DNS at NLnet Labs

Matthijs Mekking
Topics

• NLnet Labs
• DNS
• DNSSEC
• Recent events
NLnet

• Internet Provider until 1997
  – The first internet backbone in Holland
• Funding research and software projects that aid the Internet community
  – 1999, NLnet Labs
NLnet Labs

- Founded in 1999, DNSSEC
- DNS, DNSSEC, IPv6, routing
- Software development
  - NSD, Unbound, Idns, OpenDNSSEC
  - C
- Work on open standards (IETF)
  - RFCs 3750, 3904, 4641, 5702, ...
- Education
  - DNS courses, student projects
IETF

• Internet Engineering Task Force
• “The goal of the IETF is to make the Internet work better”
• Technical documents (RFC)
• http://www.ietf.org
Topics

• NLnet Labs
• DNS
• DNSSEC
• Recent events
What is DNS?

• Domain Name System
• We want to refer machines by name
  – devnology.nl instead of 62.212.74.133
• In the beginning there was HOSTS.TXT...
• ... but then the Internet grew
• Problems with traffic and load, name collisions
What is DNS?

• DNS was created in 1983 by Paul Mockapetris
  - RFCs 822 and 823
• IETF Full Standard in 1987
  - RFCs 1034 and 1035
• Enhanced, updated, modified
  - RFCs 1123, 1982, 2181, 2308, 2671 (EDNS0), 2672, 3425, 4343, 4592, 5001 (NSID), 5452, 5936 and more
DNS at IETF

• Internet Engineering Task Force
• "The goal of the IETF is to make the Internet work better"

Technical documents (RFC)

http://www.ietf.org
DNS Features

- A lookup mechanism for translating objects into other objects
- A globally, distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
  - Name space
  - Servers making the name space available
  - Clients who perform the name resolution
Name space
Name space

- Database of DNS Resource Records

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLASS</th>
<th>TTL</th>
<th>RDLEN</th>
<th>RDATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>devnology.nl</td>
<td>A</td>
<td>IN</td>
<td>3600</td>
<td>1</td>
<td>RDATA_A</td>
</tr>
<tr>
<td>devnology.nl</td>
<td>NS</td>
<td>IN</td>
<td>3600</td>
<td>1</td>
<td>RDATA_NS</td>
</tr>
</tbody>
</table>

- Different RDATA format

Domain name
ns1.transip.net

IPv4
62.212.74.133
Resource records

- SOA: Source of Authority
- A: IPv4 Address
- AAAA: IPv6 Address
- MX: Mail Server
- NS: Name Server (delegation)
- PTR: Reverse Lookup
- TXT: Arbitrary Text
- ...
Example zonefile

devnology.nl. IN SOA (  
ns0.transip.net. hostmaster.transip.nl.  
2010032002 14400 1800 604800 86400 )  
devnology.nl. IN NS ns0.transip.net.  
devnology.nl. IN NS ns1.transip.net.  
devnology.nl. IN NS ns2.transip.net.  
devnology.nl. IN MX 10 ASPMX.L.GOOGLE.COM.  
devnology.nl. IN MX 30 ASPMX3.GOOGLEMAIL.COM.  
...  
devnology.nl. IN TXT ( "v=spf1 ip4:62.212.74.133 a mx  
a:devnology.nl include:aspmx.googlemail.com ~all" )  
devnology.nl. IN A 62.212.74.133  
www.devnology.nl. IN CNAME devnology.nl.  

http://www.nlnetlabs.nl/  
© 2010 Stichting NLnet Labs  
Devnology, NL, 4 August 2010
Reverse zone

74.212.62.in-addr.arpa. IN SOA ( ns1.leaseweb.nl. postmaster.leaseweb.nl. 2002111068 14400 7200 604800 86400 )
74.212.62.in-addr.arpa. IN NS ns2.leaseweb.nl.
74.212.62.in-addr.arpa. IN NS ns3.leaseweb.org.
74.212.62.in-addr.arpa. IN NS ns1.leaseweb.nl.

1.74.212.62.in-addr.arpa. IN PTR hosted-by.leaseweb.com.
2.74.212.62.in-addr.arpa. IN PTR tiltbox.com.
...
133.74.212.62.in-addr.arpa. IN PTR devnology.nl.
...
Name resolution
Name resolution

;; QUESTION SECTION:
;www.devnology.nl. IN A

;; AUTHORITY SECTION:
nl. 172800 IN NS ns1.nic.nl.
nl. 172800 IN NS ns-nl.nic.fr.

;; ADDITIONAL SECTION:
ns1.nic.nl. 172800 IN A 193.176.144.2
ns-nl.nic.fr. 172800 IN A 192.93.0.4
ns1.nic.nl. 172800 IN AAAA 2a00:d78:0:102:193:176:144:2
Name resolution

;; QUESTION SECTION:
;www.devnology.nl. IN A

;; AUTHORITY SECTION:
devnology.nl. 7200 IN NS ns0.transip.net.
devnology.nl. 7200 IN NS ns1.transip.net.
devnology.nl. 7200 IN NS ns2.transip.net.

;; ADDITIONAL SECTION:

• Additional section is empty, need to query for ns{0,1,2}.transip.net
Name resolution

;; QUESTION SECTION:
www.devnology.nl.  IN  A

;; ANSWER SECTION:
www.devnology.nl.  86400 IN  CNAME  devnology.nl.
devnology.nl.    86400 IN  A   62.212.74.133
Reverse zone

; <<< DiG 9.7.0-P1 <<< -x 62.212.74.133
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id:23068
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
;; ADDITIONAL: 0

;; QUESTION SECTION:
;133.74.212.62.in-addr.arpa.  IN  PTR

;; AUTHORITY SECTION:
74.212.62.in-addr.arpa. 77364 IN  SOA
ns1.leaseweb.nl. postmaster.leaseweb.nl. 2002111068 14400
7200 604800 86400

http://www.nlnetlabs.nl/
© 2010 Stichting NLnet Labs
## DNS on the wire

<table>
<thead>
<tr>
<th>QR</th>
<th>Opcode</th>
<th>AA</th>
<th>TC</th>
<th>RD</th>
<th>RA</th>
<th>Z</th>
<th>RCODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QDCOUNT</th>
<th>ANCOUNT</th>
<th>NSCOUNT</th>
<th>ARCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Authoritative NS

• Makes the name space available
  - Zone files vs Database backends
  - Master vs. Slaves
  - Zone transfers
    • Incremental zone transfers – RFC 1995
    • DNS NOTIFY – RFC 1996
    • TSIG and SIG(0) – RFC 2845 and 2931
  - Dynamic updates (DHCP) – RFC 2136
Topics

• NLnet Labs
• DNS
• DNSSEC
• Recent events
What's the threat?

- DNS Threat Analysis (RFC 3833)
  - Packet interception
    - Confidentiality, Integrity, Availability
  - ID Guessing & Query prediction
    - devnology.nl IN A 6.6.6.6
  - Name chaining
    - devnology.nl IN NS ns0.evilguy.com
  - Denial of service (flooding name servers)
    - Slave servers
What's the threat?

• Confidentiality?
  - DNS is public data
  - IPSec

• Availability?
  - As with any network service
  - DNSSEC does not prevent Denial of Service (in fact it makes it worse)

• Integrity
  - DNSSEC will ensure integrity
Cache poisoning

• Provide false data to a caching name server (query prediction, id guessing)
• Based on a flaw in the DNS, first answer is the correct one, ignore duplicates
Cache poisoning

• How does a resolver know a response is expected?
  – Arrives on the same UDP port
  – Question section matches
  – Query ID matches
  – The Authority and Additional sections represent names that are within the same domain as the question: this is known as "bailiwick checking".
Kaminsky attack

- Based on ID guessing (16 bits)
- Prerequisite is that the data is not in the cache
- High TTL is sort of defense mechanism (but not against the Kaminsky attack)
Real response

;; QUESTION SECTION:
;111.nlnetlabs.nl. IN NS

;; AUTHORITY SECTION:
nlnetlabs.nl. 3600 IN SOA
open.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2010080100
28800 7200 604800 3600
Real response

;;; QUESTION SECTION:
;www.nlnetlabs.nl.  IN A

;;; ANSWER SECTION:
www.nlnetlabs.nl. 9888 IN A 213.154.224.1

;;; AUTHORITY SECTION:
nlnetlabs.nl. 10117 IN NS open.nlnetlabs.nl.
nlnetlabs.nl. 10117 IN NS ns3.domain-registry.nl.

;;; ADDITIONAL SECTION:
open.nlnetlabs.nl. 528 IN A 213.154.224.1
open.nlnetlabs.nl. 9162 IN AAAA 2001:7b8:206:1::53
Fake response

;; QUESTION SECTION:
;111.nlnetlabs.nl. IN A

;; ANSWER SECTION:
111.nlnetlabs.nl. 9888 IN A 6.6.6.1

;; AUTHORITY SECTION:
nlnetlabs.nl. 10117 IN NS ns1.evilguy.com.
nlnetlabs.nl. 10117 IN NS ns2.transip.net.

;; ADDITIONAL SECTION:
open.nlnetlabs.nl. 528 IN A 213.154.224.1
open.nlnetlabs.nl. 9162 IN AAAA 2001:7b8:206:1::53

http://www.nlnetlabs.nl/
© 2010 Stichting NLnet Labs
Kaminsky attack

1.foo.nl?

foo.nl SOA

- Invalid ID
- Duplicate

1.foo.nl!
6.6.6.1

1.foo.nl!
NXDOMAIN

http://www.nlnetlabs.nl/
© 2010 Stichting NLnet Labs
Kaminsky attack

9.foo.nl?

foo.nl SOA
9.foo.nl A 6.6.6.1
foo.nl NS ns.evil

9.foo.nl!
6.6.6.1

9.foo.nl!
NXDOMAIN
- Duplicate

Devnology, NL, 4 August 2010

http://www.nlnetlabs.nl/
© 2010 Stichting NLnet Labs
Kaminsky attack

• Solution 1: add more randomness
  - UDP source port randomization
  - \(2^{16} \times 2^{11} = 2^{27} = 134\) million
  - Short term solution

• Solution 2: DNSSEC
DNSSEC

- DNS Security Extensions
  - RFC 4034, 4035
- Data origin authentication, data integrity
- Public key cryptography
  - The DNSKEY Record
- Adds signatures to responses
  - The RRSIG Record
## DNSSEC RRs

### DNSSEC Resource Records

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLASS</th>
<th>TTL</th>
<th>RDLEN</th>
<th>RDATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>devnology.nl</td>
<td>DNSKEY</td>
<td>IN</td>
<td>3600</td>
<td>1</td>
<td>RDATA_DNSKEY</td>
</tr>
<tr>
<td>devnology.nl</td>
<td>RRSIG</td>
<td>IN</td>
<td>3600</td>
<td>1</td>
<td>RDATA_RRSIG</td>
</tr>
</tbody>
</table>

### ORIG TYPE

<table>
<thead>
<tr>
<th>ORIG TYPE</th>
<th>ALGO.</th>
<th>LABELS</th>
<th>ORIG TTL</th>
<th>SIG EXPIRE</th>
<th>SIG START</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA</td>
<td>RSASHA1</td>
<td>2</td>
<td>3600</td>
<td>01/09/2010</td>
<td>01/08/2010</td>
</tr>
</tbody>
</table>

### KEY TAG

- **KEY TAG**: 12345
- **SIGNER NAME**: devnology.nl
- **SIGNATURE**: AwEE3dF0...

### FLAGS

- **FLAGS**: 257
- **PROTOCOL**: 3
- **ALGORITHM**: RSASHA1
- **PUBLIC KEY**: AQPSKmy...
DNSSEC RRs

- DNSKEY: Public key
- RRSIG: Signature
- DS: Delegation Signer
  - Provides a secure path at the delegation (between parent zone and child zone)
- NSEC: Denial of Existence
  - broodjeaap.nl is proven not to exist
- NSEC3: Hashed Denial of Existence
DNSSEC RRs

devnology.nl. IN RRSIG SOA 5 2 3600 (20100831131949 20100803131949 46792 devnology.nl. RYY.../yik= )

... devnology.nl. IN DNSKEY 257 3 5 AwE...htWV
devnology.nl. IN RRSIG DNSKEY 5 2 3600 ...
devnology.nl. IN NSEC www.devnology.nl. A NS SOA MX TXT (RRSIG NSEC DNSKEY )
devnology.nl. IN RRSIG NSEC 5 2 86400 ...
www.devnology.nl. IN CNAME devnology.nl.
www.devnology.nl. IN RRSIG CNAME 5 3 360 ...
www.devnology.nl. IN NSEC devnology.nl. CNAME RRSIG NSEC
www.devnology.nl. IN RRSIG NSEC 5 3 86400 ...

http://www.nlnetlabs.nl/
© 2010 Stichting NLnet Labs

development, NL, 4 August 2010
DNSSEC query

;; ANSWER SECTION:
devnology.nl. 3600 IN A 62.212.74.133
devnology.nl. 3600 IN RRSIG A 5 2 3600 20100831131949 20100803131949 46792 devnology.nl. TO+EysNigcB/rXBZ89mv310KZnX3/2xp6Cl0r96cUg10qNXU11RCoHQteeW705AFtqV0e8WK7QMVFSpu0TRTnXNwcEDIP/qvzBu7bMSjCM7XejDg1ff+WgfJ5Ra4C1Dvryq4Rj03kKzQPSBiE9DiK03zcQgUCEVEdJ03YrY+NbY= ;{id = 46792}

;; AUTHORITY SECTION:
devnology.nl. 3600 IN NS ns0.transip.net.
devnology.nl. 3600 IN NS ns1.transip.net.
devnology.nl. 3600 IN RRSIG NS 5 2 3600 20100831131949 20100803131949 46792 devnology.nl. LTqB1PmqOC3YaBYedq6sHM3tssVwtAx8M106I2y0NynCcY2oRyRK4Mti19eJ/0H98J0en0j6u9KQtzEUGXb0Ik+MLIBntNwxF1CTBEyvmJp9U+9E6Rt0tv1Np1cH3Lsf+UXaXajPxkeFJpuE/Q6YQsNwP2zqtGkQl/I09XPWvU= ;{id = 46792}
DNSSEC Status

• A response can now be
  - Secure
  - Insecure
  - Bogus
  - Indeterminate

• Up to local policy how to handle these states
How to validate?

- Resolver needs to know the public key
  - Trust Anchor
- Key distribution is difficult
- Solution: Sign the delegation
  - The DS Record
  - DNS Root Trust Anchor: “one key to rule them all”
- Luckily, the root has been signed:)
  - As of 15 July 2010
DNS Root Trust Anchor

. IN DNSKEY 257 3 8
AwEAAagAIK1VZrpC6Ia7gEzahOR+9W29euxhJhV
VLOyQbSEW008gcCjFFVQUTf6v58fLjwBd0YI0Ez
rAcQqBGCzh/RStIo08g0NfnfL2MTJRkxoXbfDaU
eVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkJ
f5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1a
pAzvN9dlzEheX7ICJBBtuA6G3LQpzW5h0A2hzCT
MjJPJ8LbqF6dsV6DoBQzgu10sGIcGOY170yQdXf
Z57relSQageu+ipAdTTJ25AsRTAoub80NGcLmqr
AmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihzθ=
{id = 19036 (ksk), size = 2048b}
DNSSEC RRs

• In the root zone:
  - dk. IN DS 26887 8 2 A1AB8546B80E438A7DFE0EC559A7088EC5AED3C4E0D26B1B60ED3735F853DFD7
  - dk. IN RRSIG DS 8 1 172800 20100810000000 20100802230000 41248 . o23Xc...

• Points to the DNSKEY in the dk zone:
  - dk. IN DNSKEY 256 3 8 AwEAA... ; keytag=55594
  - dk. IN DNSKEY 257 3 8 AwEAA... ; keytag=26887
  - dk. IN RRSIG DNSKEY 8 1 86400 20100805191323 20100729141045 26887 dk. WLuD3...

• Resolver can now build chain of trust
Name resolution

;dnssec.dk. IN A @k.root-servers.net

;; AUTHORITY SECTION:
dk. 172800 IN NS a.nic.dk.
dk. 172800 IN NS b.nic.dk.
...
dk. 172800 IN DS 26887 8 2 A1AB8546B80E438A7DFE0EC559A7088EC5AED3C4E0D26B1B60ED3735 F853DFD7
dk. 172800 IN RRSIG DS 8 1 172800 20100810000000 20100802230000 41248 . o23Xc... ; signed with root key
;; ADDITIONAL SECTION:
a.nic.dk. 172800 IN A 212.88.78.122
b.nic.dk. 172800 IN A 193.163.102.222
Name resolution

; dnssec.dk. IN A @a.nic.dk

;; AUTHORITY SECTION:
dnssec.dk. IN NS ns1.gratisdns.dk.
dnssec.dk. IN NS ns2.gratisdns.dk.

8afgsvl5sgurhqbipm0fdbvr5jq1frp2.dk. 3600 IN NSEC3 1 1 17
FAC981985022A210 8AFHAQVUPD0DDIRUTFL1NE5QONPO1CJ5 A NS
SOA TXT RRSIG DNSKEY NSEC3PARAM

8afgsvl5sgurhqbipm0fdbvr5jq1frp2.dk. 3600 IN RRSIG NSEC3

isab28efbcpglup6uanh61dnolc8g0tq.dk. 3600 IN NSEC3 1 1 17
FAC981985022A210 ISAH6L4MDDHR8KHCHFHC6SG7N6TG708

isab28efbcpglup6uanh61dnolc8g0tq.dk. 3600 IN RRSIG NSEC3

;; ADDITIONAL SECTION:
ns1.gratisdns.dk. 86400 IN A 109.238.48.13

http://www.nlnetlabs.nl/
Name resolution

; dnssec.dk. IN A @ns1.gratisdns.dk

; ; ANSWER SECTION:
dnssec.dk. 43200 IN A 193.3.157.13

dnssec.dk. 43200 IN RRSIG A 5 2 43200 20100901114809

; ; AUTHORITY SECTION:
dnssec.dk. 43200 IN NS ns4.gratisdns.dk.
dnssec.dk. 43200 IN NS ns3.gratisdns.dk.
dnssec.dk. 43200 IN NS ns5.gratisdns.dk.
dnssec.dk. 43200 IN NS ns2.gratisdns.dk.
dnssec.dk. 43200 IN NS ns1.gratisdns.dk.
dnssec.dk. 43200 IN RRSIG NS 5 2 43200
Name resolution

;; Number of trusted keys: 1
;; Domain:.
[T] . 86400 IN DNSKEY 256 3 8 ;{id = 41248 (zsk), ...}
 . 86400 IN DNSKEY 257 3 8 ;{id = 19036 (ksk), ...}
[T] dk. 172800 IN DS 26887 8 2 a1ab8546b80e438a7dfe0ec559a7088ec5aed3c4e0d26b1b60ed3735f853dfd7
 ;; Domain: dk.
[T] dk. 86400 IN DNSKEY 257 3 8 ;{id = 26887 (ksk), ...}
dk. 86400 IN DNSKEY 256 3 8 ;{id = 55594 (zsk), ...}
 ;; Domain: dnssec.dk.
[S] dnssec.dk. 43200 IN DNSKEY 257 3 5 ;{id = 58693...}
dnssec.dk. 43200 IN DNSKEY 256 3 5 ;{id = 26751...}
[S] dnssec.dk. 43200 IN A 193.3.157.13
Denial of existence

;miss.nlnetlabs.nl. IN A @open.nlnetlabs.nl

;; AUTHORITY SECTION
nlnetlabs.nl. 3473 IN SOA open.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2010080100 28800 7200 604800 3600
nlnetlabs.nl. 3473 IN RRSIG SOA 5 2 10200 20100829005003
nlnetlabs.nl. 1543 IN NSEC _jabber._tcp.nlnetlabs.nl. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY
nlnetlabs.nl. 1543 IN RRSIG NSEC 5 2 3600 20100829005003
mirre.nlnetlabs.nl. 3596 IN NSEC moby-dick.nlnetlabs.nl. A AAAA RRSIG NSEC
mirre.nlnetlabs.nl. 3596 IN RRSIG NSEC 5 3 3600
NSEC Issues

• More signatures needed
• Zone walking
• Solution: Hashed version of Denial of Existence
  – The NSEC3 Record – RFC 5155
Hashed version

• Simplified

;miss.nlnetlabs.nl. IN A @open.nlnetlabs.nl

h(www.nlnetlabs.nl.) = 11
h(miss.nlnetlabs.nl.) = 12
h(_jabber._tcp.nlnetlabs.nl.) = 13

11.nlnetlabs.nl. 1543 IN NSEC3 13.nlnetlabs.nl. A AAAA
Hashed version

; dnssec.dk. IN DS @a.nic.dk

;; AUTHORITY SECTION:
...
8afgsvl5sgurhqbiɒpm0fdбрv5jq1frp2.dk. 3600 IN NSEC3 1 1 17 FAC981985022A210 8AFHAQVUPD0DDIRUTFL1NE5Q0NPO1CJ5 A NS SOA TXT RRSIG DNSKEY NSEC3PARAM
8afgsvl5sgurhqbiɒpm0fdбрv5jq1frp2.dk. 3600 IN RRSIG NSEC3
isab28efbcp(glup6uanh61dnolc8g0tq.dk. 3600 IN NSEC3 1 1 17 FAC981985022A210 ISAH6L4MDDHLR8KHCHFHC6SG7N6TG708
isab28efbcp(glup6uanh61dnolc8g0tq.dk. 3600 IN RRSIG NSEC3
Operational practices

• RFC 4641
• Re-signing
  – Signatures have a lifetime to prevent replay attacks
  – Signature validity period should be long enough to last the weekend
• Key rollover
  – Crypto analysis
  – Operational practices
Key rollover

• Be aware of DNS caches!
  – Old DNSKEY might still be in the cache
  – Old RRSIGs might still be in the cache
  – Switching without care might take your zone offline

• Be aware of your delegation!
  – DS Record in the parent must match your DNSKEY
  – ZSK / KSK split (Flags: 256 / 257)
ZSK vs KSK

| 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 ? | Protocol | Algorithm |

• SEP (Security Entry Point) bit
  - 0: 'ZSK'
  - 1: 'KSK' (Only sign DNSKEY set)

– DS record must match a SEP
Key rollover

• Double sign your zone
  - Until old key expires from the cache
  - Remove old key
  - Drawback: Increased zone size

• Pre-publish your new key
  - Introduce new key, unused
  - Retire old key, use new key
  - Remove old key
  - Drawback: Increased rollover duration
DNSSEC weaknesses

- Increased DNS response packet size
- Increased workload for the resolvers
- Hierarchical trust level
- Time synchronization
- Complex to implement and operate
  - OpenDNSSEC
The whole picture
Topics

• NLnet Labs
• DNS
• DNSSEC
• Recent events
Recent events

• The root is signed!
  - DS in the root:
    .bg, .br, .cat, .cz, .dk, .edu, .lk, .na, .org, .tm, .uk
  - Coming: .arpa, .fr, .nl, .se, ...

• http://www.youtube.com/watch?v=b9j-sfP9GUU
Recent events

• Trust anchor distribution is a pain
• Automatic updating of Trust Anchors (at the resolver)
  - RFC 5011
  - Regular polling of SEP keys
  - Introduces the REVOKED bit
  - Not meant for those who have a secure delegation
  - Autotrust: RFC 5011 implementation
Recent events

• Algorithm Rollover
  - RFC 5702 introduces RSASHA2
  - DNSSEC says that all RRsets need to be signed with each algorithm
  - DNSKEY may expire from the cache before its signatures do
Recent events

• Algorithm Rollover and Automatic Updating of Trust Anchors
  – We need to double sign (because of use of multiple algorithms)
  – We need to revoke
? • http://www.nl.netlabs.nl
• http://www.opendnssec.org
• http://blog.nominet.org.uk/tech/2010/05/24/436
• http://www.root-dnssec.org/