Central Registry Solutions™

DNSSEC: problems and solutions for ISPs, web hosts and registrars

UKNOF 15, Rochdale

January 21, 2009

About Central Registry Solutions

Central Registry Solutions was formed to help customers navigate the ICANN application process and provide advice about how to set up and maintain registry services for new Top Level Domains (TLDs). CRS offers registry services and provides distribution of domains and a portfolio of online services.

Central Registry Solutions brings together two recognized leaders in the Internet Industry

- CentralNic who has provided flexible and stable registry services since 1994
- Network Solutions, who brings experience and extensive market reach as the original registrar since its founding in 1979

CentralNic
www.centralnic.com

NetworkSolutions.

CRS Central Registry Solutions™

Agenda

- DNSSEC Deployment Overview
- Consumer demand
- Operational impact
- Signing zones
- Managing key rollover
- Unsolved problems
- Off the shelf solutions
- Conclusion

1. DNSSec Deployment Overview

DNSSEC: problems and solutions for ISPs, web hosts and registrars

2. Consumer demand

3. Operational impact

3.1 Response packet inflation

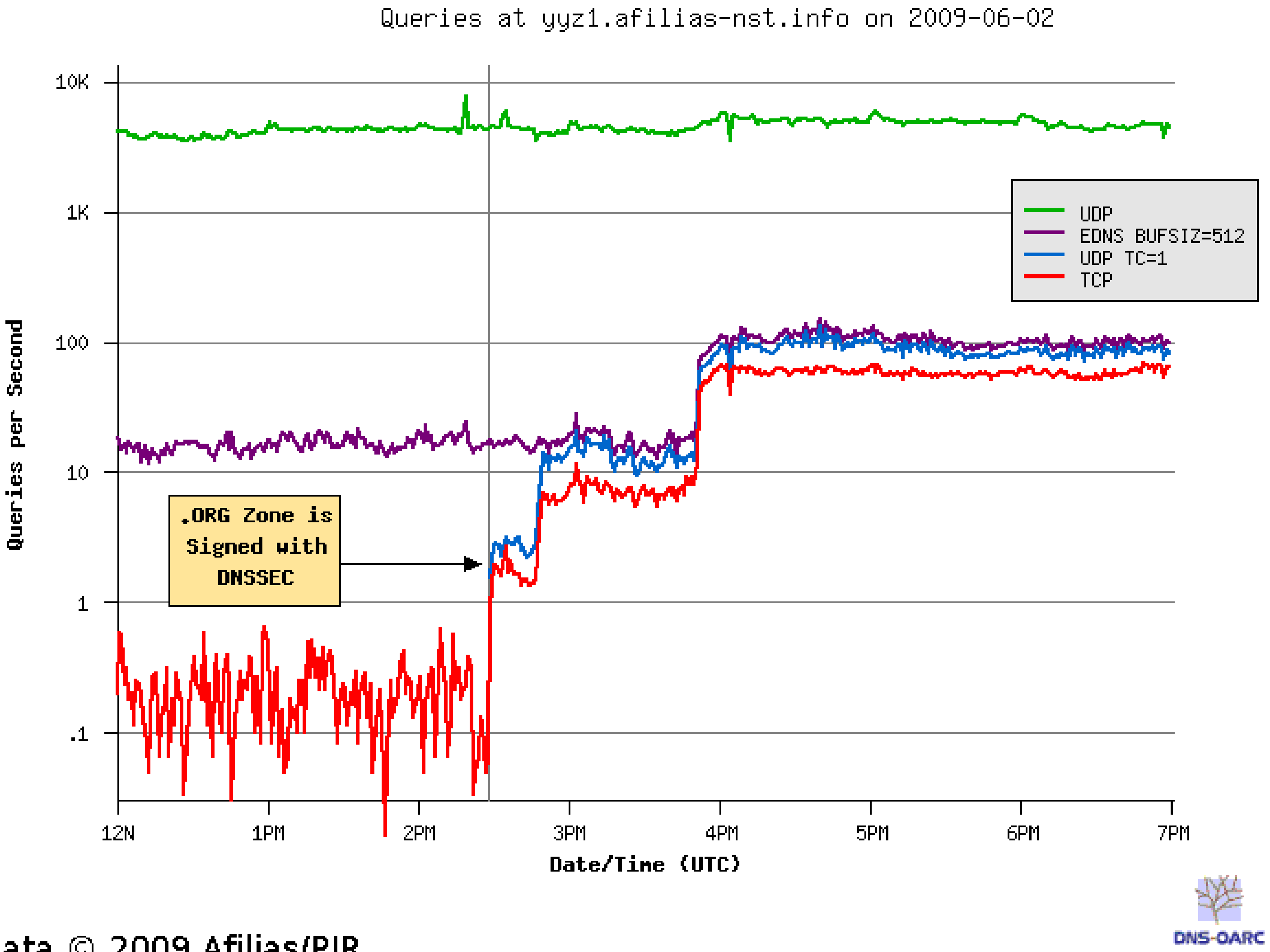
DNSSEC: problems and solutions for ISPs, web hosts and registrars

3.2 EDNS support

3.3 UDP fragmentation

3.4 TCP query volume inflation

DNSSEC: problems and solutions for ISPs, web hosts and registrars



Data © 2009 Afilias/PIR

Source: Duane Wessels, DNS-OARC, June 2009

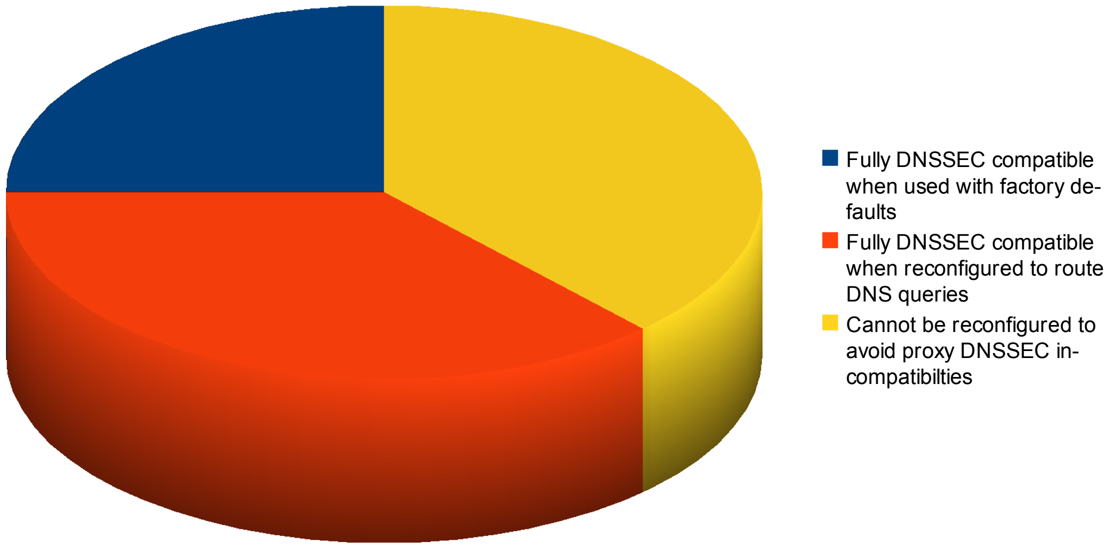
DNSSEC: problems and solutions for ISPs, web hosts and registrars

3.5 NXDOMAIN interception

DNSSEC: problems and solutions for ISPs, web hosts and registrars

3.6 CPE

DNSSEC: problems and solutions for ISPs, web hosts and registrars



Source: Ray Bellis, Nominet, September 2008

4. Signing zones

4.1 Storing and transmitting zone data

4.2 generating zone data

4.3 securing keying data

5. Managing key rollover

5.1 pushing DS keys to parent registries

5.1.1 EPP <secDNS>

DNSSEC: problems and solutions for ISPs, web hosts and registrars

5.1.2 issues for resellers (non registrars)

5.2 DLV

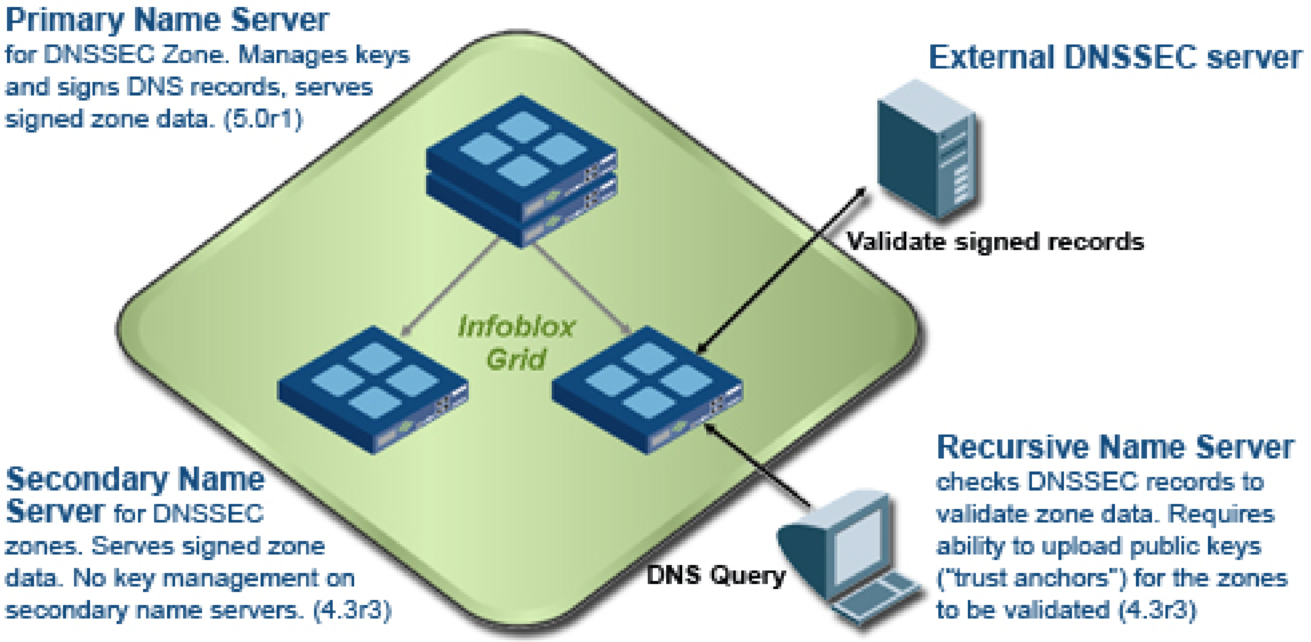
6. Unsolved problems

6.1 Domain name transfers

7. Off-the-shelf solutions

7.1 Infloblox

DNSSEC: problems and solutions for ISPs, web hosts and registrars



Primary Name Server for DNSSEC Zone. Manages keys and signs DNS records, serves signed zone data. (5.0r1)

External DNSSEC server

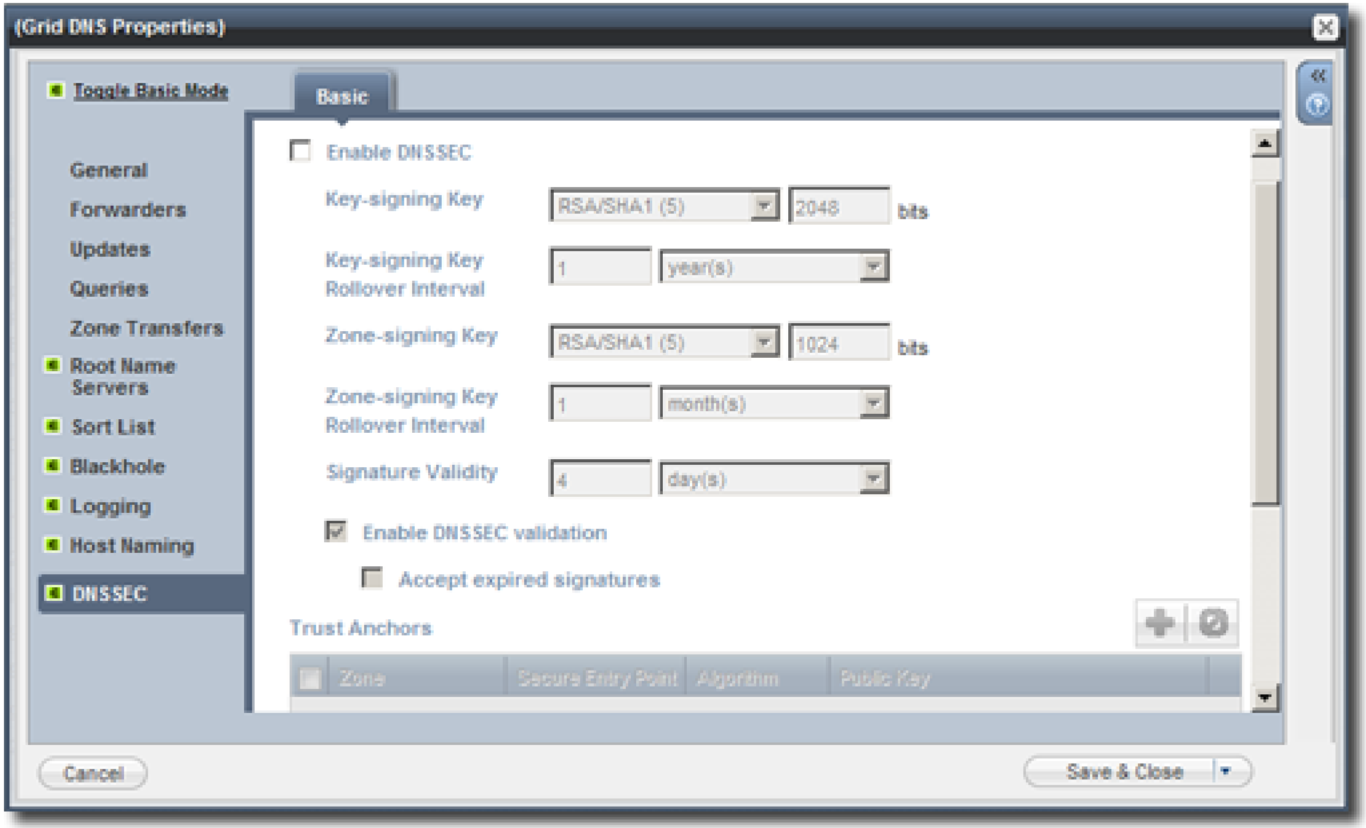
Validate signed records

Secondary Name Server for DNSSEC zones. Serves signed zone data. No key management on secondary name servers. (4.3r3)

Recursive Name Server checks DNSSEC records to validate zone data. Requires ability to upload public keys ("trust anchors") for the zones to be validated (4.3r3)

Source: Infoblox.com

DNSSEC: problems and solutions for ISPs, web hosts and registrars



(Grid DNS Properties)

□ Enable DNSSEC

Key-signing Key: RSA/SHA1 (5), 2048 bits

Key-signing Key Rollover Interval: 1 year(s)

Zone-signing Key: RSA/SHA1 (5), 1024 bits

Zone-signing Key Rollover Interval: 1 month(s)

Signature Validity: 4 day(s)

☑ Enable DNSSEC validation

□ Accept expired signatures

Trust Anchors

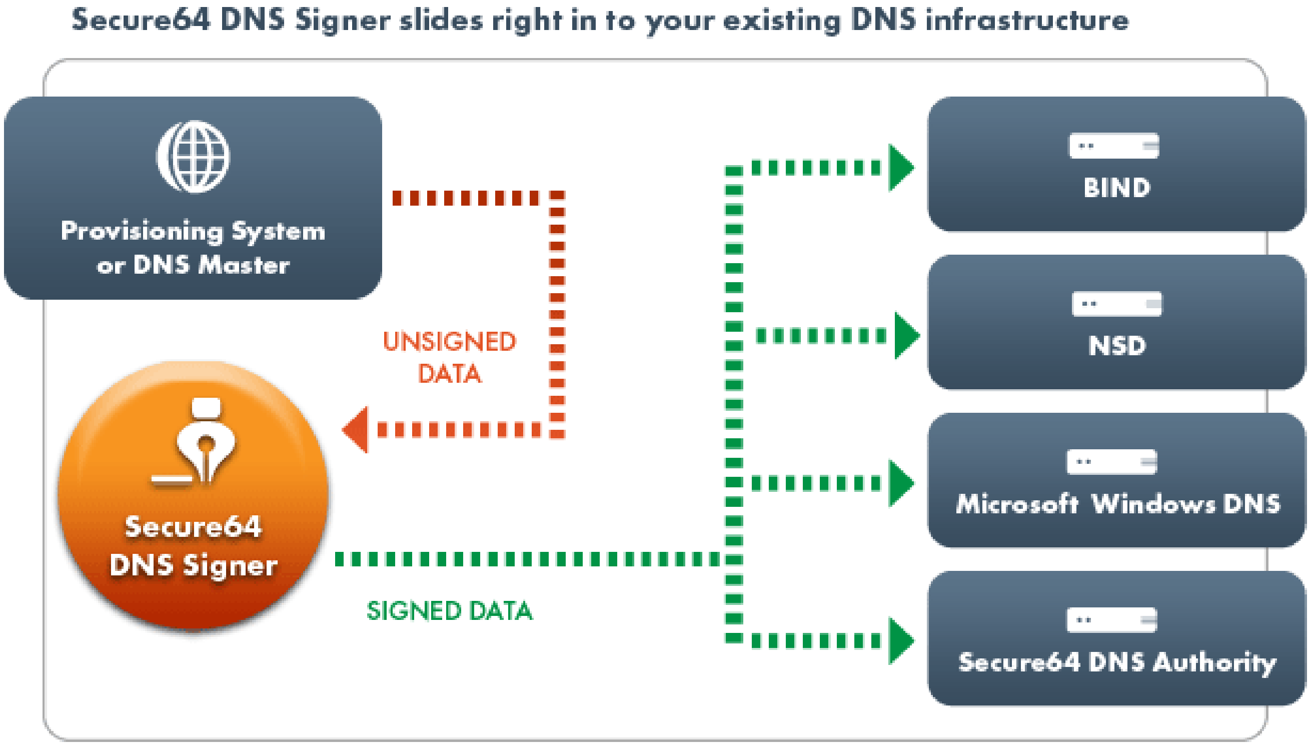
□	Zone	Secure Entry Point	Algorithm	Public Key

Source: Infoblox.com

DNSSEC: problems and solutions for ISPs, web hosts and registrars

7.2 Secure64

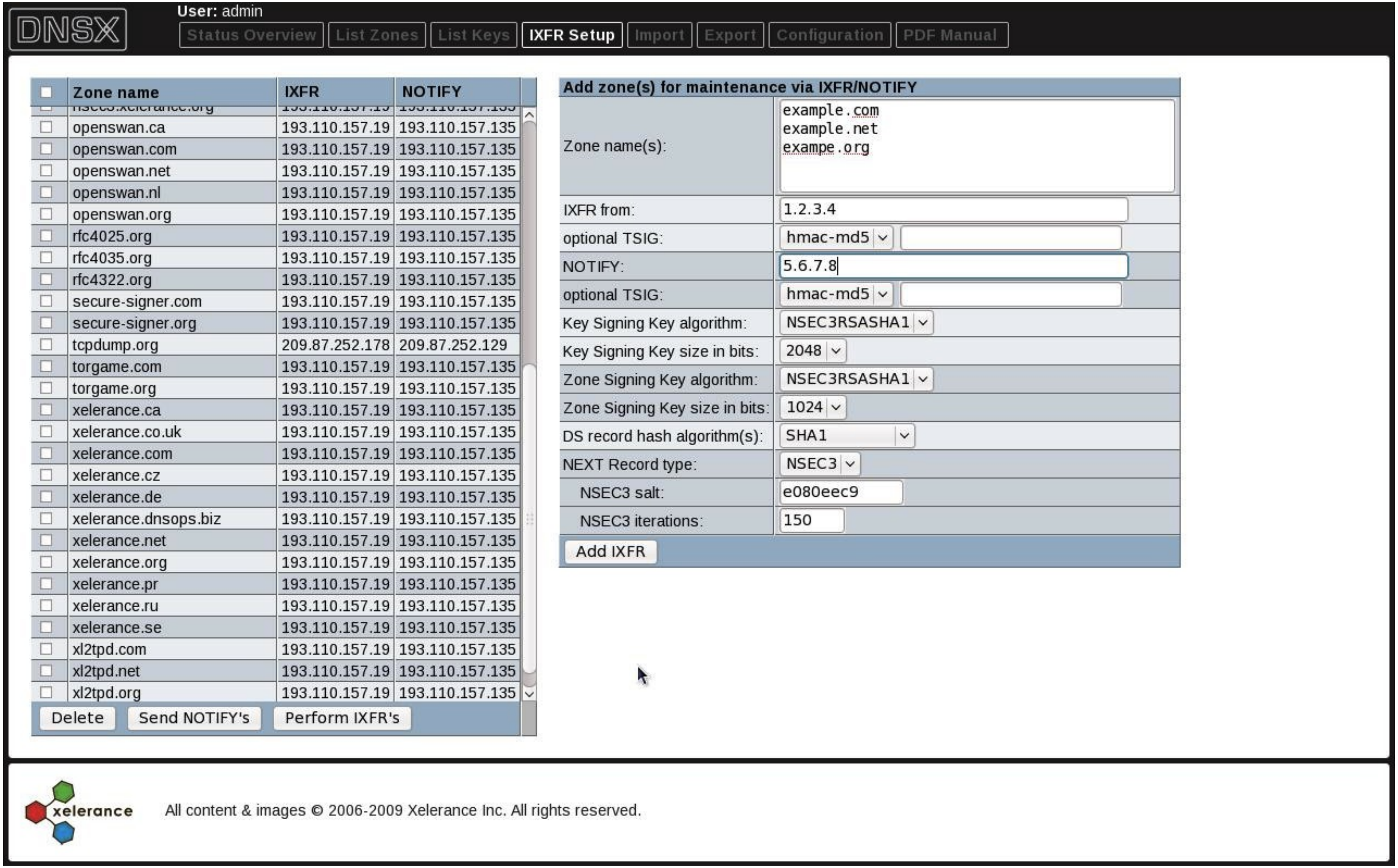
DNSSEC: problems and solutions for ISPs, web hosts and registrars


Secure64 DNS Signer slides right in to your existing DNS infrastructure
Provisioning System or DNS Master
UNSIGNED DATA
Secure64 DNS Signer
SIGNED DATA
BIND
NSD
Microsoft Windows DNS
Secure64 DNS Authority

Source: Secure64.com

7.3 Xelerance

DNSSEC: problems and solutions for ISPs, web hosts and registrars



□	Zone name	IXFR	NOTIFY
□	nsec3.xelerance.org	193.110.157.19	193.110.157.135
□	openswan.ca	193.110.157.19	193.110.157.135
□	openswan.com	193.110.157.19	193.110.157.135
□	openswan.net	193.110.157.19	193.110.157.135
□	openswan.nl	193.110.157.19	193.110.157.135
□	openswan.org	193.110.157.19	193.110.157.135
□	rfc4025.org	193.110.157.19	193.110.157.135
□	rfc4035.org	193.110.157.19	193.110.157.135
□	rfc4322.org	193.110.157.19	193.110.157.135
□	secure-signer.com	193.110.157.19	193.110.157.135
□	secure-signer.org	193.110.157.19	193.110.157.135
□	tcpdump.org	209.87.252.178	209.87.252.129
□	torgame.com	193.110.157.19	193.110.157.135
□	torgame.org	193.110.157.19	193.110.157.135
□	xelerance.ca	193.110.157.19	193.110.157.135
□	xelerance.co.uk	193.110.157.19	193.110.157.135
□	xelerance.com	193.110.157.19	193.110.157.135
□	xelerance.cz	193.110.157.19	193.110.157.135
□	xelerance.de	193.110.157.19	193.110.157.135
□	xelerance.dnsops.biz	193.110.157.19	193.110.157.135
□	xelerance.net	193.110.157.19	193.110.157.135
□	xelerance.org	193.110.157.19	193.110.157.135
□	xelerance.pr	193.110.157.19	193.110.157.135
□	xelerance.ru	193.110.157.19	193.110.157.135
□	xelerance.se	193.110.157.19	193.110.157.135
□	xl2tpd.com	193.110.157.19	193.110.157.135
□	xl2tpd.net	193.110.157.19	193.110.157.135
□	xl2tpd.org	193.110.157.19	193.110.157.135

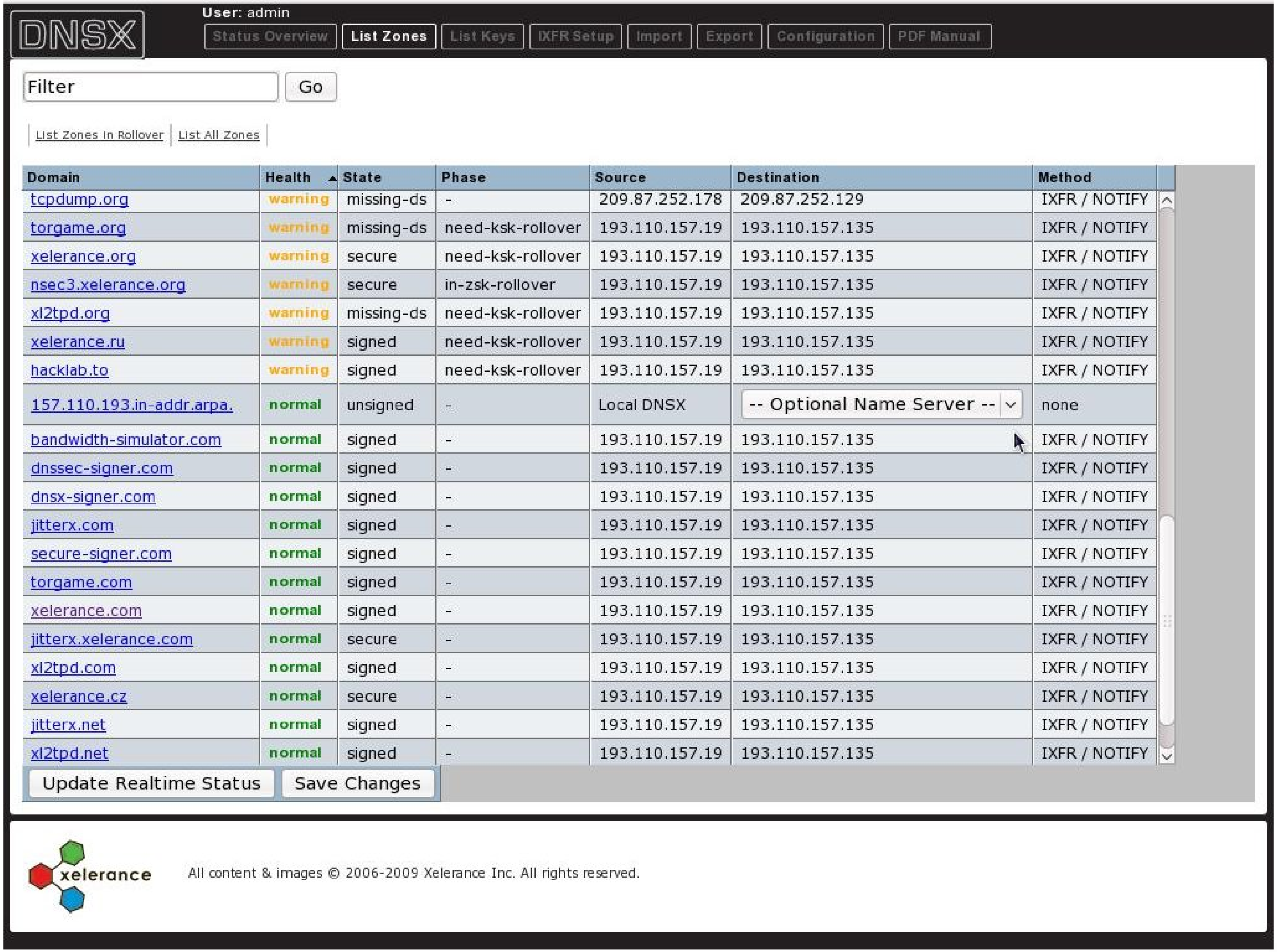
Add zone(s) for maintenance via IXFR/NOTIFY

Zone name(s):	example.com example.net exampe.org
IXFR from:	1.2.3.4
optional TSIG:	hmac-md5
NOTIFY:	5.6.7.8
optional TSIG:	hmac-md5
Key Signing Key algorithm:	NSEC3RSASHA1
Key Signing Key size in bits:	2048
Zone Signing Key algorithm:	NSEC3RSASHA1
Zone Signing Key size in bits:	1024
DS record hash algorithm(s):	SHA1
NEXT Record type:	NSEC3
NSEC3 salt:	e080eec9
NSEC3 iterations:	150

All content & images © 2006-2009 Xelerance Inc. All rights reserved.

Source: Paul Wouters

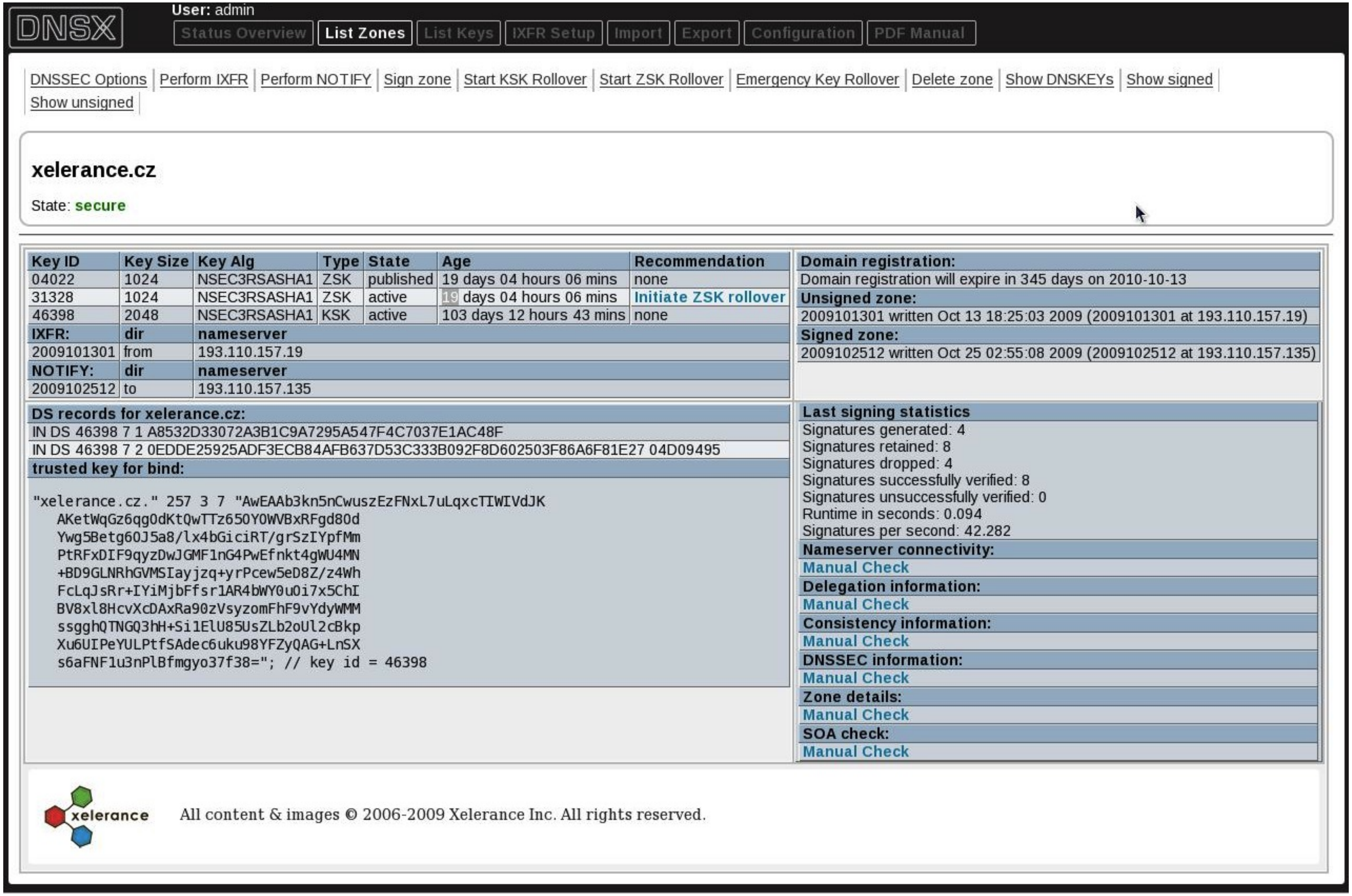
DNSSEC: problems and solutions for ISPs, web hosts and registrars



Domain	Health ▲	State	Phase	Source	Destination	Method
tcpdump.org	warning	missing-ds	-	209.87.252.178	209.87.252.129	IXFR / NOTIFY
torgame.org	warning	missing-ds	need-ksk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xelerance.org	warning	secure	need-ksk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
nsec3.xelerance.org	warning	secure	in-zsk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xl2tpd.org	warning	missing-ds	need-ksk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xelerance.ru	warning	signed	need-ksk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
hacklab.to	warning	signed	need-ksk-rollover	193.110.157.19	193.110.157.135	IXFR / NOTIFY
157.110.193.in-addr.arpa.	normal	unsigned	-	Local DNSX	-- Optional Name Server --	none
bandwidth-simulator.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
dnssec-signer.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
dnsx-signer.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
jitterx.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
secure-signer.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
torgame.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xelerance.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
jitterx.xelerance.com	normal	secure	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xl2tpd.com	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xelerance.cz	normal	secure	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
jitterx.net	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY
xl2tpd.net	normal	signed	-	193.110.157.19	193.110.157.135	IXFR / NOTIFY

Source: Paul Wouters

DNSSEC: problems and solutions for ISPs, web hosts and registrars



DNSX
User: admin
Status Overview
List Zones
List Keys
IXFR Setup
Import
Export
Configuration
PDF Manual
DNSSEC Options | Perform IXFR | Perform NOTIFY | Sign zone | Start KSK Rollover | Start ZSK Rollover | Emergency Key Rollover | Delete zone | Show DNSKEYs | Show signed | Show unsigned

xelerance.cz

State: **secure**

Key ID	Key Size	Key Alg	Type	State	Age	Recommendation
04022	1024	NSEC3RSASHA1	ZSK	published	19 days 04 hours 06 mins	none
31328	1024	NSEC3RSASHA1	ZSK	active	19 days 04 hours 06 mins	Initiate ZSK rollover
46398	2048	NSEC3RSASHA1	KSK	active	103 days 12 hours 43 mins	none

IXFR:	dir	nameserver
2009101301	from	193.110.157.19
NOTIFY:	**dir**	**nameserver**
2009102512	to	193.110.157.135

Domain registration:
Domain registration will expire in 345 days on 2010-10-13

Unsigned zone:
2009101301 written Oct 13 18:25:03 2009 (2009101301 at 193.110.157.19)

Signed zone:
2009102512 written Oct 25 02:55:08 2009 (2009102512 at 193.110.157.135)

DS records for xelerance.cz:

```
IN DS 46398 7 1 A8532D33072A3B1C9A7295A547F4C7037E1AC48F
IN DS 46398 7 2 0EDDE25925ADF3ECB84AFB637D53C333B092F8D602503F86A6F81E27 04D09495
```

trusted key for bind:

```
"xelerance.cz." 257 3 7 "AwEAAb3kn5nCwuszEzFNxL7uLqxcTIWIVdJK
   AKetWqGz6qg0dKtQwTTz650Y0WVBxRFgd80d
   Ywg5Betg60J5a8/lx4bGiciRT/grSzIYpfMm
   PtRFxDIF9qyzDwJGMF1nG4PwEfnkt4gWU4MN
   +BD9GLNRhGVMSIayjzq+yrPcew5eD8Z/z4Wh
   FcLqJsRr+IYiMjbFfsr1AR4bWY0u0i7x5ChI
   BV8xl8HcvXcDAxRa90zVsyzomFhF9vYdyWMM
   ssghQTNGQ3hH+Si1ElU85UsZLb2oUl2cBkp
   Xu6UIPeYULPtfSAdec6uku98YFZyQAG+LnSX
   s6aFNF1u3nPlBfmgyo37f38="; // key id = 46398
```

Last signing statistics
Signatures generated: 4
Signatures retained: 8
Signatures dropped: 4
Signatures successfully verified: 8
Signatures unsuccessfully verified: 0
Runtime in seconds: 0.094
Signatures per second: 42.282

Nameserver connectivity:
Manual Check

Delegation information:
Manual Check

Consistency information:
Manual Check

DNSSEC information:
Manual Check

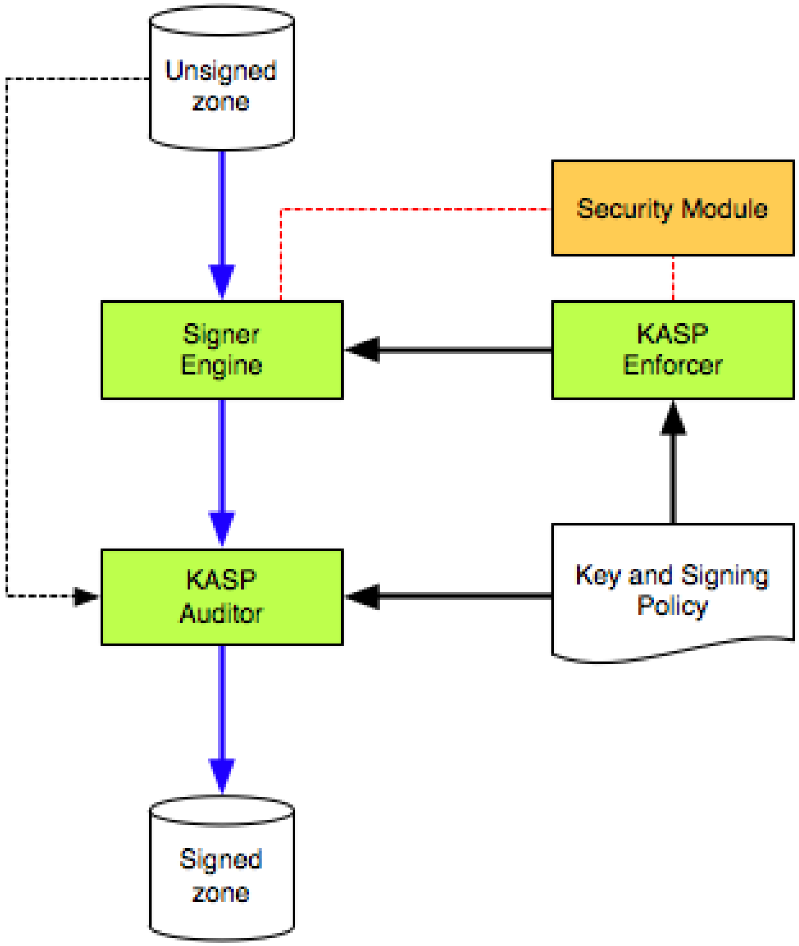
Zone details:
Manual Check

SOA check:
Manual Check

Source: Paul Wouters

7.4 OpenDNSSEC

DNSSEC: problems and solutions for ISPs, web hosts and registrars



Source: OpenDNSSEC.org

7.5 BIND

7.6 PowerDNSSEC

8. Conclusion