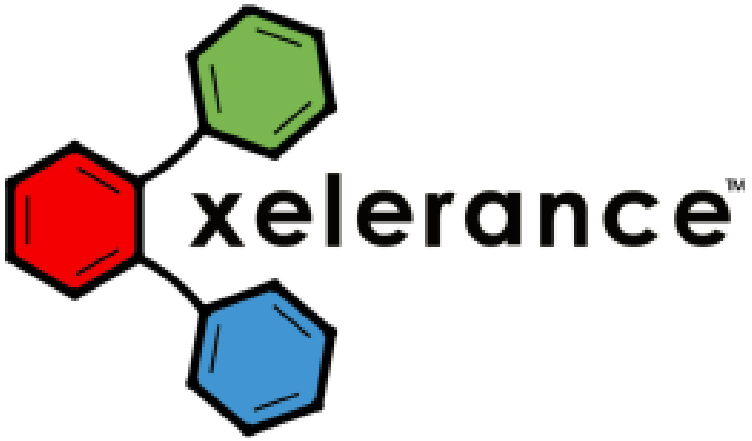


Who is Xelerance

Xelerence Corporation is a company with a dedicated team of experienced software developers, network designers and consultants providing support, development and network design services for businesses from ISP's to Fortune 100 companies

Our initial flagship solution “Openswan” is found as the core of many IPsec based VP products, ranging from enterprise rollouts consumer electronics.

xelerance

Our Solutions

- VPN solutions
- DNS / DNSSEC deployments
- Authentication Management
- Embedded Linux development
- Custom development

The DNSSEC difference

DNS

- Fairly straightforward simple concept
- Setup once and forget about it – easy to pickup
- Forgiving for human errors

- Integrated differently with each organisation, usually features webgui and db
- Data never expires,delays with nameservers not critical
- Core standard everywhere

DNSSEC

- Conceptually hard for average zone admin
- Continuous effort required to maintain signed zones
- Human errors have dire consequences.
- Does not fit in currently deployed DNS infrastructure
- Data becomes stale, smooth integration with nameserver required
- Non-uniform deployment

Some minor extra things you need to know

- DNSSEC includes keys. There are two different kinds:
  - zone signing keys (ZSK)
  - key signing keys (KSK)
- KSK is authenticated by a DS RR, which is a hash of the public key
- DS RR is stored in the parent

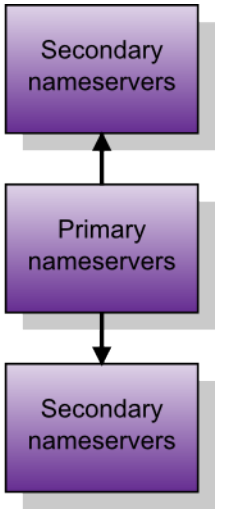
- Four combinations, three useful:
  - ZSK online, KSK online
  - ZSK online, KSK offline
  - use KSK as ZSK, keep it online (one key)
  - use KSK as ZSK, keep it offline (not very useful)

Types of DNS deployments: no IPAM, just Unix

- bind9 on one Unix system
- secondary systems by friendly arrangement
- IPAM done with vi.
- RCS/CVS for files, “if Bob remembers to do it”

→ easiest place to “deploy” DNSSEC.

just add “dnssec-signzone”
resign zone with cron?
never roll any keys



Types of DNS deployments: no IPAM, just Unix: “secure”

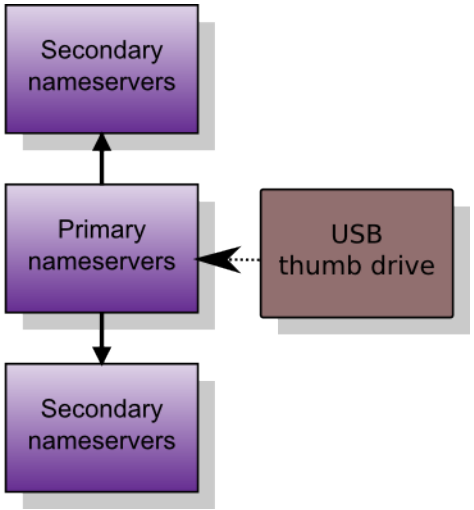
- same as before
- use seperate ZSK and KSK
- put KSK on USB thumb drive

→ very secure, as long as you remember to insert key every month.

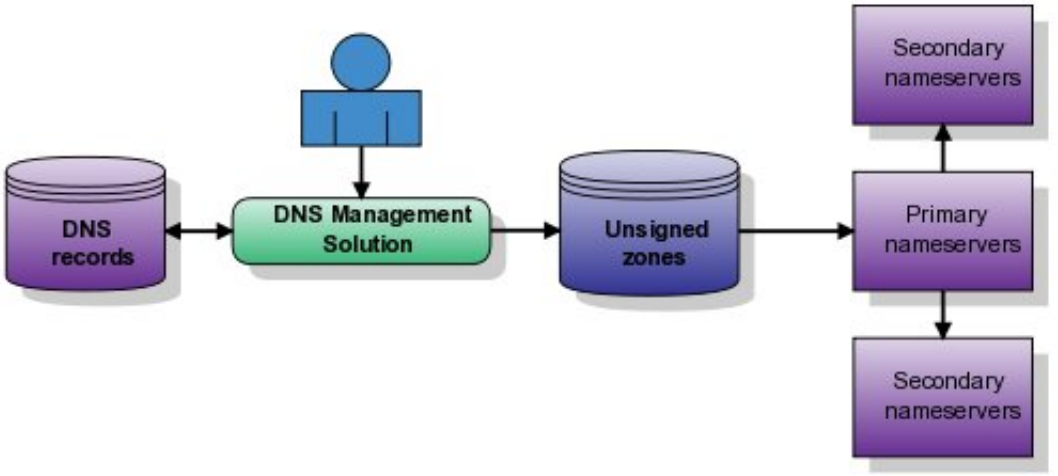
→ (and you don't take vacations)

→ no key roll-over capabilities

→ hard to do with bind9 tools.

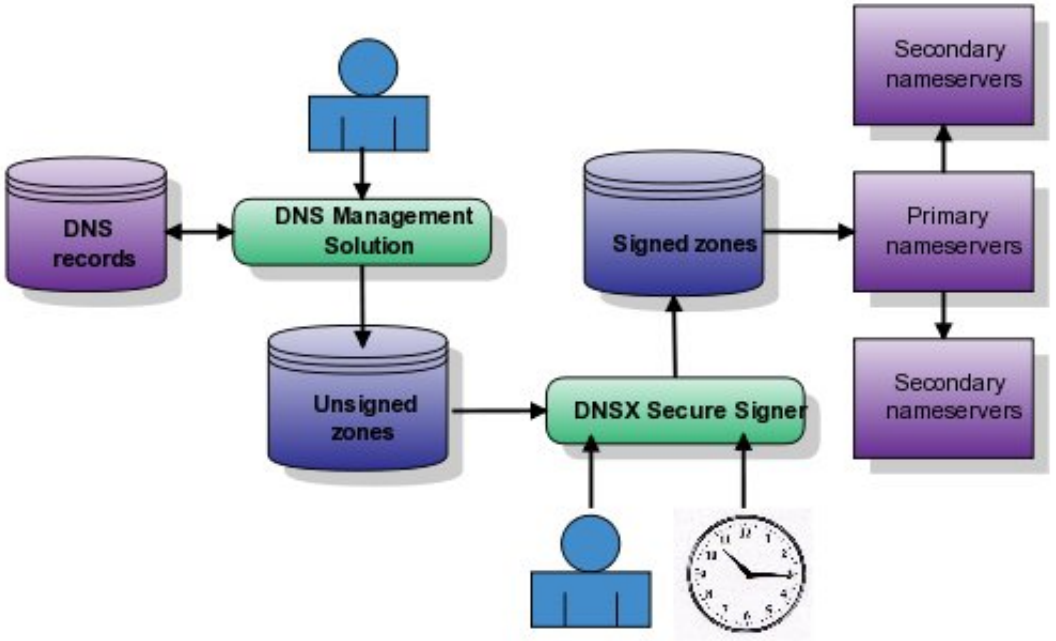


Typical DNS Deployment Basic IPAM solution



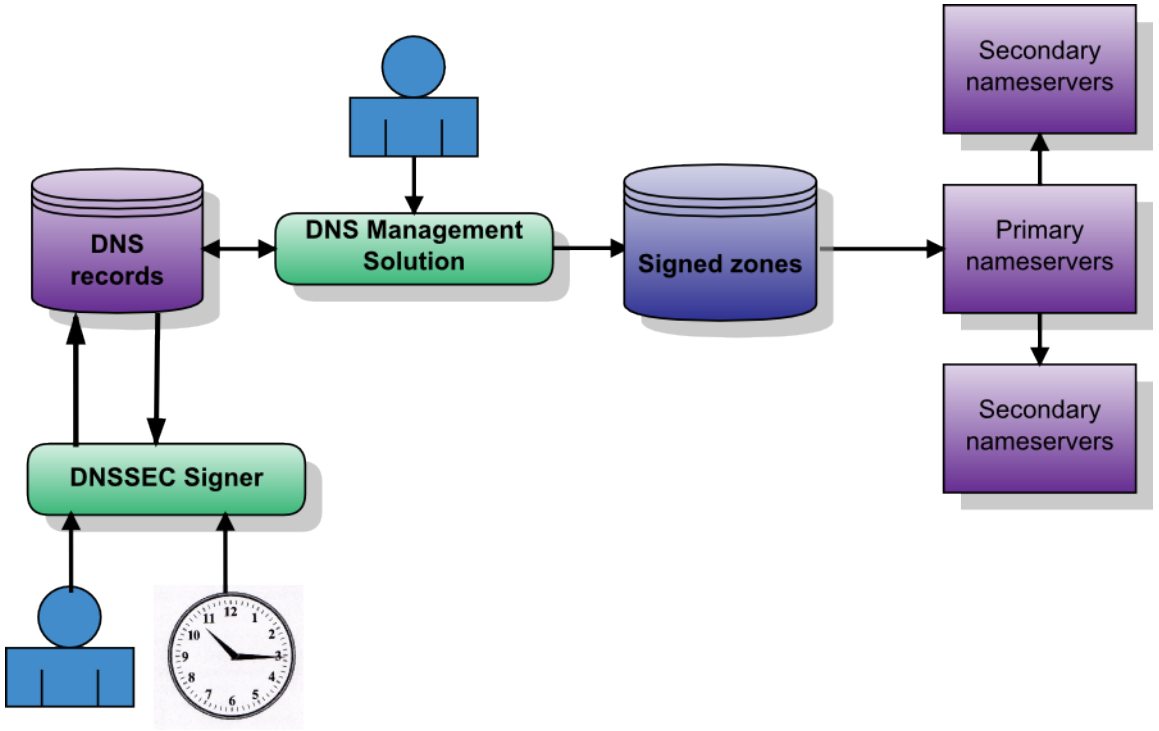
- dns zone files are generated by IPAM system
- IPAM pushes data to primary name server. Many options exist:
  - scp, dns-xfer (AXFR), dynamic-update, ftp (pull), http (pull), even NFS, LDAP/ActiveDirectory.

DNSSEC is easy to integrate into basic IPAM solution



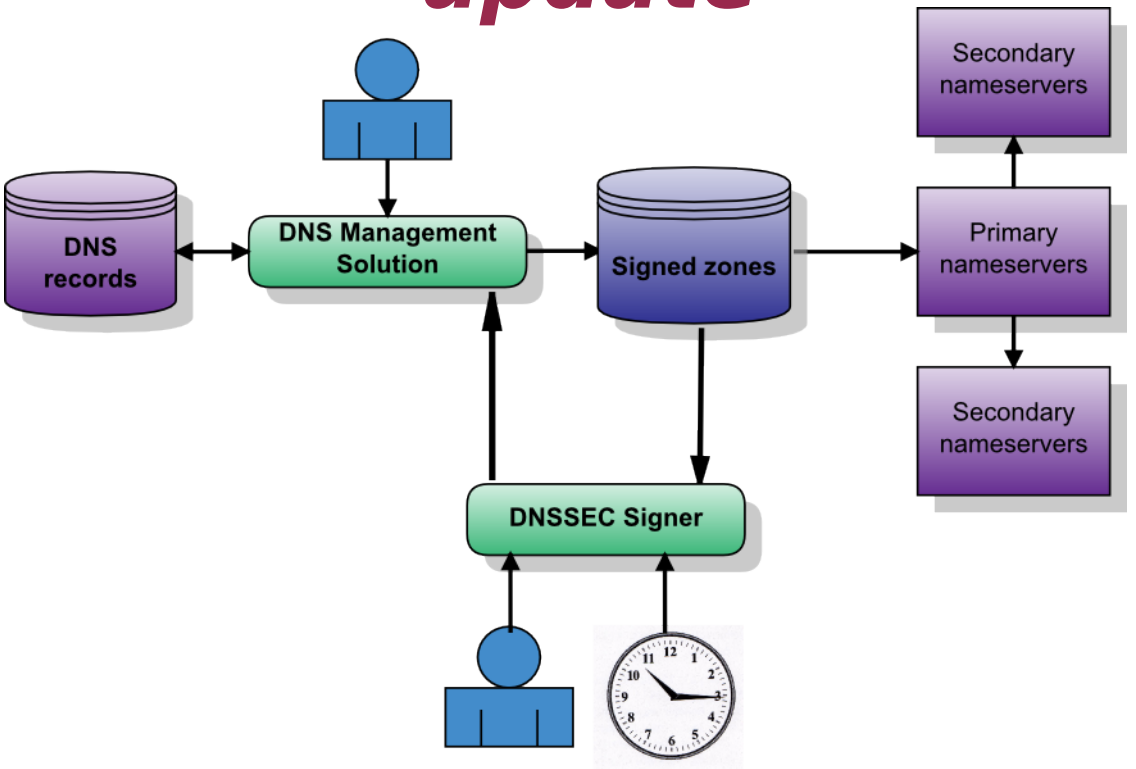
- Push signed zones via SSH/SFTP
- Push signed zones via NFS/SMB
- *DNS AXFR from unsigned zone, DNS-AXFR from signed zone.*

DNSSEC integration into open IPAM solution



- dnssec signer interacts with database directly
- inserts records as appropriate, possibly incrementally.
- rest of infrastructure remains the same
- *IPAM solution centric.*

DNSSEC integration into IPAM solution that supports dynamic update



- dnssec signer pulls unsigned records from stealth "primary", using ixfr
- dnssec signer does dns-update to insert DNSSIG RR.
- *uses only DNS protocols. Requires IPAM to support dynamic update.*

Feature set of DNSX: Secure Signer

- DNSSEC operations
  - Key Signing Keys and Zone Signing Keys management
  - Zone signing and re-signing management
  - Key rollover management (KSK and ZSK)
  - Emergency key rollover support
  - DLV support – standard configuration uses dlv.isc.org

- DNSSEC and DNS records management
  - DS record management (fully automatic if we are parent and child)
  - DS record support on external parent (point to proper TLD pages)
  - System wide and per-domain DNSSEC settings for key types, key sizes, signature lifetime, re-sign interval

DNSX Secure Signer

FIPS 140-2 compliant hardware RNG

Feature set of DNSX: Secure Signer

- Automation support
  - All features except “DS upload to external parent” can be set to
    automatic or manual on a system-wide and per-domain basis

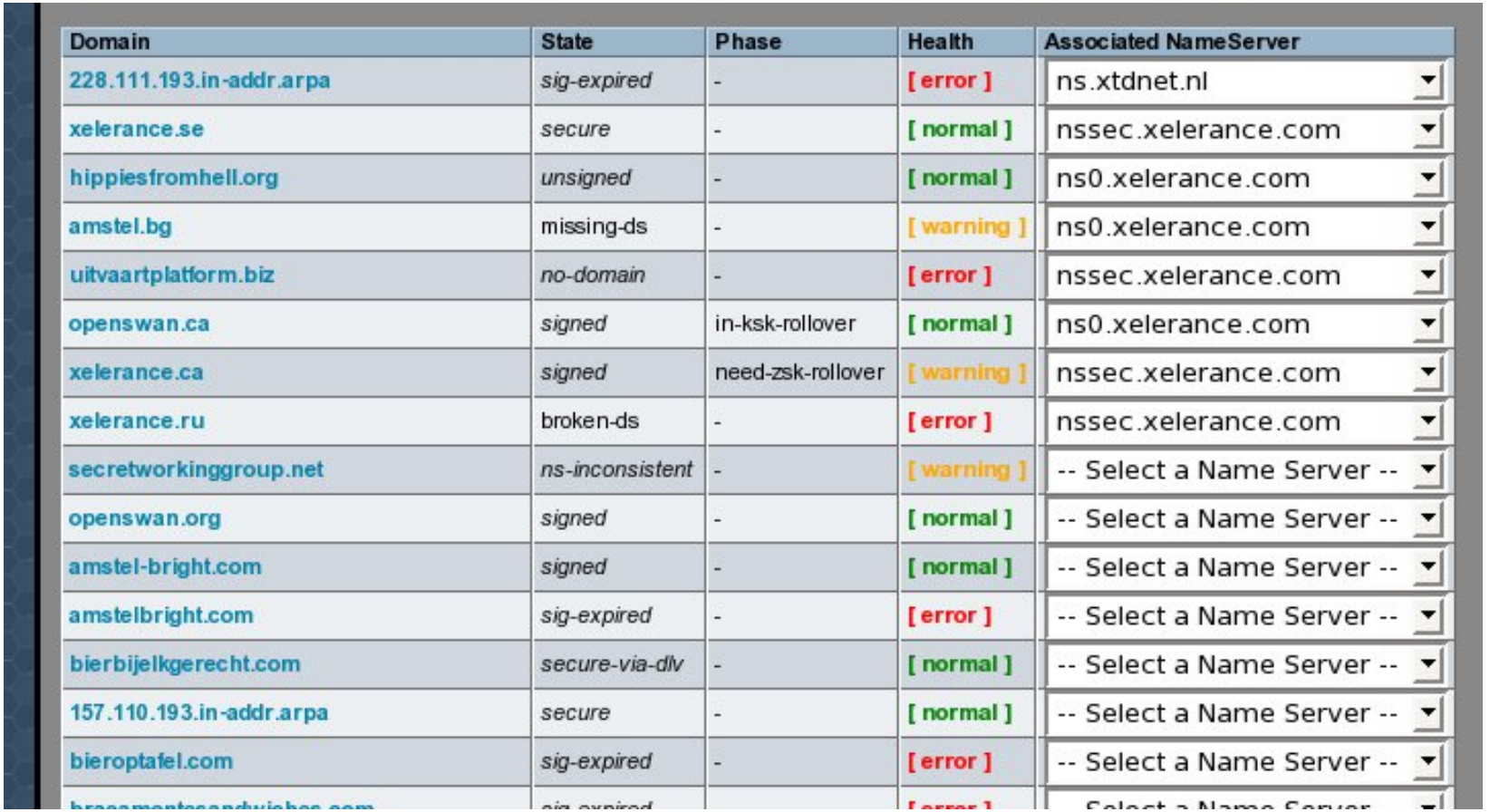
- Nameserver integration
  - Data verification, operational verification
  - Upload support via SSH/SFTP
  - Reload / restart support via SSH/SFTP

Questions?

Feature set of DNSX: Secure Signer

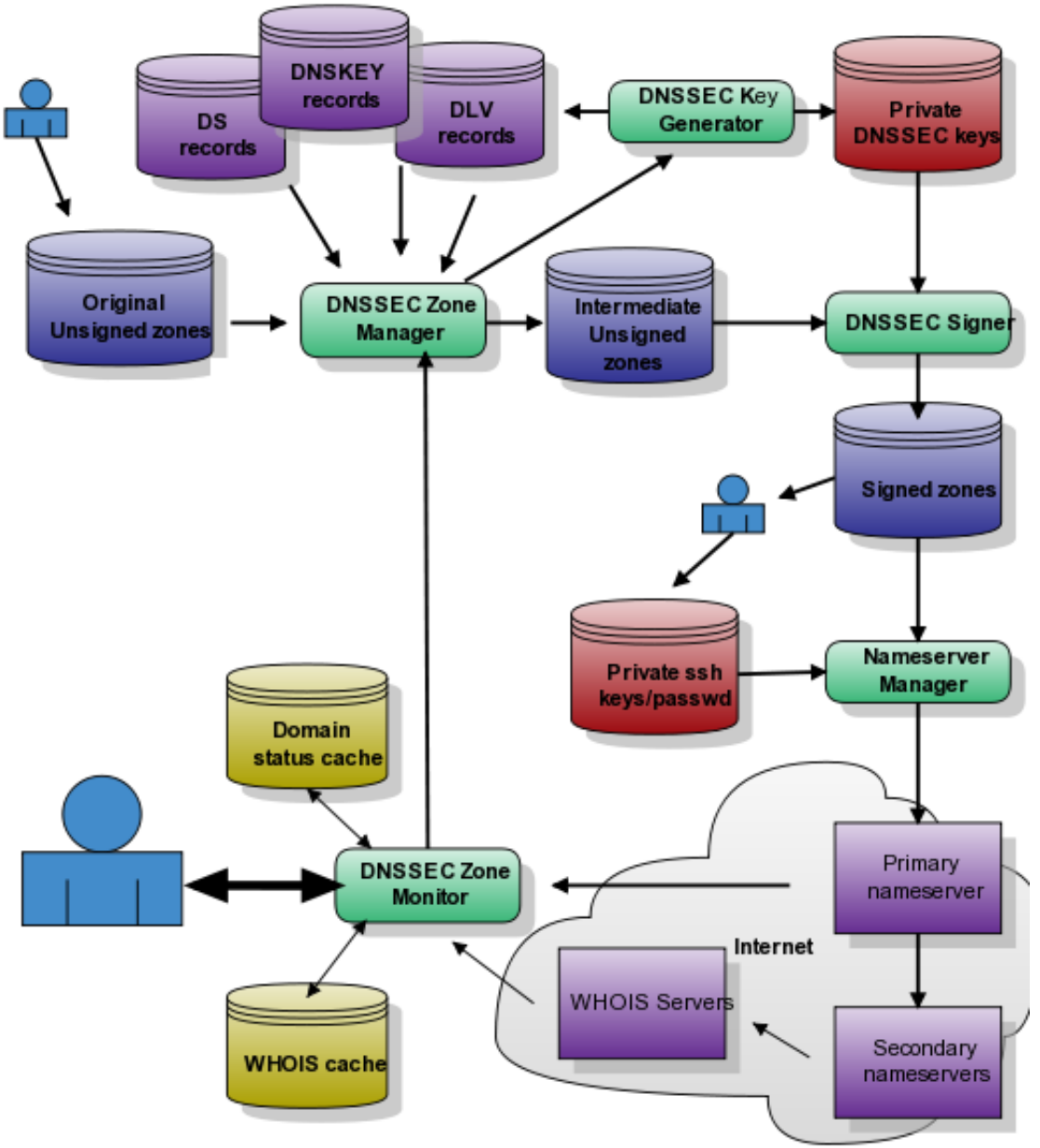
- Online mode
  - Active verification of DNSSEC records, zones and nameservers
  - Notification of imminent or occurring issues
- Offline mode
  - As secure as it gets – but no live zone data verifications
  - Use laptop with browser as graphical console
  - Use browser or USB media for export / import of zone data
- Backup / Restore
  - All private keys and backups are encrypted using OpenPGP

DNSX Screenshot



Domain	State	Phase	Health	Associated NameServer
228.111.193.in-addr.arpa	*sig-expired*	-	[error]	ns.xtdnet.nl
xelerance.se	*secure*	-	[normal]	nssec.xelerance.com
hippiesfromhell.org	*unsigned*	-	[normal]	ns0.xelerance.com
amstel.bg	missing-ds	-	[warning]	ns0.xelerance.com
uitvaartplatform.biz	*no-domain*	-	[error]	nssec.xelerance.com
openswan.ca	*signed*	in-ksk-rollover	[normal]	ns0.xelerance.com
xelerance.ca	*signed*	need-zsk-rollover	[warning]	nssec.xelerance.com
xelerance.ru	broken-ds	-	[error]	nssec.xelerance.com
secretworkinggroup.net	*ns-inconsistent*	-	[warning]	-- Select a Name Server --
openswan.org	*signed*	-	[normal]	-- Select a Name Server --
amstel-bright.com	*signed*	-	[normal]	-- Select a Name Server --
amstelbright.com	*sig-expired*	-	[error]	-- Select a Name Server --
bierbijelkgerecht.com	*secure-via-dlv*	-	[normal]	-- Select a Name Server --
157.110.193.in-addr.arpa	*secure*	-	[normal]	-- Select a Name Server --
bieroptafel.com	*sig-expired*	-	[error]	-- Select a Name Server --

DNSX Inside


DS records
DNSKEY records
DLV records
DNSSEC Key Generator
Private DNSSEC keys
Original Unsigned zones
DNSSEC Zone Manager
Intermediate Unsigned zones
DNSSEC Signer
Signed zones
Private ssh keys/passwd
Nameserver Manager
Domain status cache
DNSSEC Zone Monitor
Primary nameserver
Internet
WHOIS Servers
Secondary nameservers
WHOIS cache