DNSSEC Implementation
Considerations and Risk Analysis

ENOG 12 Yerevan, Armenia Oct 2016
richard.lamb@icann.org
DNS is a part of all IT ecosystems (much more than one expects)
The Problem: DNS Cache Poisoning Attack

www.majorbank.se = ?
5.6.7.8

DNS Resolver

DNS Server

www.majorbank.se = 1.2.3.4

Attacker

www.majorbank.se = 5.6.7.8

Attacker webserver

www @ 5.6.7.8

Password database

Get page
Login page

Username / Password
Error
The Bad: DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4M machines, 100 countries, $14M

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse websites, send email, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

Securing it

- DNS converts names (www.bnrcr.fi.cr) to numbers (201.220.29.26)
- Make sure we get the right numbers (DNSSEC)
- Verify the identity and encrypt data
The Bad: Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – “Iranian cyber army”
- 13 Aug 2010 - Chinese gmail phishing attack
- 25 Dec 2010 Tunisia DNS Hijack
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

*A Brief History of DNS Hijacking - Google
The Business Case for DNSSEC

• Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.

• DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

• DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.
DNSSEC interest from governments

- Sweden, Brazil, Netherlands, Czech Republic and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC. “A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,”[2].
- 2008 US .gov mandate. 85% operational. [3]

http://fedv6-deployment.antd.nist.gov/snap-all.html
Thank you Geoff Huston
DNSSEC - Where we are

- Deployed on 1340/1500 TLDs (2 Oct 2016 .am .in .af .tm .kg .cn .se .de .ru .pф .com .uk .nl .fr .in .us .my مليسيا .asia .tw 台湾, .kr 한국 .net, .org, .post, +ntlds, .ibm .berlin)
- Root signed** and audited
- > 89% of domain names could have DNSSEC
- Required in new gTLDs. Basic support by ICANN registrars
- Growing ISP support* - ~16% end users “validate”.
- 3rd party signing solutions***
- S/W H/W support: NLNetLabs, ISC, Microsoft, PowerDNS,KNOT, Secure64...? openssl, postfix, XMPP, mozilla: early DANE support
- IETF standard on DNSSEC TLS certificates (RFC6698) and others
- Growing support from major players...(Apple iPhone/iPad, Google 8.8.8.8, hosting co Cloudflare DNSSEC by default, German email providers...)

Stats: https://rick.eng.br/dnssecstat/
* COMCAST /w 20M and others; most ISPs in SE ,CZ.
**Int’l bottom-up trust model /w 21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ.
*** Partial list of registrars: https://www.icann.org/en/news/in-focus/dnssec/deployment
But...

• But deployed on only ~3% of 2\textsuperscript{nd} level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*, comcast.com).

• DNSChanger and other attacks highlight today’s need. (e.g end-2-end DNSSEC validation would have avoided the problems)

• Innovative security solutions (e.g., DANE) highlight tomorrow’s value.

DNSSEC: So what’s the problem?

• Not enough IT departments know about it or are too busy putting out other security fires.

• When they do look into it they hear old stories of FUD and lack of turnkey solutions and CDN support.

• Registrars*/CDNs/DNS providers see no demand leading to “chicken-and-egg” problems.

*but required by new ICANN registrar agreement
DNSSEC: A Global Platform for Innovation or.. I* $mell opportunity !
Game changing Internet Core Infrastructure Upgrade

• “More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. ..” – Vint Cerf (June 2010)
For Techies and other Dreamers
Too many CAs. Which one can we trust? DNSSEC to the rescue....

CA Certificate roots ~1482
Symantec, Thawte, Godaddy

DNSSEC root - 1

Internet of Things
IoT

Content security
Commercial SSL
Certificates for
Web and e-mail

DANE and other yet to be
discovered security
innovations, enhancements,
and synergies

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility” DANE

Crypto currencies
and e-commerce?

E-mail security SMIME,
DKIM RFC4871

Cross-
organizational and
trans-national
authentication and
security

Securing VoIP

Domain Names

Login security
SSHFP RFC4255

https://www.eff.org/observatory
Opportunity: New Security Solutions

- Improved Web SSL and certificates for all*
- Secured e-mail (SMTP+S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational authentication, security
- Secured content delivery (e.g. configurations, updates, keys) – Internet of Things
- Securing Smart Grid efforts
- Increasing trust in e-commerce
- Securing cryptocurrencies and other new models
- First global FREE PKI

A good ref: 
http://www.internetsociety.org/deploy360/dnssec/

*IETF standards complete and more currently being developed
DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.
DNSSEC: We have passed the point of no return

- Fast pace of deployment at the TLD level
- Deployed at root
- Supported by software
- Growing support by ISPs
- Required by new gTLDs

→ Inevitable widespread deployment across core Internet infrastructure
Design Considerations
How do I sign a zone?
That's it

dnssec-signzone mydomain.zone mydomain.zone.signed

www.abc.com. IN A 192.101.186.125

www.abc.com. IN A 192.101.186.125
IN RRSIG A 8 3 3600
20130926030000 20130909030000 32799
www.abc.com.
N7upFHNplnIiXAEMOTefeujrwymNxF 8D6/
poaorvdthhvoxniaij2wugvbCGvUMjayDhVnK9vAq
tvhuiAnxzxsIIP4ZbtIgtz/
hbTKByySx1Y0u9aRD1ik=
One way to do this

nameserver
mydomain.zone

signer
mydomain.zone

keys

mydomain.zone.signed
or...another

It’s a question of risk / trust, but is does not have to be expensive
Goals

• Reliable
• Trusted
• Cost Effective (for you)
Reliable

• Keep design simple
• Monitoring – DNSSEC is time sensitive!
• People – develop checklists and documentation
Cost Effectiveness
Cost Effectiveness

• Risk Assessment
• Cost Benefit Analysis
Business Benefits and Motivation
(from “The Costs of DNSSEC Deployment” ENISA report)

- Become a reliable source of trust and boost market share and/or reputation of zones;
- Lead by example and stimulate parties further down in the chain to adopt DNSSEC;
- Earn recognition in the DNS community and share knowledge with TLD’s and others;
- Provide assurance to end-user that domain name services are reliable and trustworthy;
- Look forward to increasing adoption rate when revenue is an important driver. Deploying DNSSEC can be profitable;
Risk Assessment

• Identify your risks
  – Reputational
    – Competition
    – Loss of contract
  – Legal / Financial
    – Who is the relying party?
    – SLA
    – Law suits

• Build your risk profile
  – Determine your acceptable level of risk
Vulnerabilities

• False expectations
• Key compromise
• Signer compromise
• Zone file compromise
Cost Benefit Analysis

Setting reasonable expectations means it doesn’t have to be expensive
From ENISA Report

• “....organizations considering implementing DNSSEC can greatly benefit from the work performed by the pioneers and early adopters.”

• Few above 266240 Euros: Big Spenders: DNSSEC as an excuse to upgrade all infrastructure; embrace increased responsibility and trust through better governance.

• Most below 36059 Euros: Big Savers: reuse existing infrastructure. Do minimum.
Anticipated Capital and Operating Expense

- Being a trust anchor requires mature business processes, especially in key management;
- Investment cost also depends on strategic positioning towards DNSSEC: leaders pay the bill, followers can limit their investment;
- Financial cost might not outweigh the financial benefits. Prepare to write off the financial investment over 3 to 5 years, needed to gear up end-user equipment with DNSSEC.
Other Cost Analysis

• People
  – Swedebank – half a FTE
  – Occasional shared duties for others

• Facilities
  – Datacenter space
  – Safe ~ $100 - $14000

• Crypto Equip ~ $5-$40000

• Bandwidth ~ 4 x

Trusted
Trust

- Transparent
- Secure
Transparency
Transparency

• The power of truth
  • Transparency floats all boats here

• Say what you do

• Do what you say

• Prove it
Say what you do

- Setting expectations
- Document what you do and how you do it
- Maintain up to date documentation
- Define Organization Roles and responsibilities
- Describe Services, facilities, system, processes, parameters
Learn from CA successes (and mistakes)

• The good:
  – The people
  – The mindset
  – The practices
  – The legal framework
  – The audit against international accounting and technical standards

• The bad:
  – Diluted trust with a race to the bottom (>1400 CA’s)
  – DigiNotar
    • Weak and inconsistent polices and controls
    • Lack of compromise notification (non-transparent)
    • Audits don’t solve everything (ETSI audit)
Say What You Do - Learn from Existing Trust Services

• Borrow many practices from SSL Certification Authorities (CA)
  • Published Certificate Practices Statements (CPS)
    – VeriSign, GoDaddy, etc..
  • Documented Policy and Practices (e.g., key management ceremony, audit materials, emergency procedures, contingency planning, lost facilities, etc...)
Say What You Do - DNSSEC Practices Statement

• DNSSEC Policy/Practices Statement (DPS)
  – Drawn from SSL CA CPS
  – Provides a level of assurance and transparency to the stakeholders relying on the security of the operations.
  – Regular re-assessment
  – Management signoff
    • Formalize - Policy Management Authority (PMA)
Documentation - Root

91 Pages and tree of other documents!

Root DPS
Documentation - .SE

22 pages, Creative Commons License!
Do what you say

• Follow documented procedures / checklists
• Maintain logs, records and reports of each action, including incidents.
• Critical operations at Key Ceremonies
  – Video
  – Logged
  – Witnessed
Key Ceremony

A filmed and audited process carefully scripted for maximum transparency at which cryptographic key material is generated or used.
Prove it

• Audits
  – 3rd party auditor $$
  – ISO 27000 $$ etc..
  – Internal
Prove it - Audit Material

- Key Ceremony Scripts
- Access Control System logs
- Facility, Room, Safe logs
- Video
- Annual Inventory
- Logs from other Compensating Controls
- Incident Reports
Prove it

• Stakeholder Involvement
  – Publish updated material and reports
  – Participation, e.g. External Witnesses from
    – local Internet community
    – Government
  – Listen to Feedback
Prove it

• Be Responsible
  – Executive Level Involvement
    • In policies via Policy Management Authority
    • Key Ceremony participation
Security
Building in security

• Getting the machinery for DNSSEC is easy (BIND, NSD/Unbound, OpenDNSSEC, etc..).

• Finding good security practices to run it is not.
Security

• Physical
• Logical
• Crypto
Physical

– Environmental
– Tiers
– Access Control
– Intrusion Detection
– Disaster Recovery
Physical - Environmental

• Based on your risk profile
• Suitable
  – Power
  – Air Conditioning
• Protection from
  – Flooding
  – Fire
  – Earthquake
Physical - Tiers

• Each tier should be successively harder to penetrate than the last
  – Facility
  – Cage/Room
  – Rack
  – Safe
  – System

• Think of concentric boxes
Physical - Tier Construction

• Base on your risk profile and regulations
• Facility design and physical security on
  – Other experience
  – DCID 6/9
  – NIST 800-53 and related documents
  – Safe / container standards
Physical – Safe Tier
Physical – Safe Tier
Physical – Tamper Evident Packaging
Physical - Access Control

• Base on your risk profile

• Access Control System
  – Logs of entry/exit
  – Dual occupancy / Anti-passback
  – Allow Emergency Access

• High Security: Control physical access to system independent of physical access controls for the facility
Physical - Intrusion Detection

• Intrusion Detection System
  – Sensors
  – Motion
  – Camera

• Tamper Evident Safes and Packaging

• Tamper Proof Equipment
Physical - Disaster Recovery

• Multiple sites
  – Mirror
  – Backup

• Geographical and Vendor diversity
Logical

• Authentication (passwords, PINs)
• Multi-Party controls
Logical - Authentication

- **Procedural:**
  - REAL passwords
  - Forced regular updates
  - Out-of-band checks

- **Hardware:**
  - Two-factor authentication
  - Smart cards (cryptographic)
Logical - Multi-Party Control

• Split Control / Separation of Duties
  – E.g., Security Officer and System Admin and Safe Controller

• M-of-N
  – Built in equipment (e.g. HSM)
  – Procedural: Split PIN
  – Bolt-On: Split key (Shamir, e.g. ssss.c)
Crypto

• Algorithms / Key Length
• Crypto Hardware
Crypto - Algorithms / Key Length

- Factors in selection
  - Cryptanalysis
  - Regulations
  - Network limitations
## Crypto - Key Length

- Cryptanalysis from NIST: **2048 bit RSA SHA256**

<table>
<thead>
<tr>
<th>Year</th>
<th>Min. Bit Strength</th>
<th>Algorithm Suites</th>
<th>Key Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Now-&gt;2010</td>
<td>80</td>
<td>DSA/SHA-1, RSA/SHA-1</td>
<td>Both: 1024 bits</td>
</tr>
<tr>
<td>2010-&gt;2029</td>
<td>112</td>
<td>DSA/SHA-256, RSA/SHA-256</td>
<td>Both: 2048 bits</td>
</tr>
<tr>
<td>2030 and Beyond</td>
<td>128</td>
<td>DSA/SHA-256, RSA/SHA-256</td>
<td>Both: 3072 bits</td>
</tr>
</tbody>
</table>

Crypto - Algorithms

• Local regulations may determine algorithm
  – GOST
  – DSA

• Network limitations
  – Fragmentation means shorter key length is better
  – ZSK may be shorter since it gets rolled often
  – Elliptical is ideal – but not commonplace
Crypto - Algorithms

• NSEC3 if required
  – Protects against zone walking
  – Avoid if not needed – adds overhead for small zones
  – Non-disclosure agreement?
  – Regulatory requirement?
  – Useful if zone is large, not trivially guessable (only “www” and “mail”) or structured (ip6.arpa), and not expected to have many signed delegations (“opt-out” avoids recalculation).
Crypto - Hardware

• Satisfy your stakeholders
  – Doesn’t need to be certified to be secure (e.g., off-line PC)
  – Can use transparent process and procedures to instill trust
  – But most Registries use or plan to use HSM. Maybe CYA?

• AT LEAST USE A GOOD Random Number Generator (RNG)!

• Use common standards avoid vendor lock-in.
  – Note: KSK rollover may be ~10 years.

• Remember you must have a way to backup keys!
Crypto - Hardware Security Module (HSM)

• FIPS 140-2 Level 3
  – Sun SCA6000 (~30000 RSA 1024/sec) ~$10000 (was $1000!!)
  – Thales/Nciphernshield (~500 RSA 1024/sec) ~$15000
  – Ultimaco

• FIPS 140-2 Level 4
  – AEP Keyper (~1200 RSA 1024/sec) ~$15000
  – IBM 4765 (~1000 RSA 1024/sec) ~$9000

• Recognized by your national certification authority
  – Kryptus (Brazil) ~ $2500

Study:
Crypto - PKCS11

• A common interface for HSM and smartcards
  – C_Sign()
  – C_GeneratePair()

• Avoids vendor lock-in - somewhat

• Vendor Supplied Drivers (mostly Linux, Windows) and some open source
Crypto - Smartcards / Tokens

- Smartcards (PKI) (card reader ~$12)
  - Smartcard HSM ~$20
  - Feitian ~$5-10
  - Aventra ~$11

- TPM
  - Built into many PCs

- Token
  - Aladdin/SafeNet/Feitian USB e-Token ~$50

- Open source PKCS11 Drivers available
  - OpenSC

- Has RNG

- Slow ~0.5-10 1024 RSA signatures per second
Crypto - Random Number Generator

X `rand()`

X Netscape: Date+PIDs

✓ LavaRand

? System Entropy (/dev/random-urandom)

? H/W, Quantum Mechanical (laser) $$

✓ Standards based (FIPS, NIST 800-90A)

✓ Built into CPU chips

Crypto - FIPS 140-2 Level 4 HSM

Root, .FR, .CA ...
Crypto – FIPS Level 3 HSM

• But FIPS 140-2 Level 3 is also common
• Many TLDs using Level 3 .com, .se, .uk, .com, etc... $10K-$40K
An implementation can be this...
Physical Security

- An electromagnetic shielding datacenter (following GJBz20219-94 “C” level of PRC) is being used, and only authorized persons may access.
- HSMs and hidden master servers are kept in the electro-magnetic shielding datacenter.
- A backup system is established in disaster datacenter in Chengdu, with the same security insurance level as that of Beijing.

Physical Security
...or this
..or this (from .cr .ar)

Offline Laptop with TPM

Sign ZSKs with KSK

Generate KSK

Secure Offline Environment

Transport KSK signed DNSKEY RRsets

Transport public half of ZSKs

Offline/online DNSSEC Signer with TPM

Generate ZSKs

Sign zones with ZSK

Online/off-net DNSSEC Signer with TPM

Sign zones with KSK

Offline Laptop with TPM

Generate ZSKs

Secure Offline Environment
…or even this

**Off-line**

DATA CENTER

CAGE

RACK

SAFE
All in tamper evident bags
KSK on FD
Live O/S DVD
laptop
RNG

**Off-net**

DATA CENTER

CAGE

RACK

zonefile

ZSKs

signer

firewall

hidden master

FD with public ZSKs
FD with KSK signed DNSKEY RRsets
Learn from others mistakes
ISP’s and other validating resolver operators

• Learn from experience of others*. When someone else’s DNSSEC system fails, e.g., signatures expire, who gets the phone call? YOU DO.
• It is happening less and less (a few times a year) but have an email response ready and
• If necessary use the Negative Trust Anchor** option found in some resolvers to temporarily disable validating the problematic zone

*COMCAST US ISP ~20M customers
Signing Operations – DNSSEC and Vacations

• Learn from the experience of others. Technology is easy. Managing people is hard. DNSSEC signatures are time limited. If the signature validity period is too long, you will not be able to recover from a compromise too quickly.

• If the validity period is too short, you might not be able to replace failed equipment or get a hold of your engineers on vacation.

• Therefore many DNSSEC signatures are good for 1 to 2 weeks (about how long someone in the US takes a vacation 😊)
Signing Operations – Monitoring Signature Expiry

• The biggest problem we have seen with DNSSEC deployments has been expired signatures. Do you really want signatures to renew on December 31? Who is going to be around if things fail?

• Monitor the expiry time of your zone using a script or an outside service. Send out email/SMS if a DNSSEC signature is about to expire. Plenty of tools*

• The Internet technical community is small but global. Have one of them run a script to monitor your systems and you do the same for them. Just like you might do with secondary name servers.

*http://dnsviz.net/
http://www.zonecheck.fr/
http://dnscheck.iis.se/ (note: has undelegated option for testing new zones)
Signing Operations – Openness = Trust

• At these early stages of DNSSEC mistakes will happen. Being public about such mistakes and how you fix them builds trust and sets expectations*.

• Sharing those experiences helps others and makes you the expert.

• Being “found out” later can destroy an operation

“One obstacle for the implementation of DNSSEC is the lack of guidance for individual domain holders regarding which requirements should be defined - in particular for small and medium-sized businesses. In order to remedy that obstacle, .SE has written a guide as an aid and tool for municipalities that have the intention to implement DNSSEC, but this guide also applies to other types of organizations in both the public and private sectors.”

https://www.iis.se/english/domains/tech/recommendations-for-dnssec-deployment/

Anne-Marie Eklund Löwinder
Chief Information Security Officer
.SE (The Internet Infrastructure Foundation)
Setting reasonable expectations means it doesn’t have to be expensive
You do not need a fortress, just detect if something is touched
But all must have:

- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators

Useful IETF RFCs:
Demo Implementation

- Key lengths – KSK:2048 RSA  ZSK:1024 RSA
- Rollover – KSK:as needed  ZSK:90 days
- RSASHA256 NSEC3
- Physical – HSM/smartcards inside Safe inside Rack inside Cage inside Commercial Data Center
- Logical – Separation of roles: cage access, safe combination, HSM/smartcard activation across three roles
- Crypto – use FIPS certified smartcards as HSM and RNG
  - Generate KSK and ZSK offline using RNG
  - KSK use off-line
  - ZSK use off-net
Off-Line Key generator and KSK Signer

DATA CENTER

CAGE

RACK

SAFE

smartcards

KSK+RNG

KSK+RNG

KSK+RNG

Live O/S DVD

reader

laptop

Flash Drive

KSK signed DNSKEYs

Encrypted ZSKs
Off-Net Signer

DATA CENTER

CAGE

RACK

Flash Drive

KSK signed DNSKEYs

Encrypted ZSKs

zonefile

signer

firewall

hidden master

nameserver

hidden master

nameserver

hidden master

nameserver
Key Management

- Sign ZSKs with KSK
- Generate ZSKs
- Generate KSK
- Secure Key Generation and Signing Environment
- Offline Laptop
- Transport KSK signed DNSKEY RRsets and Encrypted ZSKs
- Online/off-net DNSSEC Signer
- Sign zones with ZSK
- unsigned zone
- signed zone

Animated slide
Simple Key Management Scripts
Keeping things signed

• If the signatures are going to expire soon, sign the zone
• Define “soon”
• Also sign if a record has changed
• That’s it!
while(1) {
    t = time
    if((exp - t) < 5 days) {
        inc = t
        exp = t + 10 days
        touch infile
    }
    if new infile {
        cat infile keys > zonefile
        increment zonefile SOA serial
        signzone -s inc -e exp zonefile
        zsk-current ksk
        rndc reload
    }
    sleep 1 second
}
Rolling keys

• Mind the cache – DNS resolvers have memory
• Publish the new ZSK before signing with it
  – Put the new ZSK in the DNSKEY RRset along with old ZSK and wait until everyone see its
• Sign the zone with the new ZSK until you want to change it
• But do not un-Publish the old ZSK until no one may need it
# Key Rollover Schedule - Root

<table>
<thead>
<tr>
<th>T-10</th>
<th>T+0</th>
<th>T+10</th>
<th>T+20</th>
<th>T+30</th>
<th>T+40</th>
<th>T+50</th>
<th>T+60</th>
<th>T+70</th>
<th>T+80</th>
<th>T+90</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
<td>ZSK</td>
</tr>
<tr>
<td></td>
<td>pre-publish</td>
<td>post-publish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
<td>KSK</td>
</tr>
<tr>
<td></td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
<td>publish+sign</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[https://www.iana.org/dnssec](https://www.iana.org/dnssec)
generate zsk-new
cat zsk-new zsk-current ksk > keys
touch infile
sleep >2xTTL
copy zsk-new zsk-current
touch infile
sleep >2xTTL
cat zsk-current ksk > keys
touch infile
sleep >2xTTL