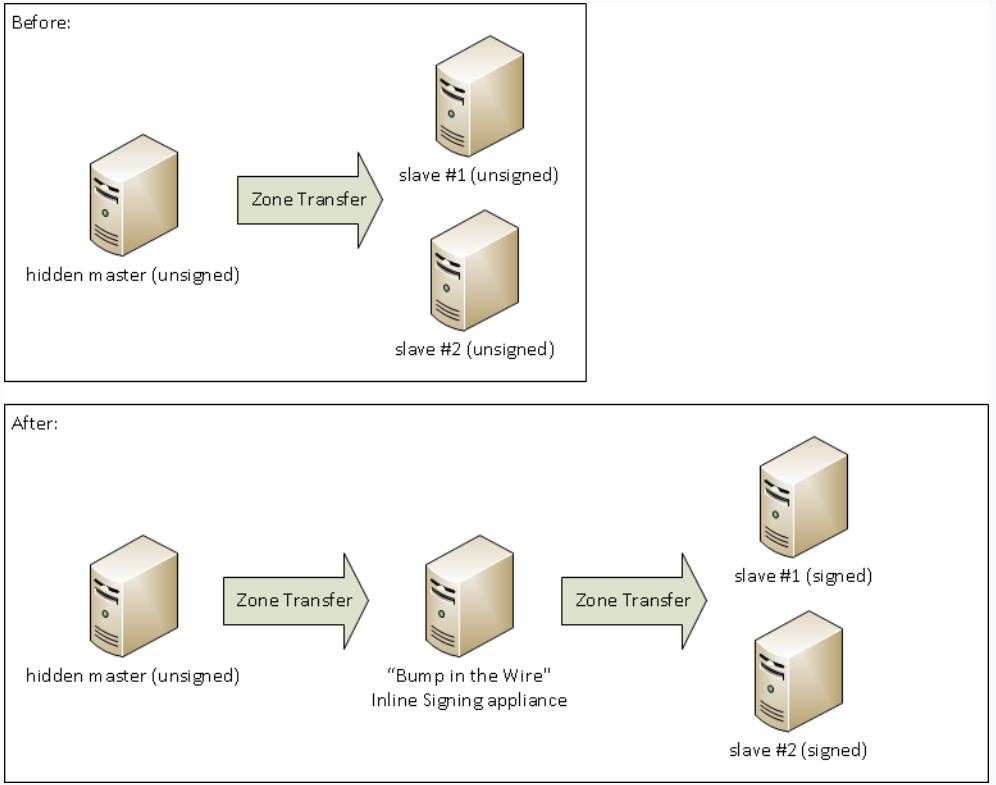
- Digitally sign domain names in name servers
- Build DNSSEC “chain-of-trust” - by submitting your public key info (DS) to parent zone

Internet Access

- Enable DNSSEC validation in DNS resolvers
- Ready for the ICANN KSK rollover on 11 Oct 2017 - by installing both old and new keys

DNS Hosting Service – DNSSEC Signing Architecture

- Method 1:
- “Bump in the Wire”



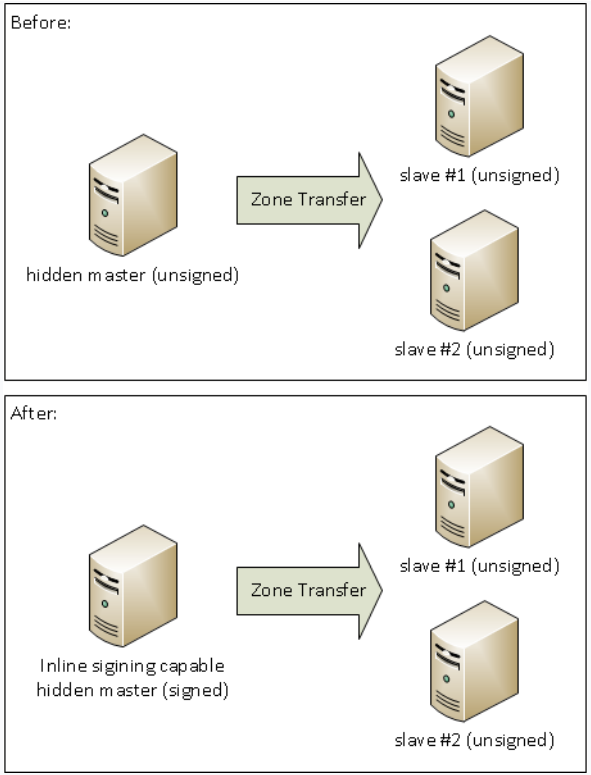
Method 1: “Bump in the Wire”

- The **Good** thing is:
  - As the signing process is separated from master, no (or only very little) change business logic on zone management are need to adjust in masters.
  - Also separated signing unit help archive higher level security (when use of HSM), availability (when using HA) and flexibility (switching signing appliance)

- The **Bad** thing is:
  - You need to manage new devices (the signer) and zones hosted inside.
  - Amendments on zone transfer setting are required (on hidden master, signer and slaves).

DNS Hosting Service - DNSSEC Signing Architecture

- Method 2:
- Master Server



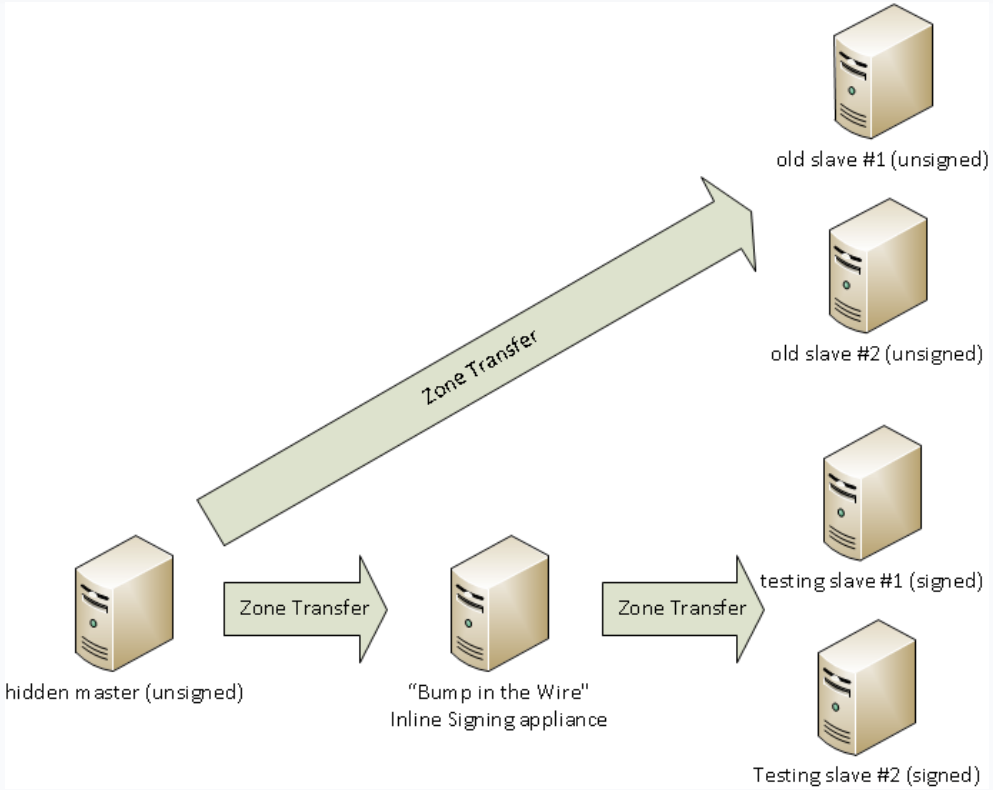
Method 2: Master Server

- The **Good** thing is:
  - No additional device/unit required.
  - Zone transfer settings remain unchanged.

- The **Bad** thing is:
  - Only limited choices of master name servers with signing ability.
  - DNSSEC signed zone requires periodic re-signing, which is a cryptographic function that is CPU intensive. If your DNS zone is dynamic or changes frequently, it also adds to higher CPU loads on your master.
  - If higher security is preferable, you may want to use HSM to protect DNSSEC keys (KSK, ZSK). Master must be capable to make use of HSM stored DNSSEC keys (say support PKCS #11).

HKIRC Approach and Testing

- "Bump in the Wire“
- Allows higher flexibility, manageability, security and availability.



DNSSEC Parameter Values

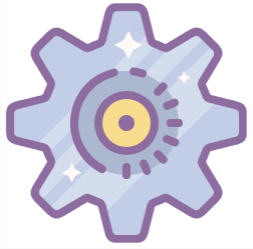
- E.g. KSK / ZSK key algorithm, length, rollover frequency

HKIRC's DNSSEC enabling guide

- RFC6781 - DNSSEC Operational Practices, Version 2: https://tools.ietf.org/rfc/rfc6781.txt
- NIST, Secure Domain Name System (DNS) Deployment Guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
- DNSSEC Operations: Setting the Parameters: http://www.dnssec-deployment.org/wp-content/uploads/sites/2/2012/02/Setting-the-Parameters-20091124032.pdf

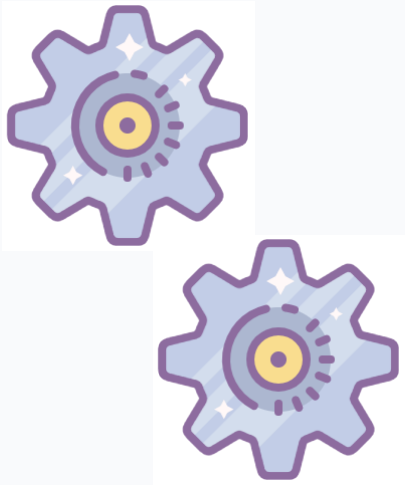
Example Parameters 1

Parameter	Example value from .hk zone
KSK Algorithm	**8 (RSA/SHA256)**
KSK Key Length	**2048 bit**
KSK DNSKEY TTL	1 day
Publish DNSKEY of standby KSK	yes
KSK Keyroll Frequency	**yearly**
KSK Keyroll Mechanism	Double Signature Rollover Method
ZSK Algorithm	**8 (RSA/SHA256)**
ZSK Key Length	**1024 bit**
ZSK DNSKEY TTL	1 day
Publish DNSKEY of standby ZSK	yes
ZSK Keyroll Frequency	**monthly**
ZSK Keyroll Mechanism	Pre-publish Rollover Method



Example parameters 2

Authenticated Denial of Existence	**NSEC3**
NSEC3PARAM Hash Algorithm	1 (SHA-1)
NSEC3PARAM Opt-Out flag	0 (clear, use Opt-Out)
NSEC3PARAM Iterations	10
NSEC3PARAM Salt	Used
NSEC3 TTL	1 day
NSEC3PARAM TTL	15 min
SOA TTL	15 min
SOA Refresh	30 min
SOA Retry	15 min
SOA Expire	14 days
SOA Minimum	1 day
RRSIG TTL	Follow RR
RRSIG Signature Validity Period	30 days
RRSIG Signature Re-signing Frequency	**daily**
Public DS of KSK with 2 algorithms	yes



Building the Chain of Trust with Parent DNS Zone

- After the signing of domain names, remember to …
  - **Update your DS records to parent zone through your domain name registrar.**

Performance Figure – Before and After

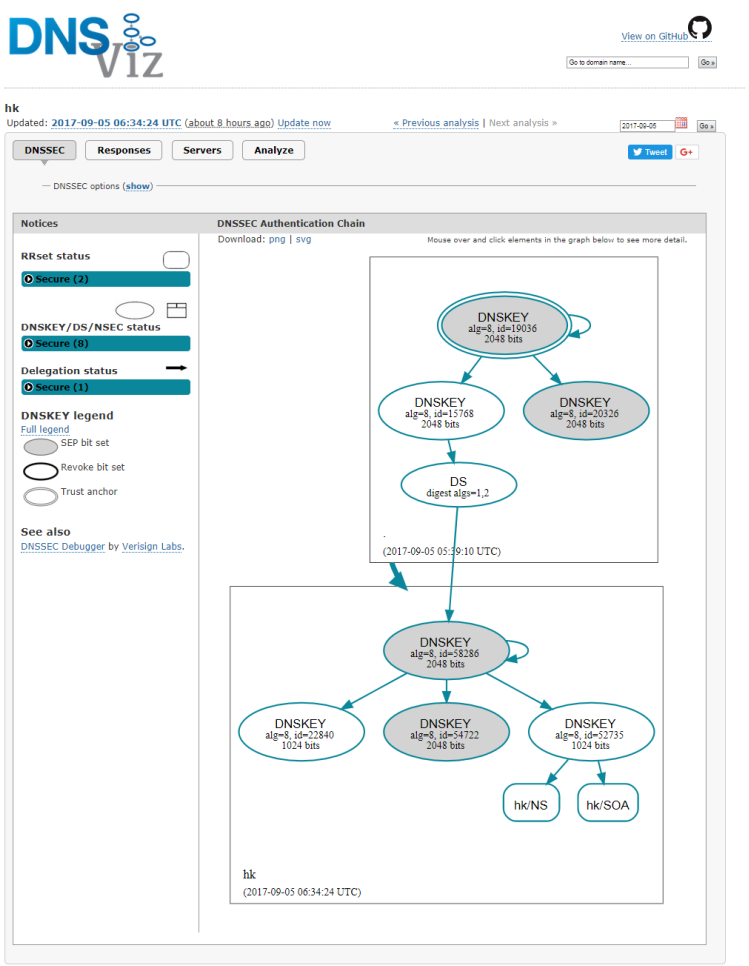
- Volume of Query (QPS) - increase of **6%**
- Volume of Response traffic (Packet size) – increased **6x**
- TCP queries – from nearly nothing to small amount

- Some studies says: Provision for the growth
  - Volume of query : **2 to 4 times**
  - Volume of response traffic: **10 to 15 times**

- Consider
  - Deploy by batch - DNS zone by zone
  - Keep monitor the performance

DNSSEC Signing – Testing Tools

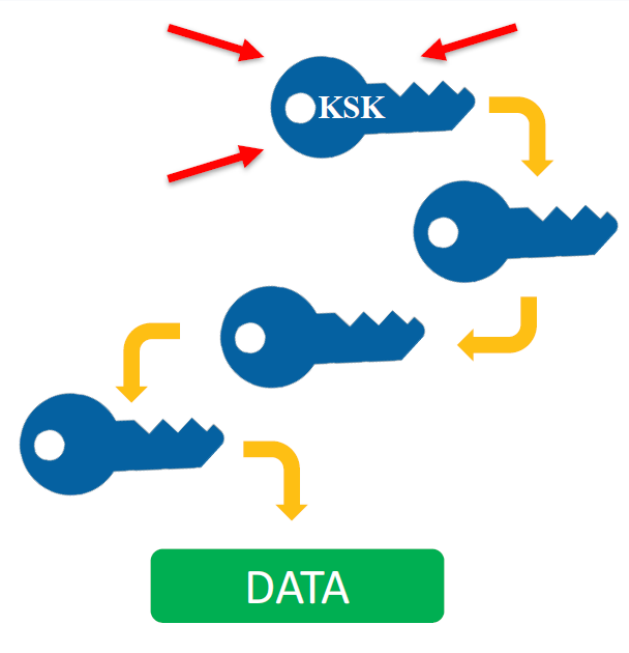
- Web tools to check DNSSEC signing:
  - http://dnssec-debugger.verisignlabs.com
  - http://dnsviz.net
  - https://internet.nl/
  - https://www.zonemaster.fr



- Before we talk about how to Enable DNSSEC Validation in DNS resolver ……
- What is Root Zone DNSSEC KSK?
- And it is being rollover?

The Root Zone DNSSEC KSK

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy
- Public portion of the KSK is configuration parameter in DNS validating revolvers



“Rollover” of the Root Zone DNSSEC KSK

- **There has been one functional, operational Root Zone DNSSEC KSK**
  - Called “**KSK-2010”** key tag: **19036**
  - Since 2010, nothing before that
- **A new KSK has been put into production this year**
  - Call it “**KSK-2017”** key tag: **20326**
  - An orderly succession for continued smooth operations

```
>dig . DNSKEY
;; ANSWER SECTION:
86396 IN DNSKEY 257 3 8 (
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh
/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXp
oY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGO
Yl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
) ; KSK; alg = RSASHA256 ; key id = 19036
86396 IN DNSKEY 257 3 8 (
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN
7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8
efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY
A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
) ; KSK; alg = RSASHA256 ; key id = 20326
```

ICANN New KSK-2017 Schedule

Enable DNSSEC Validation in DNS Resolver

- Method 1: Configure and use BIND built-in managed-keys
- All versions of BIND since April 2017 (i.e. 9.9.10, 9.10.5, 9.11.1 and later) include a hard-coded copy of the new root KSK

```
options {
        ...
        dnssec-validation auto;
        ...
};
```

- RFC 5011 - automated updates of DNSSEC trust anchors

Enable DNSSEC Validation in DNS Resolver

- Method 2: Configure and use custom managed-keys in named.conf

```
options {
        ...
        dnssec-validation yes;
        ...
};

managed-keys {
# This KSK-2010 key (19036)
. initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=";
# This KSK-2017 key (20326)
. initial-key 257 3 8
"AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
R1AkUTV74bU=";
};
```

DNSSEC Validation Deployment and Testing

- Multiple resolvers? Turn on validation one-by-one and monitor the effect
- HKIRC had set up 3 examples aiming to facilitate you to test your DNSSEC resolvers show as below:

State	Testing Domain	Explanations
Insecure	**disabled.dnssec.hkirc.hk**	not DNSSEC enabled
Secure	**enabled.dnssec.hkirc.hk**	DNSSEC enabled and verification is successful
Bogus	**failed.dnssec.hkirc.hk**	DNSSEC enabled and verification is failed

Root Zone KSK Rollover Go Live on 11 Oct 2017

- What to do……
- Before 11 Oct 2017 Deadline
  - DNSSEC validating resolver – ready the New Root Zone KSK and check
  - Automated update (RFC5011) or Manual setup
- On 11 Oct 2017
  - Keep watch and standby for the unexpected
  - OK to turn off DNSSEC validation while you fix (but do turn it back on!)
- Monitor the ICANN timeline (any schedule change?)
  - https://www.icann.org/resources/pages/ksk-rollover/
  - https://automated-ksk-test.research.icann.org/
  - https://www.icann.org/dns-resolvers-checking-current-trust-anchors
  - https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

Let's deploy DNSSEC!

1. Sign domain names
2. Setup Chain of Trust (submit DS records)
3. Enable DNSSEC validation
4. Ready New Root zone KSK by 11 Oct 2017
5. Test before deployment

- Collaborate, welcome to test together
- Marketing co-operation are welcome
- **Build a more secure Hong Kong Internet**

Q & A

For icons in this slide - Link to Icons8

KEEP IN TOUCH

Email

info@hkirc.hk

finance@hkirc.hk

marketing@hkirc.hk

www.hkirc.hk

Phone

P : (852) 2319 2303

F : (852) 2319 2626

Address

Unit 501, Level 5, Core C,

Cyberport 3, 100 Cyberport

Road, Hong Kong