xelerance

Maintenance is key

DNSX
SECURE SIGNER

DNSX
SECURE RESOLVER

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

Patrick Naubert
patrickn@xelerance.com
www.xelerance.com

Xelerance Corporation

- Based in Canada, privately owned
- DNSX Secure Signer deployed at TLDs, Registrars, universities, US Government, etc.
- DNSSEC consulting clients include TLDs, Registrars, large Canadian bank, Linux distributions, etc.
- Member of IETF, RIPE, DNS-OARC,
  DHS DNSSEC Deployment Group, DNSSEC Coalition Group, Fedora Linux
- Author of DNSSEC related RFCs
- Presented at Black Hat, GovSec, SANS, SecTor, CanSecWest, InfoSecurity Canada, DNS-OARC, etc.

xelerance

DNSX SECURE SIGNER

DNSSEC made simple

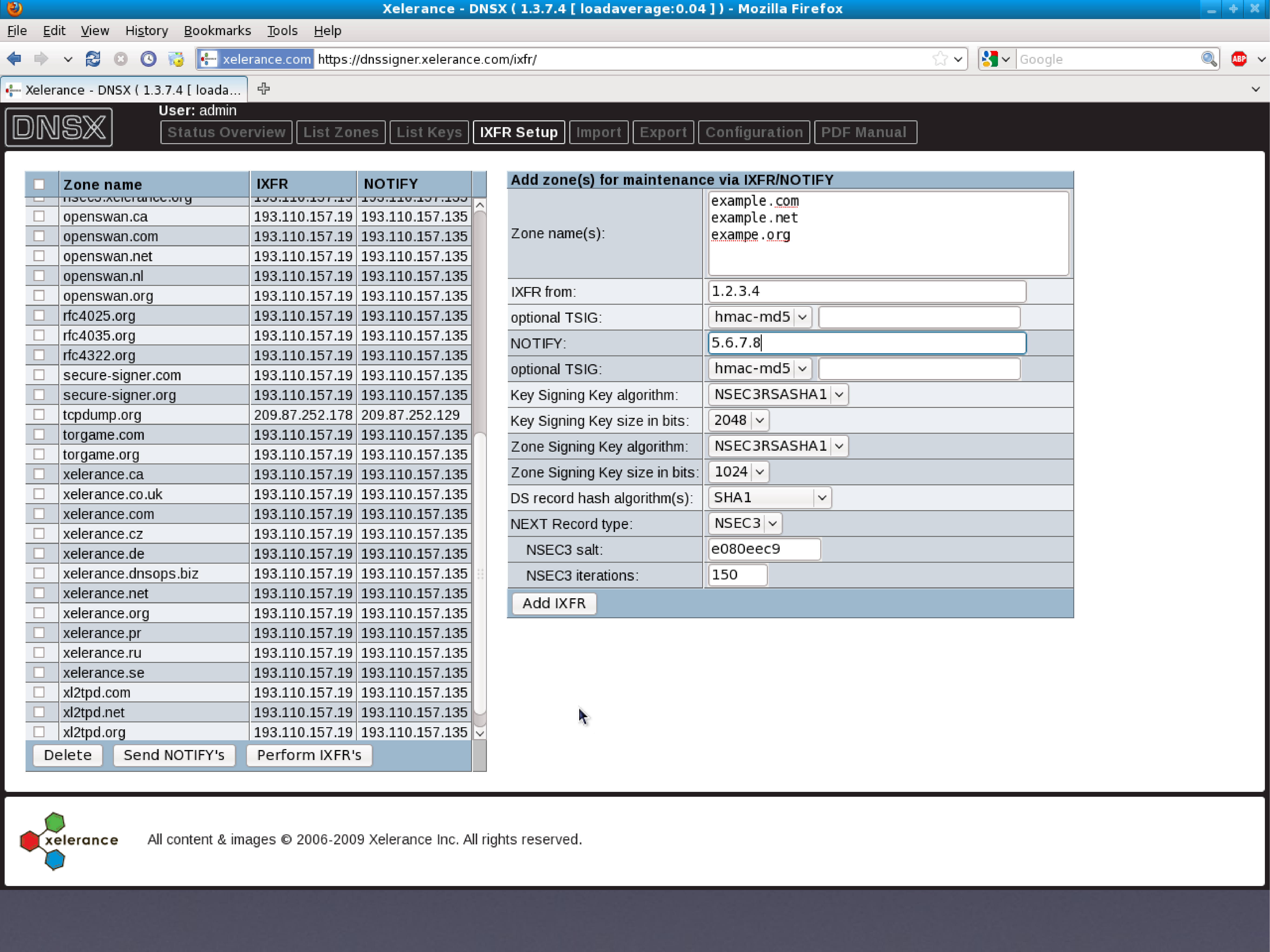
- Proactive DNSSEC management solution
- Extensive WEB interface
- JSON API available for custom integration
  - iphone example app, easy website integration
- Advanced Active Monitoring
- Seamless integration with IXFR, AXFR and TSIG
- Hardware Security Module: FIPS 140-2 Level3

Did we mention simple ?

- Fully automated KSK rollover
- DS record submission to supporting Registrars
  - GoDaddy, GKG.net, InternetX, etc.
- DLV record submission to ISC DLV Registry
- Signature re-use and expiry spreading
- Domain expiration monitoring
- DNS early warning system

Secure resolving

- Full DNSSEC and DLV validating resolver
- Powerful web interface for key configuration
- Support corporate DNSSEC Trust Anchors
- Harden regular DNS traffic
- DNSSEC statistics
- Cache and DNSSEC validation diagnostics

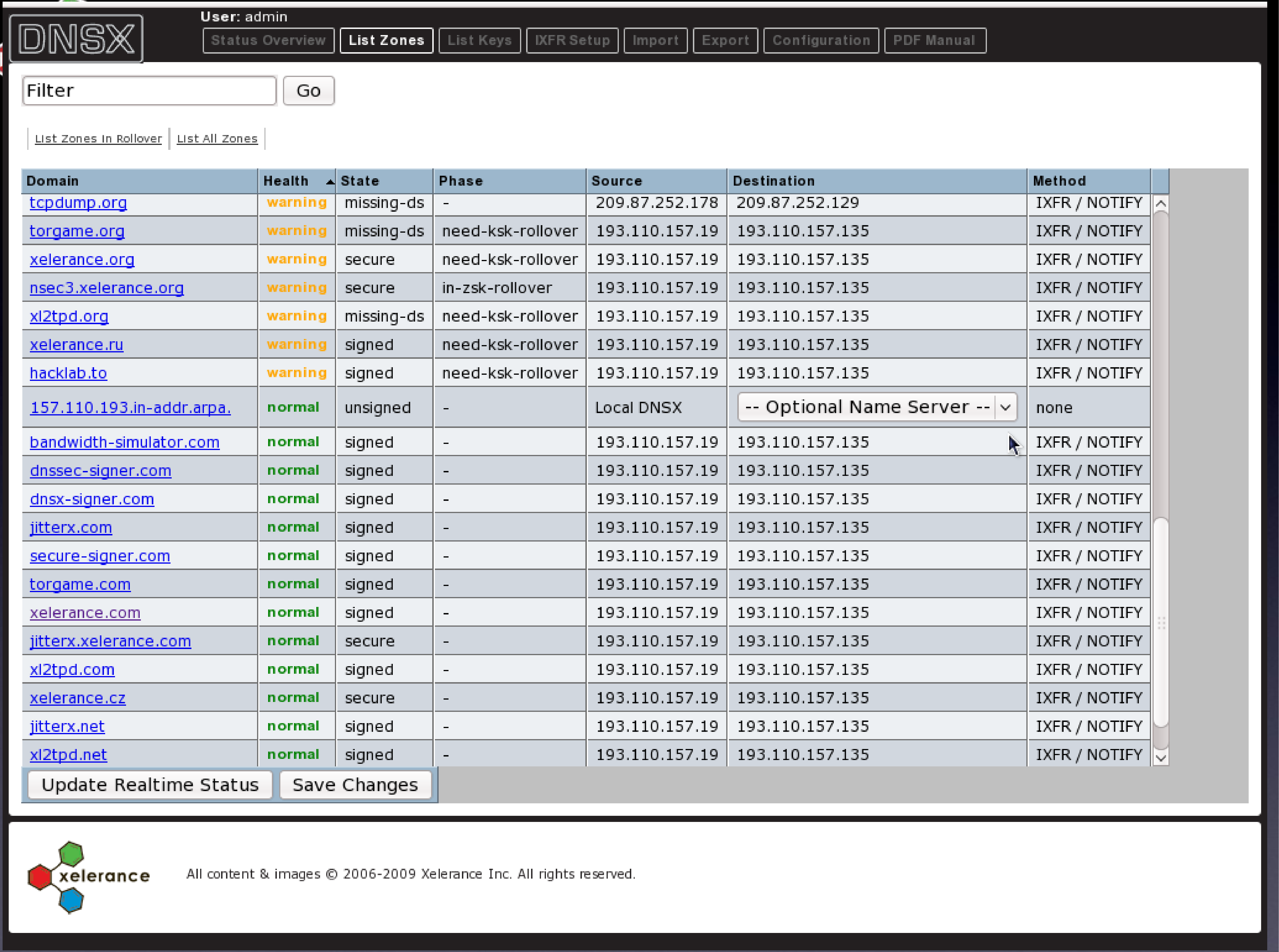


□	Zone name	IXFR	NOTIFY
□	nsec3.xelerance.org	193.110.157.19	193.110.157.135
□	openswan.ca	193.110.157.19	193.110.157.135
□	openswan.com	193.110.157.19	193.110.157.135
□	openswan.net	193.110.157.19	193.110.157.135
□	openswan.nl	193.110.157.19	193.110.157.135
□	openswan.org	193.110.157.19	193.110.157.135
□	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

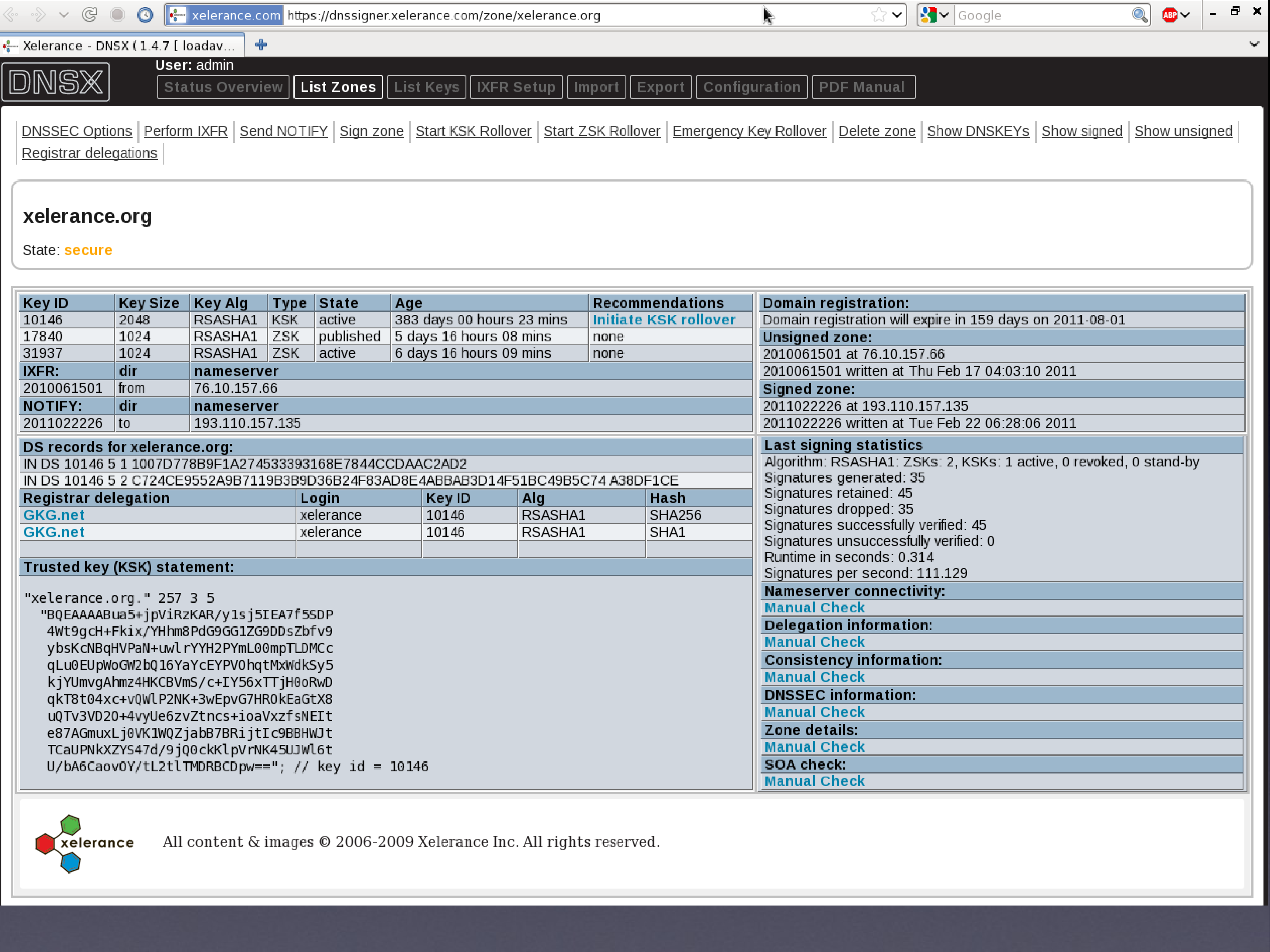
Add zone(s) for maintenance via IXFR/NOTIFY

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.



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


xelerance.com
https://dnssigner.xelerance.com/zone/xelerance.org
Google
Xelerance - DNSX (1.4.7 [loadav...
DNSX
User: admin
Status Overview
List Zones
List Keys
IXFR Setup
Import
Export
Configuration
PDF Manual
DNSSEC Options | Perform IXFR | Send NOTIFY | Sign zone | Start KSK Rollover | Start ZSK Rollover | Emergency Key Rollover | Delete zone | Show DNSKEYs | Show signed | Show unsigned | Registrar delegations

xelerance.org

State: secure

Key ID	Key Size	Key Alg	Type	State	Age	Recommendations
10146	2048	RSASHA1	KSK	active	383 days 00 hours 23 mins	Initiate KSK rollover
17840	1024	RSASHA1	ZSK	published	5 days 16 hours 08 mins	none
31937	1024	RSASHA1	ZSK	active	6 days 16 hours 09 mins	none

IXFR:	dir	nameserver
2010061501	from	76.10.157.66
NOTIFY:	**dir**	**nameserver**
2011022226	to	193.110.157.135

Domain registration:

Domain registration will expire in 159 days on 2011-08-01

Unsigned zone:

2010061501 at 76.10.157.66

2010061501 written at Thu Feb 17 04:03:10 2011

Signed zone:

2011022226 at 193.110.157.135

2011022226 written at Tue Feb 22 06:28:06 2011

DS records for xelerance.org:

IN DS 10146 5 1 1007D778B9F1A274533393168E7844CCDAAC2AD2

IN DS 10146 5 2 C724CE9552A9B7119B3B9D36B24F83AD8E4ABBAB3D14F51BC49B5C74 A38DF1CE

Registrar delegation	Login	Key ID	Alg	Hash
GKG.net	xelerance	10146	RSASHA1	SHA256
GKG.net	xelerance	10146	RSASHA1	SHA1

Trusted key (KSK) statement:

```
"xelerance.org." 257 3 5
  "BQEAAAABua5+jpViRzKAR/y1sj5IEA7f5SDP
   4Wt9gcH+Fkix/YHhm8PdG9GG1ZG9DDsZbfv9
   ybsKcNBqHVPaN+uwlrYYH2PYmL00mpTLDMCc
   qLu0EUpWoGW2bQ16YaYcEYPVOhqtMxWdkSy5
   kjYUmvgAhmz4HKCBVmS/c+IY56xTTjH0oRwD
   qkT8t04xc+vQWlP2NK+3wEpvG7HROkEaGtX8
   uQTv3VD2O+4vyUe6zvZtncs+ioaVxzfsNEIt
   e87AGmuxLj0VK1WQZjabB7BRijtIc9BBHWJt
   TCaUPNkXZYS47d/9jQ0ckKlpVrNK45UJWl6t
   U/bA6CaovOY/tL2tlTMDRBCDpw=="; // key id = 10146
```

Last signing statistics

Algorithm: RSASHA1: ZSKs: 2, KSKs: 1 active, 0 revoked, 0 stand-by
Signatures generated: 35
Signatures retained: 45
Signatures dropped: 35
Signatures successfully verified: 45
Signatures unsuccessfully verified: 0
Runtime in seconds: 0.314
Signatures per second: 111.129

Nameserver connectivity:

Manual Check

Delegation information:

Manual Check

Consistency information:

Manual Check

DNSSEC information:

Manual Check

Zone details:

Manual Check

SOA check:

Manual Check