DNSSEC Deployment in Canada

Norm Ritchie
norm.ritchie@cira.ca

Paul Wouters
paul@xelerance.ca
Who is CIRA?

- Canadian Internet Registration Authority
  - Not-for-profit corporation delegated the dot-ca domain
- Manage the dot-ca domain
  - Domain name registry, whois service and authoritative DNS
  - Policy development
  - Registrar accreditation
  - Dispute resolution
- Represent Canada as a member of ICANN and other international organizations
Who is Xelerance?

- DNSSEC consultants
- DNSSEC appliance vendor
- IETF & RIPE participant (dnsops, dnsext, dnswg)
  - (co) author of Internet standards (RFC's)
- Member of DNS-OARC (DNS at the TLD level)
- Member of DNSSEC Deployment (US government)
- Author of open source software (Linux IPsec, DNS etc)
Today's Session

- Why DNSSEC
- Status of global deployment
- Status of CIRA's deployment
- DNSSEC Primer
- How to setup DNSSEC with 3 commands
- Demonstration of Test Bed
Current DNS Limitations

- DNS is fundamentally insecure
- Vulnerable to “Man In The Middle” attacks
  - Insecure wi-fi (Airport hotspots, Starbucks, etc)
  - Compromised ISP name servers
  - Malicious redirection to online advertisement websites
- Vulnerable to name server compromises
- Attacks more successful due to increased bandwidth
- Vulnerable to data poisoning
Cache poisoning attack – brute force
The Summer of Fear: Kaminsky Vulnerability

Without source port randomization, this only takes about 65535 packets

If you lose the race, try bogus12346

Overrides cache
What is DNSSEC?

➤ RFCs for adding digital signatures to DNS data
➤ Provides authenticity of data
➤ Adds secure delegations from parent to child, creating trust hierarchies (“path of trust”)
➤ Provides provable denial of existence
➤ Compromised name servers detected and ignored
➤ DNS data manipulation detected and ignored
Why deploy DNSSEC now?

- The Kaminsky vulnerability is still a serious exploitable risk
- Increased DNS and name server attacks
- DNSSEC tools have matured enough
  - With RFC-5155 ("NSEC3") confidentiality of the zone remains intact
- Operating System vendors have implemented DNSSEC for end-users. ISPs are starting to deploy or test DNSSEC-capable resolving name servers
Why deploy DNSSEC now?

- ICANN deployed “Interim Trust Anchor Repository” to ease TLD DNSSEC key distribution to third parties
- ISC's DNSSEC Lookaside Verification (DLV) Registry assists signed domains within unsigned TLD's (.com)
- The root should be signed June 2010
- There is good operational experience by various TLDs
Phases of DNSSEC Deployment at CIRA

- Research and analysis of impact (completed)
- Deployment of signed zone to test bed (completed)
- Initial testing with hand picked zones (started)
- "Friends & Family" phase (starting today!)
  - Open for all interested parties
    - DNS admins, ISPs, banks, government, consultants, you
- Migrate deployment from testing to production (late 2010)
Some interesting findings

• Zone file grew from 180MB to 670MB
• Software signing on 16 core Xeon E5540 @2.53ghz yields 3900 1024bit RSA sigs/second (5-10 minutes)
• Hardware signing on the same machine using a Sun SCA6000 HSM (FIPS 140-2 Level 3) card yields 1700 sigs/second (benchmark yields 13000 sigs/second)
• Zone signing takes between 5-15 minutes depending on signature re-use
Operational experiences with DNSSEC

• named grew to 4+ GB of RAM on pri. and sec. ns
  – On 32bit machines, max is 3GB of RAM per process!

• Any zone size increase x2 due to zone reloading

• If named runs out of ram in AXFR/IXFR, it tries again!
  – Consuming endless bandwidth between primary and secondaries

• Zone will double again during an algorithm rollover (eg NSEC3RSASHA1 to RSASHA256 in the near future)
Continued effort on DNSSEC

- Continued involvement with the DNS community
  - DNS-OARC, ICANN, IETF, RIPE, dnssec-deployment, DNSSEC Coalition, Registrars, etc
- Continued analysis of impact on DNS infrastructure
- Assist with development of open source DNS software
- Some open issues yet to be resolved
  - How to receive keys? From Registrar or Registrant? Transfers?
  - Monitoring? What to do if we detect broken DNSSEC at Registrant?
  - Automatic Registrant key updates ("triggers or timers")?
Friends and Family
Friends & Family phase: A short HOWTO

- 5 Minute primer on DNSSEC
- Using the signed .ca zone on your computer or phone
- Using the signed .ca zone on your name servers
- How to sign your zone using 3 simple commands
- Submitting DNSSEC keys for your domains to CIRA
- Verifying the correct operations of your signed zone.
- Troubleshooting
Components of DNSSEC

- Collector - takes public keys from Registrants
- Signer - creates and “rolls over” cryptographic keys and digital signatures for all DNS data
  - This includes signing the Registrant's public key fingerprints
- Authoritative name server - serves the signed zone
- Validating resolving name server - verifies public keys, signatures and passes DNS data to applications
Traditional DNS

The root (".") \rightarrow .com \rightarrow xelerance.com
Add a public key to zone
Sign zone with private key
Give hash(pubkey) to parent
Rinse and Repeat
New DNS Resource Record types

- The DNSKEY record
- The RRSIG record
- The NSEC record
- The NSEC3 record
- The DS record
- The public key
- The digital signature
- Enumerate the data present and absent
- Improved privacy over NSEC3
- Build path of trust to child zone
New DNS flags (bits in packet)

- The DO bit
- The AD bit
- The CD bit
- DNSSEC OK
- Authenticated Data
- Checking Disabled
After DNSSEC validation, answers can be

- Secure – Validated from a trusted key
- Insecure – Validated where possible, no trusted key
- Bogus – Invalidated (wrong key, expired signature, etc)
- Unknown – ServFail, etc.
Signed zone example

```
xelerance.ca. 3600 IN SOA ns1.xelerance.net. hostmaster.xelerance.ca. (2009102902 ; serial 18000 ; refresh (5 hours) 3600 ; retry (1 hour) 864000 ; expire (1 week 3 days) 3600 ; minimum (1 hour)
)
3600 RRSIG SOA 5 2 3600 20091026214457 (20091001122509 16187 xelerance.ca. [...]04ywbf88121cZ2zDLY/LCFhQwFQE= )
3600 NS ns1.xelerance.net.
3600 RRSIG NS 5 2 3600 20091021212855 (20090922203009 16187 xelerance.ca. [...]713hZAfqTss0VA0bHs5JtwUlwC= )
3600 MX 20 cdc.xelerance.ca.
3600 RRSIG MX 5 2 3600 20091024013204 (20091001122509 16187 xelerance.ca. [...]39X9TL5LwSDEk1y5fONGRn3Zn+0= )
3600 DNSKEY 256 3 5 ( [...]1kBILtcsGQr9B0Ki6mlVw/4z8ulXrYHxUE= ) ; key id = 8060
3600 DNSKEY 257 3 5 ( [...]1yMnLoFJg2SeiK+rpuZLeQ2CCvw== ) ; key id = 58980
3600 RRSIG DNSKEY 5 2 3600 20091021212114 (20090924185012 16187 xelerance.ca. [...]k4li5PBm4wKg/nGJ1TjeyH0U2tM= )
3600 RRSIG DNSKEY 5 2 3600 20091026193516 (20090928213509 58980 xelerance.ca. [...]37qeauK+Ls1CY99ePQ== )
3600 NSEC _sip._tcp.xelerance.com. A NS SOA MX RRSIG NSEC DNSKEY
3600 RRSIG NSEC 5 2 3600 20091028012921 (20090924185012 16187 xelerance.com. [...]1s73Eq7rLuS8qj31Br3PB0HsQ= )
3600 NSEC _sip._tcp.xelerance.ca. 3600 IN SRV 1 0 5060 toronto.xelerance.ca.
```
NSEC zone

bofh.xelerance.ca. 3600 IN A 193.110.157.17
3600 RRSIG A 5 3 3600 20091024233648 (20090928213509 16187 xelerance.ca. [...])plz4KqvtSE8I6hZyHppiq5qHJ0k=)
3600 NSEC bugs.xelerance.ca. A RRSIG NSEC
3600 RRSIG NSEC 5 3 3600 20091018044015 (20090922203009 16187 xelerance.ca. [...])f3h26Y92bprLmnnvkDsm8J1oq34=)

bugs.xelerance.ca. 3600 IN A 193.110.157.140
3600 RRSIG A 5 3 3600 20091018221741 (20090922203009 16187 xelerance.ca. [...])HTrThjKWQ8hfaWyyVYLMf+Osd=)
3600 NSEC build.xelerance.ca. A RRSIG NSEC
3600 RRSIG NSEC 5 3 3600 20091017105726 (20090922203009 16187 xelerance.ca. [...])zFS+JoLFoYCdYfC4/pX6W+8FBG=)

build.xelerance.ca. 3600 IN A 193.110.157.194
3600 RRSIG A 5 3 3600 20091029034706 (20091001122509 16187 xelerance.ca. [...])AxLzhY0HhVE0cpXW1ft0fBfn8=)
3600 NSEC calendar.xelerance.ca. A RRSIG NSEC
3600 RRSIG NSEC 5 3 3600 20091020222431 (20090922203009 16187 xelerance.ca. [...])moTgbQ/UINbotP/Hi/sgRhXnaw9VU=)

calendar.xelerance.ca. 3600 IN A 193.110.157.130
3600 RRSIG A 5 3 3600 20091028221520 (20091001122509 16187 xelerance.ca. [...])CmhFG2zsiju9SW8mcHr6gAUFy8=
3600 NSEC calender.xelerance.ca. A RRSIG NSEC
3600 RRSIG NSEC 5 3 3600 20091017125356 (20090928213509 16187 xelerance.ca.)
View of a signed child in the `.ca` zone

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Class</th>
<th>TTL</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>xenadrine-xtreme-fx.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>iodns1.iovate.com</td>
</tr>
<tr>
<td>xenadrinebanned.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>iodns2.iovate.com</td>
</tr>
<tr>
<td>xenadrinecasestudies.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>iodns1.iovate.com</td>
</tr>
<tr>
<td>xelerance.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>ns0.xelerance.nl</td>
</tr>
<tr>
<td>xelerance.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>ns1.xelerance.net</td>
</tr>
<tr>
<td>xelerance.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>ns2.xelerance.org</td>
</tr>
<tr>
<td>xelerancediet.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>iodns1.iovate.com</td>
</tr>
<tr>
<td>xelerancedietpills.ca</td>
<td>IN</td>
<td>NS</td>
<td>86400</td>
<td>iodns2.iovate.com</td>
</tr>
</tbody>
</table>
View of the NSEC3 chain in the .ca zone

000F1773M1813N59TE4HBW5573LNBK.ca. 3600 IN NSEC3 1 0 10 AAAA 000F45V7UHTQT35FAAA9VYVDCM1KPJDRIU NS 3600 RRSIG NSEC3 7 2 3600 20091012195338 ( 2009100601712 8090 ca.
QSU6EbH0UXWL8yVQxTPloRKLFObg/vL6j0TS KehG6zP108T46jpBNAL4C02b11Gw6xY83N xLC859N5A/8YLLRtvv8bejM5KyjZJg1mX fgpLPTDymovpXAdVEUFdUBCR6CyqLg0HYn mn1lCw+u5+opTBEk+1xwTjEmX= )

0008M60K58KJ0HTE3VODEEG0S2304B1K.ca. 3600 IN NSEC3 1 0 10 AAAA 0009IIPHGE9U9E6AF3CMBPV1PP5042N3 NS 3600 RRSIG NSEC3 7 2 3600 20091011185305 ( 20090828201820 8090 ca.
PzY4C9tpY0E8hdQHxZHFT1L46j6RJra7VM68aKn 31jEU6i06K3f1czaa451cixO20HCT4Hd0D 5WRplO8V8X1q30A4gjDzwXmt0XP6y6y62UZ UEhUTY2q7Jiam2V91r+OTPfaPMU8iF9H2zg JsEolBAJkC3qSYK5dpnvvIByvo= )

000AL4M3RVMQH6V7SN10CU7MPPDS41K6.ca. 3600 IN NSEC3 1 0 10 AAAA 000DUC51VVDHJ36706B1D4T44FT44U4LEA NS 3600 RRSIG NSEC3 7 2 3600 20091014061403 ( 2009100211712 8090 ca.
ll/q4s55F3e07b36brkVYydwZ03qso50oULS f3HvICKnd/0n//Ph457WQMG+iXDi5nJUML mcA02ZpdpTzNqL0qdsjP2KhDpcXe2P1q+e35 S1Rb8qkrq+Ps700L15+uLEd0r1q+ied9Gx5U
Using the signed .ca zone on your computer

- Use our DNSSEC capable resolvers that have the .ca key (and all other production TLD keys)
- Europe: 193.110.157.136

- If you're reading this at Sector2009, DHCP gave these to you already!
Using the signed .ca zone with Unbound NS

- Download ca.conf: https://registrants.cira.ca/dnssec/
- Add a trusted-key statement:
  trusted-keys-file: "/etc/unbound/ca.conf"
- Add the .ca zone as stub:
  stub zone:
    name: “ca.”
    stub-addr: 192.228.22.190
    stub-addr: 192.228.22.189
    stub-prime: “no”
Using the signed .ca zone with the Bind NS

- It's very complicated to use the authoritative servers, due to priming of the unsigned NS records in the root.
- Use a forward zone and the resolvers instead.
- First enable DNSSEC in the options `{ }` section:
  
  `dnssec-enable yes;`
  `dnssec-validation yes;`

- Download and add the ca key file in `named.conf`:
  `include "/etc/named/ca.conf"`
Using the signed .ca zone with the Bind NS

• Add the forwarding zone for .ca:

  zone “ca.” IN {
    type forward;
    forwarders { 66.241.135.248; 193.110.157.136; }
  }
Common DNS Deployment
Integrating DNSSEC in existing deployments
Generate DNSSEC keys using Bind tools

- Generate two DNSKEY records
  - Zone Signing Key (ZSK) signs all DNS data in the zone
  - Key Signing Key (KSK) signs ZSK. Its fingerprint goes to parent zone.

```bash
$ dnssec-keygen -a NSEC3RSASHA1 -b 2048 -e -f KSK yourzone.ca
Kyourzone.ca.+007+62091
$ dnssec-keygen -a NSEC3RSASHA1 -b 1048 -e yourzone.ca
Kyourzone.ca.+007+61598
$ cat Kyourzone.ca.+007+6*key
yourzone.ca. IN DNSKEY 256 3 7 AwEAAfVULWe0aZEFKyqsgAEQZhcMfvzHYphvFJIfrAlbA0Jcr904IvrP AV9gJqc3j9WTFKAA36TF4SMU7Hsf6CkbbqGpF5EvRFsgHsGum1curnA uPVEsicIPMSKTgmFCR+W5r500W5CRIlsiczfzih88Vv0GCwthp20RKqojFpKNcgQ0Ytj
yourzone.ca. IN DNSKEY 257 3 7 AwEAAadrZibrxuPqYi/PYmTxHhjRUuSLmICU+j5ETdU2LT8uHcAj1xe5Y DTGIDEcp c5LzzFjnRR2NJwpLiiORxzd1EYhIC4Hy4FVavwpMwRFZTaHR df6Ljxhw01fHteCrpwVunS/ef1ZnoPeKNEWoBuYgfWpPkiZJ AAy04GsLS/AwNDRGdsgFvcElbsGGRJ51PNTcrVEhVQqaj850ZMrLcmv05jdKXbfh 3Sy/9jD3wT07BjKX/OigKoDDYaspG NycUfXzwCwh6RhcAK2fn6KqT3bM 3lpmzVwC/TiCsJqHYoGM3i5VvVrTEWE7SqulKHKIDyxVfVmgCcn74qUKl3 AKyJeGT+zL0
```
Sign zone using Bind tools

- `dnssec-signzone -3 c0ffee -H 100 -i 604800 -e \
  +1209600 -j 604800 -t -o yourzone.ca \
  -f yourzone.ca.signed -k Kyourzone.ca.+007+62091 \
  /zone/yourzone.ca Kyourzone.ca.+007+61598`
Submit your key to CIRA

• https://registrants.cira.ca/dnssec/
• Add yourself to the mailing list, dnssec@cira.ca
• Give us feedback
Canadian Internet Registration Authority

User ID

Password

Login

Forgot your userid and/or password?

© 2009 Canadian Internet Registration Authority. All rights reserved

By accessing and using CIRA’s website you agree that you have read, understood, and consent to the terms and conditions for the use of CIRA’s website, as set out in the Website Terms of Use and Privacy Policy.
Forgot your User Account and password?

Enter your dot-ca (.ca) domain name:

hypatia.ca
(e.g. example.bc.ca)

What is this?

Type the characters from the image above.

Type characters: fnznZ

Submit Cancel
## DNSSEC Key Manager

Welcome Registrant #1

<table>
<thead>
<tr>
<th>Domain</th>
<th>Status</th>
<th>Keys on file</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>hacklab.ca</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>hypatia.ca</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
</tbody>
</table>

Log Out
DNSSEC DS key registration for hypatia.ca.

The following DNSKEY secure entry point (SEP) RR was received from 64.86.69.71 at 13:07:09 03-Oct-2009:

Please verify it is the one you wish to include for your trust anchor in the CA zone.

```plaintext
DNSKEY

hypatia.ca. 3680 IN DNSKEY 257 3 5 (BQEA...Xu82p512UgXK6x...

DS Records

SHA1  hypatia.ca. IN DS 20664 5 1 901007A295E60378900B18CAAJAD3DF244F3F32
SHA256 hypatia.ca. IN DS 20664 5 2 1A2CS54390649017FC0B14E1966172F12A7B1831373F42D41FBE2093F55AF

NOTE: It will take a few moments to process your registration request. During registration processing, validation using DNSCheck is performed. This validation can take a little while to run.
```
DNSSEC key registration successful for hypatia.ca.

The following DS record(s) have been registered:

hypatia.ca. 3600 IN DNSKEY 257 3 5 (BQEAAAAB6XhWPSa6bet2ye5CLka2gsQ41l/Ff42jUSTS2lnStrLTfNDqATruLXc+owpq12UgXK6x
shX5eTq1L4oPlwrmC9uOu2bTFx4vX7dLns203d6HgxelMo0wCE8B1pIDcf8gX6BfrrY5GkU9kQkMS
rJuTuoWtbp58U7qqWjzjd2Q+0VJBoz/+1dflhL9kJ3UAFoB+eIHtaBj7d7S85IrnRqHFr4y
ICSuT8ioMjnHtPjC6ETX4Hg4Wd/CADE+h9cu3VkPj3GkSwXepe+mQe3lZREoKkICOQauBy
syyONj/D4F8pVJMNkqjHdF2aAv2dlnvMKN5jo+axbjmq== ) ; Key ID = 20664

DS Records
SHA1  hypatia.ca. IN DS 20664 5 1 901007A295E637B9B018CAA7A03D6F244F3F32
SHA256 hypatia.ca. IN DS 20664 5 2 1A2C5343E9D649017FCB814E1C966172F12A781B31373F42D41FBE2093F55AFE

Additionally, DNSCheck validation was successful. Here are your DNSCheck results:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:08:10.123</td>
<td>INFO</td>
<td>Begin testing zone consistency for hypatia.ca.</td>
</tr>
<tr>
<td>13:08:14.632</td>
<td>INFO</td>
<td>SOA at address 64.86.69.71 has serial 2009100249.</td>
</tr>
<tr>
<td>13:08:14.760</td>
<td>INFO</td>
<td>SOA at address 193.110.157.135 has serial 2009100249.</td>
</tr>
<tr>
<td>13:08:14.869</td>
<td>INFO</td>
<td>All SOA records have consistent serial numbers.</td>
</tr>
<tr>
<td>13:08:14.869</td>
<td>INFO</td>
<td>All SOA records are consistent among all name servers.</td>
</tr>
<tr>
<td>13:08:14.869</td>
<td>INFO</td>
<td>Begin testing security for hypatia.ca.</td>
</tr>
</tbody>
</table>
13:16:36.447 ERROR 2 different serials found.
13:16:36.447 INFO  All SOA records are consistent among all name servers.
13:16:36.447 INFO  Done testing zone consistency for xelerance.ca.
13:16:36.447 INFO  Begin testing DNSSEC for xelerance.ca.
13:16:36.486 INFO  Did not find DS record for xelerance.ca at parent.
13:16:36.516 INFO  Nameserver 64.86.69.71 does DNSSEC extra processing.
13:16:37.222 INFO  Servers for xelerance.ca have consistent extra processing status.
13:16:37.222 INFO  Broken chain of trust for xelerance.ca - DNSKEY found at child, but no DS was found at parent.
13:16:37.223 INFO  Checking DNSSEC at child (xelerance.ca).
13:16:37.223 INFO  DNSKEY xelerance.ca (tag 4380) is marked as a secure entry point (SEP).
13:16:37.223 INFO  At least one mandatory algorithm found for DNSKEY xelerance.ca.
13:16:37.224 INFO  DNSSEC signature RRSIG(xelerance.ca/IN/DNSKEY/1148) matches records.
13:16:37.224 INFO  DNSSEC signature valid: RRSIG(xelerance.ca/IN/DNSKEY/1148)
13:16:37.226 INFO  DNSSEC signature valid: RRSIG(xelerance.ca/IN/DNSKEY/4380)
13:16:37.226 INFO  Enough valid signatures found for xelerance.ca.
13:16:37.255 ERROR DNSSEC signature RRSIG(xelerance.ca/IN/SOA/1148) does not match the records it signs: key 1:RSA
     Verification failed key 2: keytag does not match key 3: keytag does not match
13:16:37.255 ERROR Not enough valid signatures over SOA RRset found for xelerance.ca.
13:16:37.255 INFO  DNSSEC child checks for xelerance.ca complete.
13:16:37.255 INFO  Done testing DNSSEC for xelerance.ca.
## DNSSEC Key Manager

Welcome Registrant #1

<table>
<thead>
<tr>
<th>Domain</th>
<th>Status</th>
<th>Keys on file</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>hacklab.ca</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>hypatia.ca</td>
<td>ACT</td>
<td>1 key(s) on file</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
<tr>
<td>[redacted]</td>
<td>ACT</td>
<td>Add Key</td>
</tr>
</tbody>
</table>

Log Out
View Keys for domain hypatia.ca

The following DS records are on file for this domain:

<table>
<thead>
<tr>
<th>KEYID</th>
<th>DS Records</th>
<th>De-register</th>
</tr>
</thead>
<tbody>
<tr>
<td>20064</td>
<td>SHA1 20064 5 1 901007A295E5037B909018CAA7A03D0F244F3F32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SHA256 20064 5 2 1A2C5343E9D649017FC8B14EC966172F12A7B1B31373F42D41FBE2D93F55AFE</td>
<td></td>
</tr>
</tbody>
</table>

Return to domain list

Log Out

© 2009 Canadian Internet Registration Authority. All rights reserved

By accessing and using CIRA's website you agree that you have read, understood, and consent to the terms and conditions for the use of CIRA's website, as set out in the Website Terms of Use and Privacy Policy.
DNSSEC DS key registration for hacklab.ca.

ERROR: No DNS response for hacklab.ca

Please check your DNS configuration to ensure your nameservers are responding properly.

The last DNS response received was for "hacklab.ca. IN DNSKEY" and has a status of NOERROR:

```plaintext
;; Answer received from 193.110.157.69 (103 bytes)
;; HEADER SECTION
;; id = 46859
;; qr = 1  opcode = QUERY  aa = 1  tc = 0  rd = 0
;; ra = 0  ad = 0  cd = 0  rcode = NOERROR
;; qdcount = 1  ancount = 0  nscount = 1  arcount = 1

;; QUESTION SECTION (1 record)
; hacklab.ca. IN  DNSKEY

;; ANSWER SECTION (0 records)

;; AUTHORITY SECTION (1 record)
hacklab.ca. 3600 IN SOA ns0.xelerance.net. hostmaster.hacklab.ca. ( 2009071511 ; Serial
18000 ; Refresh 3600 ; Retry 864000 ; Expire 3600 ) ; Minimum TTL

;; ADDITIONAL SECTION (1 record)
; EDNS Version 0  UDP Packetsize: 4096
; EDNS-RCODE: 0 (ONLY_RDATA)
; EDNS-FLAGS: 0x8000
```

Once you have made any necessary corrections, please try again.
Verify your signed zone works with dig

[paul@thinkpad ~]$ dig +dnssec xelerance.ca. @193.110.157.136

; <<>> DiG 9.6.1-P1-RedHat-9.6.1-6.P1.fc11 <<>> +dnssec xelerance.ca. @193.110.157.136
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 23135
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
xelerance.ca. IN A

;; ANSWER SECTION:
xelerance.ca. 7200 IN A 193.110.157.130
xelerance.ca. 7200 IN RRSIG A 7 2 7200 20091019080019 20090928153731 1148 xelerance.ca. E9gTttl/A9R7XmFK5udlliiwOZTqdliziY02Gq1x0N0Qpv4aCcp3D9EX 9/pDTPrYQHb/q6AQ2VwVbw5dmUuQCrnqZRWENZQ/i+T8Scw5uKXa7w+t dz+0/tV6xbceuU1uiYCI5bNsjDAP4p09dbaq0u4Uz0uJ0yhdx/sqPkkS lFE=

xelerance.ca

cira.acei.ca
Verify if you use DNSSEC with a browser

• Try accessing http://broken.xelerance.ca/
• If you can reach it, you were not protected by DNSSEC
Troubleshooting

• Use `dig +dnssec +cd` to get the DNS answer despite the answer being bogus/invalidated by the resolver

• Test your network using:
  - `dig -t soa ca. @192.228.22.190 +norec +ignore`
  - `dig -t soa ca @192.228.22.190 +norec +ignore +bufsize=512`
  - `dig -t soa ca @192.228.22.190 +norec +ignore +bufsize=1200`
  - `dig -t soa ca @192.228.22.190 +norec +ignore +bufsize=512 +dnssec`
  - `dig -t soa ca @192.228.22.190 +norec +ignore +bufsize=1200 +dnssec`
  - `dig -t soa ca @192.228.22.190 +norec +ignore +bufsize=4096 +dnssec`
  - `dig -t soa ca @192.28.22.190 +norec +ignore +tcp +dnssec`
ExecSum & Questions

• .ca authoritative name servers for DNSSEC testbed:
  – 192.228.22.190 and 192.228.22.189

• .ca recursive name servers for DNSSEC testbed:

• .ca DNSSEC testbed key management website:
  – https://www.cira.ca/dnssec/

• .ca DNSSEC testbed contact for mailing list:
  – dnssec@cira.ca
To the DNSCurve heckler in the crowd

• No authenticity of data (secures transport only)
• Cannot pass down the security status of data
  – destroys caching hierarchy
• Has no pluggable design for crypto (DJB saith onto the people: there shall only be my 1 ECC curve)
• Takes 99% of you CPU (crypto per DNS transaction)
• IETF draft submission by OpenDNS (!)
• Data type overloading (cool hack, but still a hack)