DNSSEC for ISPs workshop

João Damas
(joao@isc.org)

Outline of workshop

- Brief intro to DNSSEC (30’)
- Overview of zone signing (30’)
- DNSSEC validation (60’)
  - trust anchors
  - validation
  - impact of enabling validation
  - debugging
- Making DNSSEC useful for you (30’)

Brief Introduction to DNSSEC

The protocol bits

- What is DNSSEC meant to do?
- What does it do?
- How does it do it?

What is DNSSEC meant to do?

- It protects data **in transit** between an authoritative name server and a client
- **Optionally**, it can securely **link** the zones in the DNS tree

- It does not:
  - ensure data is correct, only that no one has interfered with it

What is DNSSEC meant to do?

- This **should** enable a new world of applications/services
  - –see DANE, SSHFP, new anti-spam tools

What does DNSSEC do?

- It defines a protocol to allow verification of DNS data by a client who knows the public key used to sign the DNS data.

How does DNSSEC secure DNS?

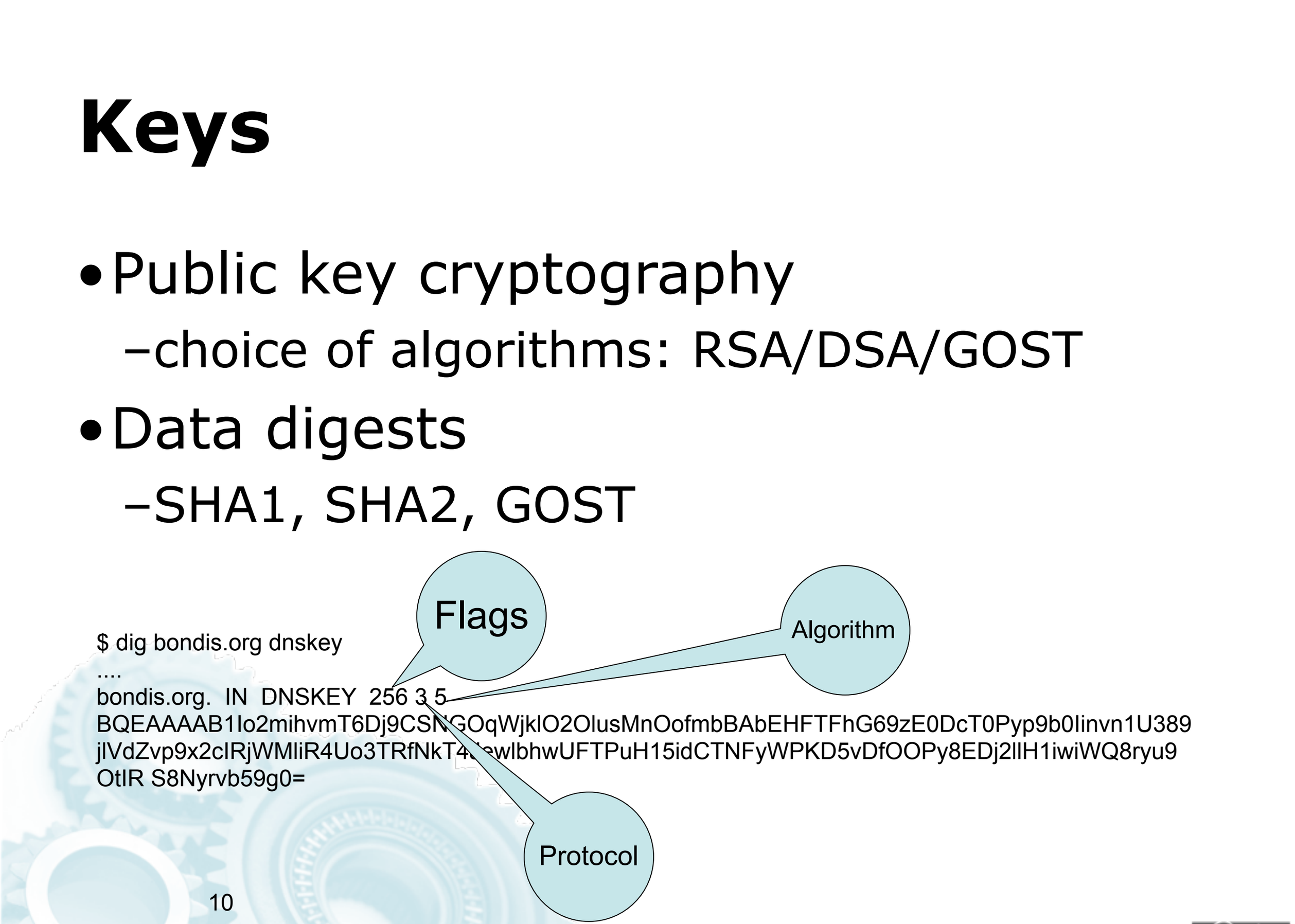
- Technical elements
- Data signing

Technical elements

- Keys
- Proof of nonexistence
- Zone links
- Signatures

Keys

- Public key cryptography
  - choice of algorithms: RSA/DSA/GOST
- Data digests
  - SHA1, SHA2, GOST



Keys

- Key Signing Key
- Zone Signing Key

- Only difference is how they are used, otherwise they are identical (1bit)

Proof of nonexistence

- Critical to avoid false negatives (e.g. interception)
- Pre-computed (DoS mitigation)
  - probably modern hardware could compute the elements in real time.
- Two ways. Both valid
  - NSEC
  - NSEC3

NSEC

NSEC

- Describe intervals between two consecutive names that existent in the zone
  - Allows “zone walking”
  - Some TLDs see this as a privacy problem
    - the problem tends to be in the whois, not in the DNS

```
-$ dig patio.bondis.org +dnssec

;; QUESTION SECTION:
;patio.bondis.org.              IN      A

;; AUTHORITY SECTION:
ns.bondis.org.          300     IN      NSEC    smtp1.bondis.org. A RRSIG NSEC
ns.bondis.org.          300     IN      RRSIG   NSEC 5 3 7200 20101215090000
20100913110215 40583 bondis.org. nYwLzU....
```

NSEC

Zone Walking

$ dig patio.bondis.org +dnssec
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN

;; QUESTION SECTION:
;patio.bondis.org. IN A

previou

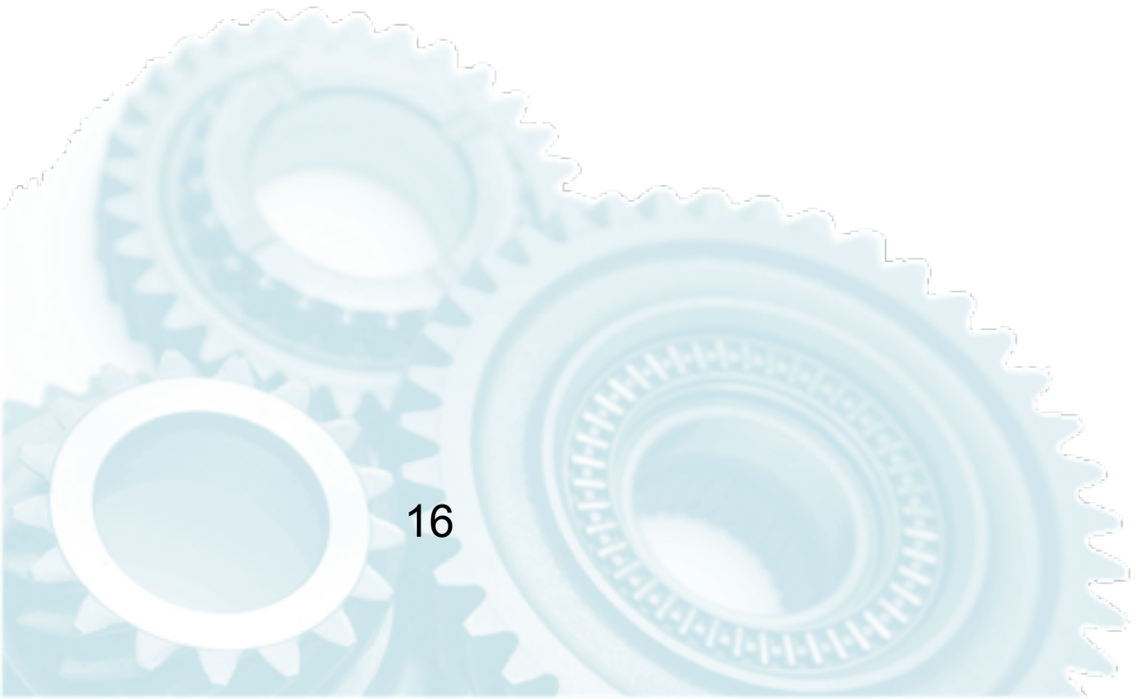
nex

;; AUTHORITY SECTION:
ns.bondis.org. 300 IN NSEC smtp1.bondis.org. A RRSIG NSEC
ns.bondis.org. 300 IN RRSIG NSEC 5 3 7200 20101215090000
20100913110215 40583 bondis.org. nYwLzUsk5Q.....

NSEC3

- Replaces the names in NSEC records with hashes of existing names
  - hard for humans to debug
- Introduces an unrelated but useful feature: opt-out

NSEC3



Linking zones

- In DNS search jumps from zone to zone via delegations

```
$ dig @a0.org.afilias-nst.info. isc.org
;; QUESTION SECTION:
;isc.org.                       IN      A
;; AUTHORITY SECTION:
isc.org.                86400   IN      NS      ams.sns-pb.isc.org.
isc.org.                86400   IN      NS      ord.sns-pb.isc.org.
isc.org.                86400   IN      NS      ns.isc.afilias-nst.info.
isc.org.                86400   IN      NS      sfba.sns-pb.isc.org.
```

Linking zones

DNSSEC creates a parallel tree.

Keys are represented in parent zones with a new record

DS (delegation signer)

```
 $ dig @a0.org.afilias-nst.info. bondis.org any
;; ANSWER SECTION:
bondis.org.          32     IN     NS     ns.bondis.org.
bondis.org.          32     IN     NS     borg.c-l-i.net.
bondis.org.          84416  IN     DS     46041 5 2
77B5E5C737CBA4D8610EF16D6161CDFF7C48F8C6A63157A900510ABC 1C52BE66
bondis.org.          84416  IN     DS     46041 5 1 4E64E49EAC3B9C6124925CDE6DE9A11A4BA9C061
```

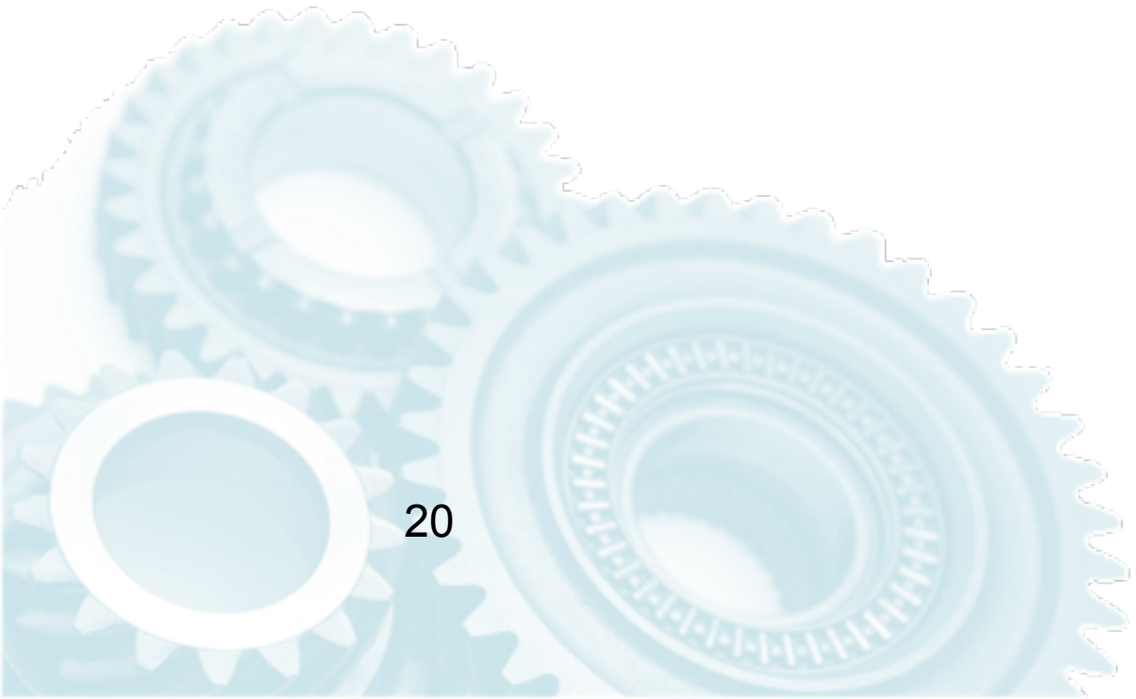
Signing the Data

- Signatures are what you can actually check to verify data is real
- Stored in the RRSIG record
  - one per name and record type

```
$ dig isc.org any +dnssec
;; QUESTION SECTION:
;isc.org.                       IN      ANY
;; ANSWER SECTION:
isc.org.            7071    IN  RRSIG   DNSKEY 5 2 7200 20110829230209 20110730230209 12892 isc.org. J7d/2l/cPUHzyg3ze....
isc.org.            7071    IN  RRSIG   DNSKEY 5 2 7200 20110829230209 20110730230209 21693 isc.org. WO2LHgs1bkK2d04FCkCG01O4Z....
isc.org.            7071    IN  DNSKEY  257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr hhCeFvAZih7yJ....
isc.org.            7071    IN  DNSKEY  256 3 5 BEAAAAO6L6BadeFzvt6J63GDGrFANfJAitCd9Njcj49y6PE1Bv6t33sE yxSVi4KWbjQgV....
isc.org.            7070    IN  RRSIG   NS 5 2 7200 20110829233225 20110730233225 21693 isc.org. QD/j5eKOVyYW+iOUTDGzo....
isc.org.            7070    IN  NS      sfba.sns-pb.isc.org.
isc.org.            7070    IN  NS      ns.isc.afilias-nst.info.
isc.org.            7070    IN  NS      ams.sns-pb.isc.org.
isc.org.            7070    IN  NS      ord.sns-pb.isc.org.
isc.org.            34420   IN  RRSIG   DS 7 2 86400 20110830154907 20110809144907 11028 org. WA/UeCd+Pi6eNmPFWAXQ5O7k....
isc.org.            34420   IN  DS      12892 5 1 982113D08B4C6A1D9F6AEE1E2237AEF69F3F9759
isc.org.            34420   IN  DS      12892 5 2 F1E184C0E1D615D20EB3C223ACED3B03C773DD952D5F0EB5C777586D E18DA6B5
```

```
WO2LHgs1bkK2d04FCkCG01O4ZakCNcw2DDWFsYHfTuaQcyy4aM8yYOAl
Bll5J7tn+oml3rkF+3ieGo3F8zAObUFCMc2cNHo3Ct6+vRCIxpDiDsCh
avJOBLnyH8M3t3blR2xarHz+rFY/lEq9mHdoNUm3qBL4uV0OZJ8ViExs xTM=
```

Overview of zone signing



DNSSEC Validation

Getting the necessary elements

- The server software
  - BIND, Unbound, PowerDNS recursor
    - we will use BIND here
- The Key material
  - https://data.iana.org/root-anchors/
  - http://www.root-dnssec.org/documentation/

Getting the necessary elements

- Tools
  - DiG (with the special sauce)
  - drill
  - wireshark
  - dnscap (https://www.dns-oarc.net/tools/dnscap)
  - aaaa

Getting our hands dirty

- First make sure DiG is ready
  - compile BIND using

    STD_CDEFINES='-DDIG_SIGCHASE=1 ./configure
  - not the cleanest code ever but it solves the problem nicely

Get the keys for the root zone

- https://data.iana.org/root-anchors/

Kjqmt7v.crt	30-Jun-2011 19:53
Kjqmt7v.csr	15-Jul-2010 19:13
draft-icann-dnssec-trust-anchor.html	15-Jul-2010 20:44
draft-icann-dnssec-trust-anchor.txt	15-Jul-2010 20:44
icann.pgp	15-Jul-2011 19:48
icannbundle.p12	15-Jul-2010 19:13
icannbundle.pem	15-Jul-2010 19:13
root-anchors.asc	15-Jul-2010 19:13
root-anchors.p7s	30-Jun-2011 19:53
root-anchors.xml	15-Jul-2010 19:13

Multiple choices. For me the more convenient is the combination of the PGP signature with the xml file...

xml has DS record. BIND needs DNSKEY

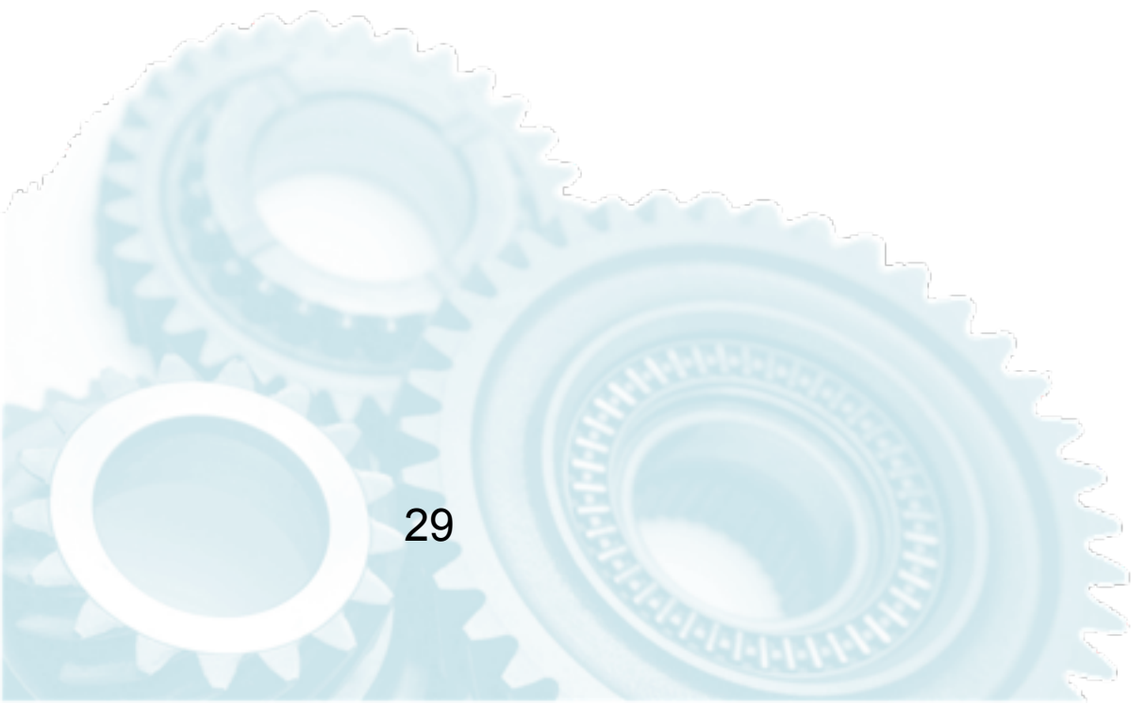
Get the keys for the root zone

- To verify, get the DNSKEY from the DNS itself
  - dig @f.root-servers.net . DNSKEY +noall +answer +multi >/tmp/root-key
- and convert to ds using a BIND utility
  - dnssec-dsfromkey -f /tmp/root-key .
- Compare the DS with the one in root-anchors.xml

Configure BIND to validate

- Introduce the validate key into named.conf
  - Manual management
    - trusted-keys
  - Automatic management
    - managed-keys

Making DNSSEC useful for you



You can use it now, to your own advantage

- Problem to be solved:

  a new server comes online or you change the SSH host key (e.g. OS change/upgrade)

  You need to manually refresh the key at all clients

or

you can use SSHFP

Using SSHFP with your SSH system

- This is something that benefits you in your daily work
- You need to:
  - generate SSHFP records and put them in the zone (one time per key)
  - Sign the zone with DNSSEC
  - configure SSH clients (one time)

Get data into the zone

- Generate SSHFP records
  - –by hand
  - –using tools, such as
    - http://www.xelerance.com/services/software/sshfp/
- Add to the corresponding server name

shuttle.c-l-i.net. IN SSHFP 2 1 575897C6164E07B920CE92416049AB33DFAF30E6

- Sign the zone

Configure the SSH client

- Add option

  VerifyHostKeyDNS yes ***(or ask)***

  to .ssh/config

- Enable EDNS0 in /etc/resolv.conf
  - options edns0
  - or use and env var in $SHELL
    - RES_OPTIONS=edns0

Voilá

- If DNSSEC validation is working OpenSSH will use the keys automatically

- https://www.dnssec-tools.org/wiki/index.php/DNSSEC-Tools_Components