



Xelerance Corporation

Trouble in paradise

- DNS is fundamentally insecure
- DNSSEC is now a survival path
- The Kaminsky attack is real. ISP nameservers are actively attacked
- DNSSEC is ready now. There is no reason not to deploy and use it

Warm up your calculators

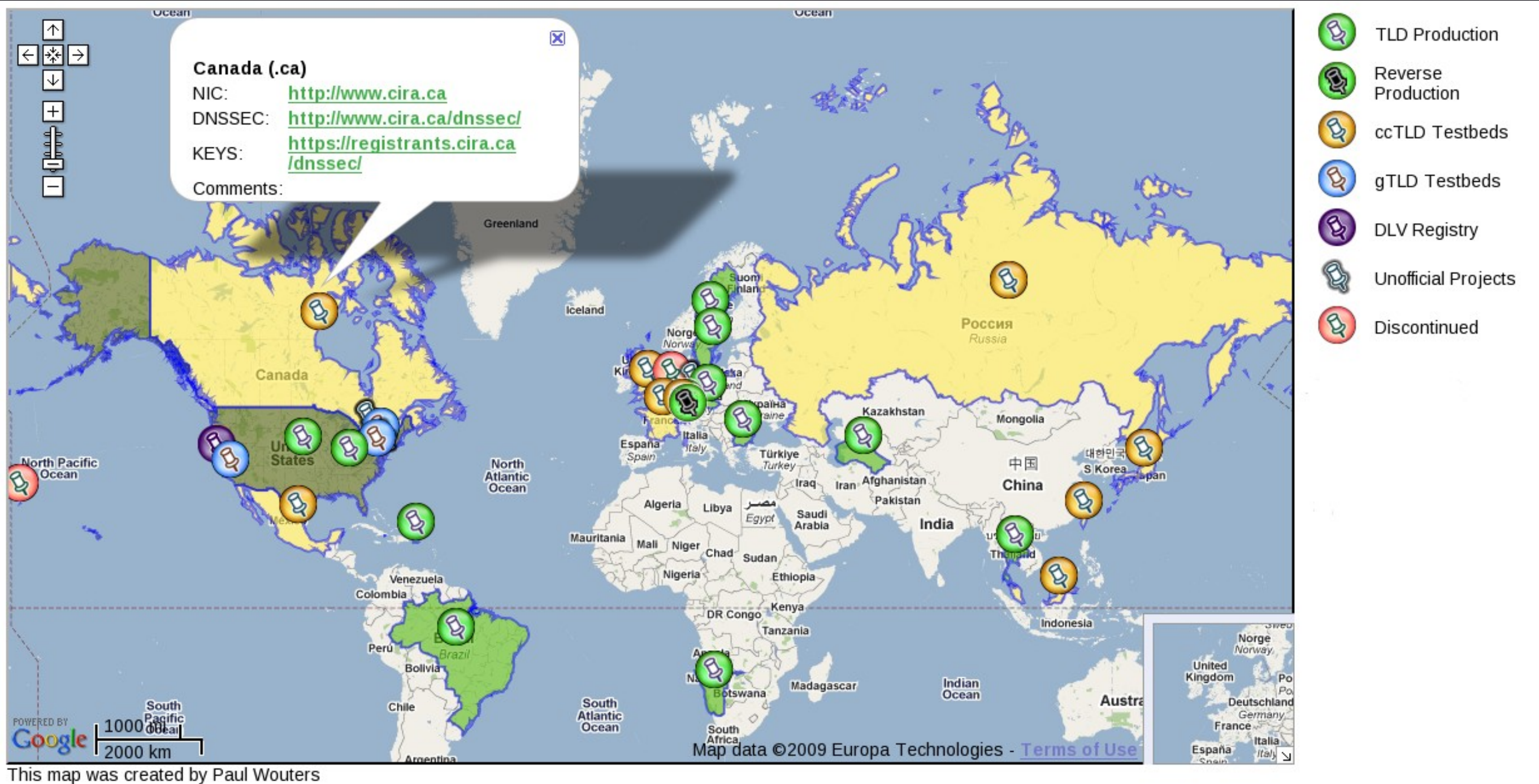
Signing time...

- DNSSEC involves creating keys and signatures.... A lot
- DNS is passive, but DNSSEC is active. This forces the administrator to be pro-active.
- DNSSEC is time sensitive. Monitoring is required!

We are going hunting...

- Keys are everywhere...Can you find them? Keep them up to date?
- If your DNS has the wrong keys, you cannot use DNS to find new keys anymore!
- Maintenance is key!

www.xelerance.com/dnssec/



There's a better way

DNSX

SECURE SIGNER

DNSX

SECURE RESOLVER

DNSX

SECURE SIGNER

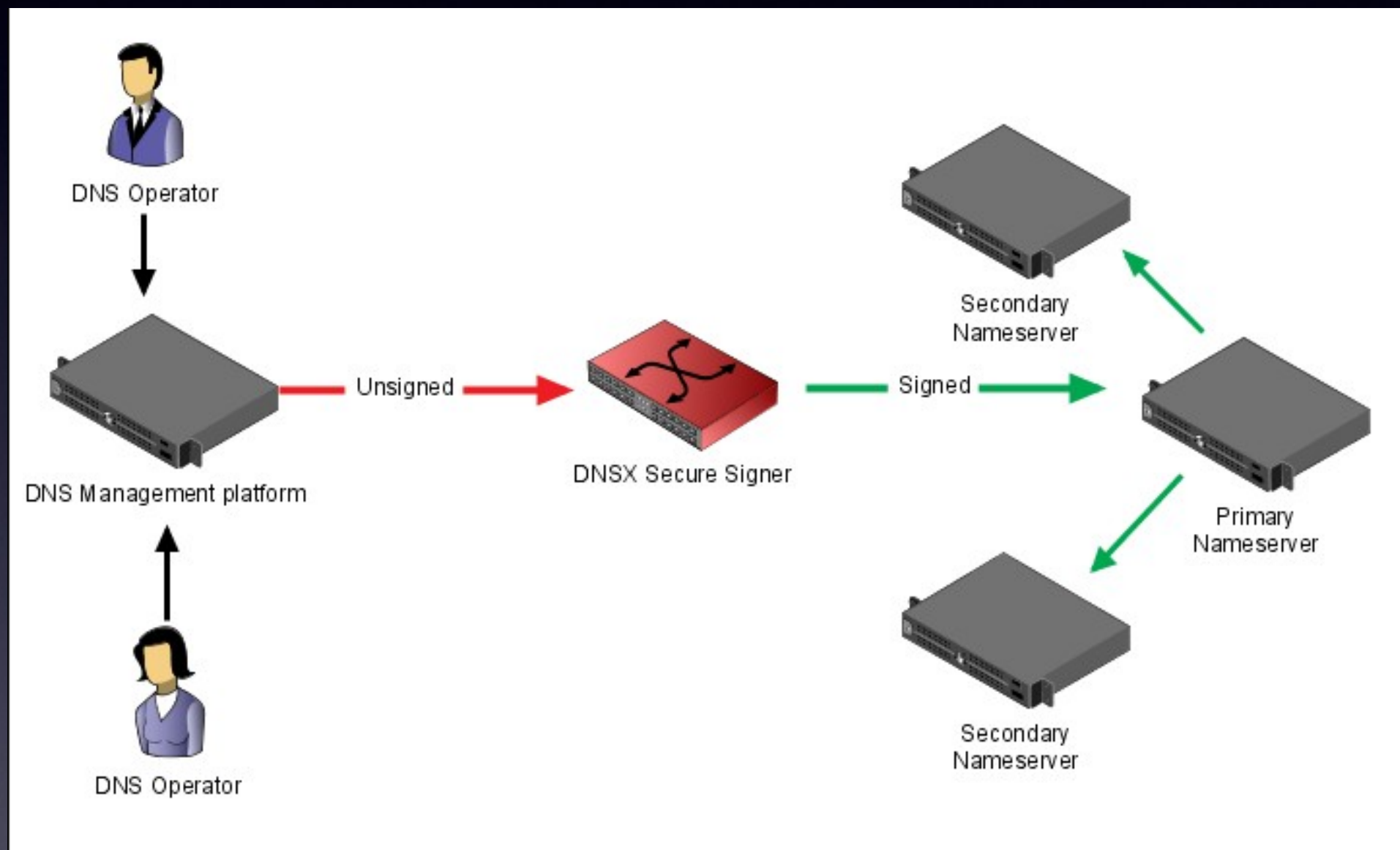
Simple, simple, simple

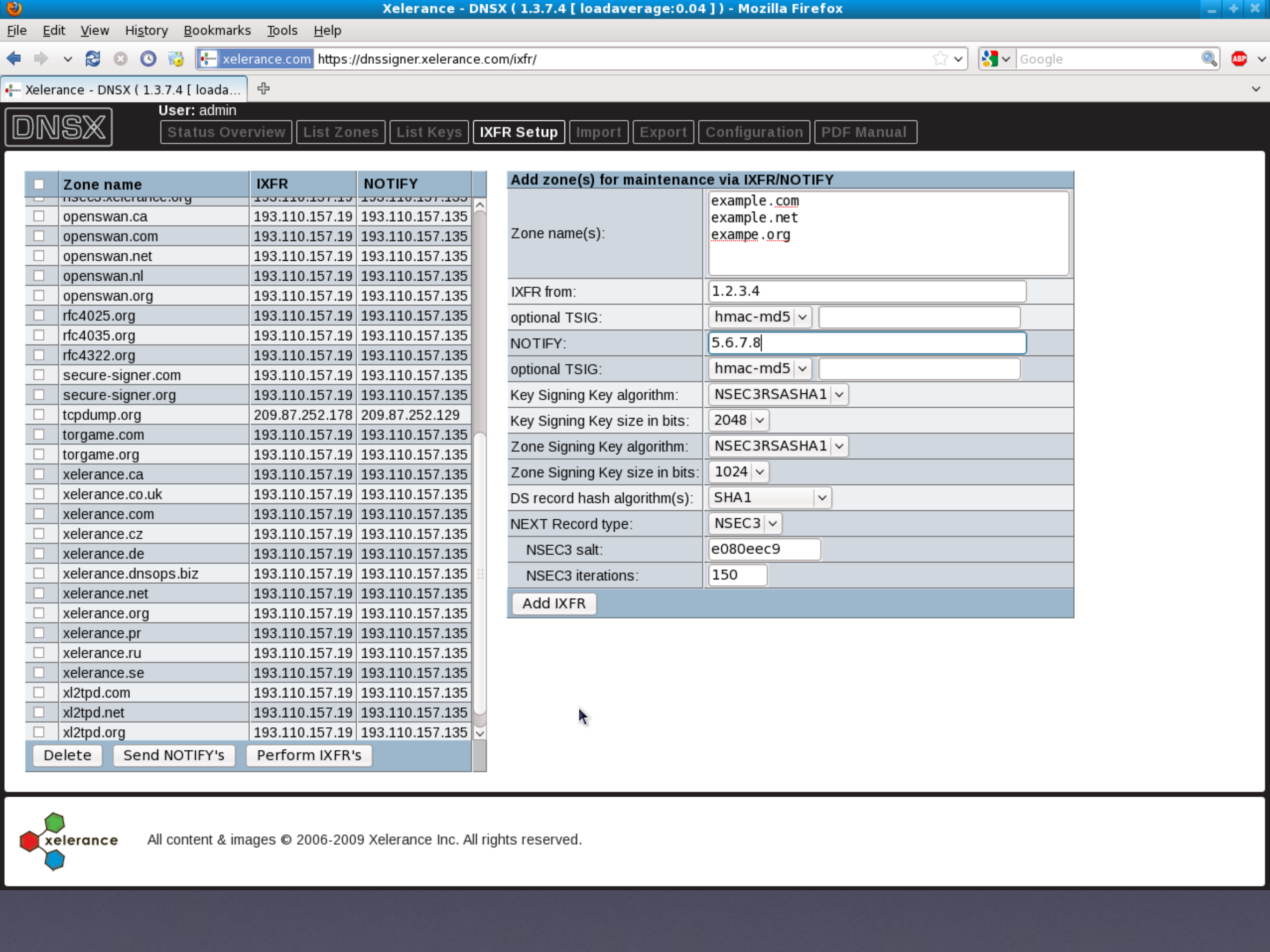
- Proactive DNSSEC management solution
- Extensive WEB interface
- API available for custom integration
- Advanced Active Monitoring
- Support for DLV Registry
- Hardware Security Module: FIPS 140-2 Level3

Did we mention simple ?

- Signature Re-use
- Signature spreading
- Automatic DS record generation
- Domain expiration monitoring
- Name server consistency checks
- Security Officer and User roles

Seamless Integration





Filter

Go

[List Zones In Rollover](#)[List All Zones](#)

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

Update Realtime Status

Save Changes



Xelerance - DNSX (1.3.7.4 [loadaverage:0.21]) - Mozilla Firefox

FileEditViewHistoryBookmarksToolsHelp

↩↲⌂⌚🔍xelerance.comhttps://dnssigner.xelerance.com/zone/xelerance.cz/

☆Google🔍ABP

Xelerance - DNSX (1.3.7.4 [loada...+

DNSX

User: admin

Status OverviewList ZonesList KeysIXFR SetupImportExportConfigurationPDF Manual

DNSSEC OptionsPerform IXFRPerform NOTIFYSign zoneStart KSK RolloverStart ZSK RolloverEmergency Key RolloverDelete zoneShow DNSKEYsShow signedShow 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				

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
PtRFxDIF9qyzDwJGMFlnG4PwEfnkt4gWU4MN
+BD9GLNRhGVMSIayjzq+yRPcew5eD8Z/z4Wh
FcLqJsRr+IYiMjbFfsr1AR4bWY0u0i7x5ChI
BV8xl8HcvXcDAxRa90zVsyzmFhF9vYdyWMM
ssgghQTNGQ3hH+Si1ElU85UsZLb2oUl2cBkp
Xu6UIPeYULPtfsAdec6uku98YFZyQAG+LnSX
s6aFNF1u3nPlBfmgyo37f38="; // key id = 46398

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)

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

xelerance

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

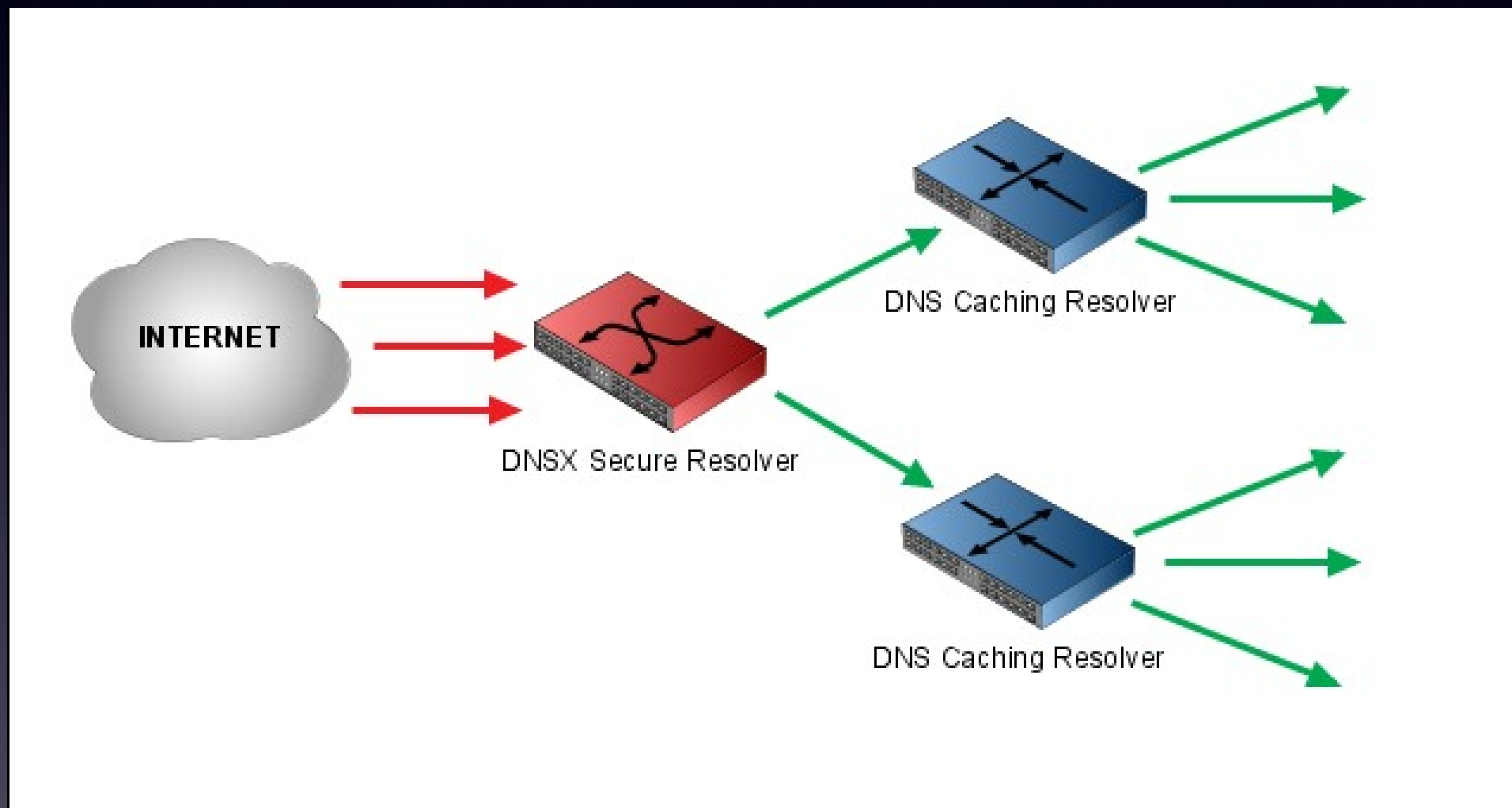
DNSX

SECURE RESOLVER

Preloaded and ready

- Full DNSSEC key management solution
- Supports signed and unsigned root scenarios
- Full DNSSEC and DLV validating resolver
- Support corporate DNSSEC Trust Anchors
- Harden regular DNS traffic
- DNSSEC statistics

Seamless Integration



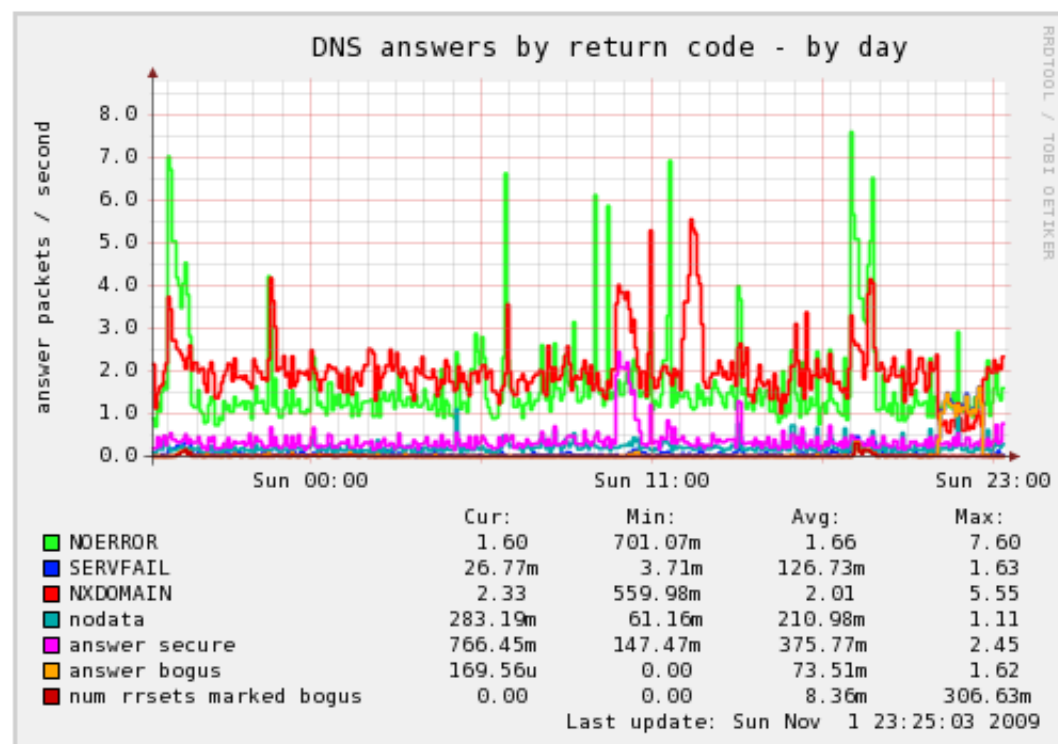
Production keys

<input type="checkbox"/>	Status	Zone	Key id	Type	Revoked	Alg	Public Key
<input type="checkbox"/>	V	bg.	61993	KSK	-	RSASHA1	AwEAAcNs [...] +8hrbDO3
<input type="checkbox"/>	V	bg.	64693	KSK	-	RSASHA1	AwEAAAdSk [...] 9fHq3+TX
<input type="checkbox"/>	V	br.	18457	KSK	-	RSASHA1	AwEAAAdDo [...] jNpy6AM=
<input type="checkbox"/>	V	ca.	46215	KSK	-	NSEC3RSASHA1	AwEAAAbTc [...] ofqO5ec=
<input type="checkbox"/>	V	cz.	7978	KSK	-	RSASHA1	AwEAAAdo9 [...] MnitkuM=
<input type="checkbox"/>	V	dnsops.biz.	53377	KSK	-	RSASHA1	AwEAAAb2O [...] EYHmwak=
<input type="checkbox"/>	V	dnsx.xelerance.com.	38478	KSK	-	RSASHA1	BQEAAAAB [...] Wkw8+Q==
<input type="checkbox"/>	V	gov.	26079	KSK	-	NSEC3RSASHA1	AwEAAAZ1O [...] 4Hf2aM8=
<input type="checkbox"/>	V	museum.	39226	KSK	-	RSASHA1	AwEAAAd4F [...] 2ICwm2E=
<input type="checkbox"/>	V	na.	24484	KSK	-	RSASHA1	AwEAAAc2V [...] Yi7sRk4v
<input type="checkbox"/>	V	org.	21366	KSK	-	NSEC3RSASHA1	AwEAAAYpY [...] AQN49PU=
<input type="checkbox"/>	V	org.	9795	KSK	-	NSEC3RSASHA1	AwEAAAZTj [...] MNoJEHU=
<input type="checkbox"/>	V	pr.	6277	KSK	-	RSASHA1	AwEAAeDP [...] ESgiDXc=
<input type="checkbox"/>	V	se.	49678	KSK	-	RSASHA1	AwEAAAdKc [...] UkNB8Qc=
<input type="checkbox"/>	V	se.	8779	KSK	-	RSASHA1	AwEAAeeG [...] yQgsTlc=
<input type="checkbox"/>	V	th.	38674	KSK	-	RSASHA1	AwEAAAcBg [...] DpbGor0=
<input type="checkbox"/>	V	th.	57559	KSK	-	RSASHA1	AwEAAAcEU [...] a972QT8=

Toggle Selected

Purge Selected

Cache Hits | Reply Time | Memory Usage | Request Type | Request Flags | Return Codes | Request Opcode | Queue



Who are we?

Xelerance

The DNSSEC Experts

- We promote Internet Security through the adoption of DNSSEC and provide solutions to automate and minimize the management overhead of DNSSEC.



Xelerance Corporation

- Based in Canada
- Privately owned
- Involved with DNSSEC longer than any other commercial company.
- Member of IETF, RIPE, DNS-OARC, DHS DNSSEC Deployment Group, DNSSEC Coalition Group.
- Author of DNSSEC related RFC's
- DNS consulting, DNSSEC migrations

Thank you