DNSSEC for ISPs workshop

João Damas
(joao@isc.org)

Outline of workshop

- Brief intro to DNSSEC
- Overview of zone signing
- DNSSEC validation
  - trust anchors
  - validation
  - impact of enabling validation
  - debugging
- Making DNSSEC useful for you

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
    - DANE: http://tools.ietf.org/wg/dane/charters

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

```
$ dig bondis.org dnskey
....
bondis.org.  IN  DNSKEY  256 3 5
BQEAAAAB1Io2mihvmT6Dj9CSNGOqWjkIO2OlusMnOofmbBAbEHFTFhG69zE0DcT0Pyp9b0Iinvn1U389
jIVdZvp9x2cIRjWMIiR4Uo3TRfNkT4JewlbhwUFTPuH15idCTNFyWPKD5vDfOOPy8EDj2lIH1iwiWQ8ryu9
OtIR S8Nyrvb59g0=
```

Keys

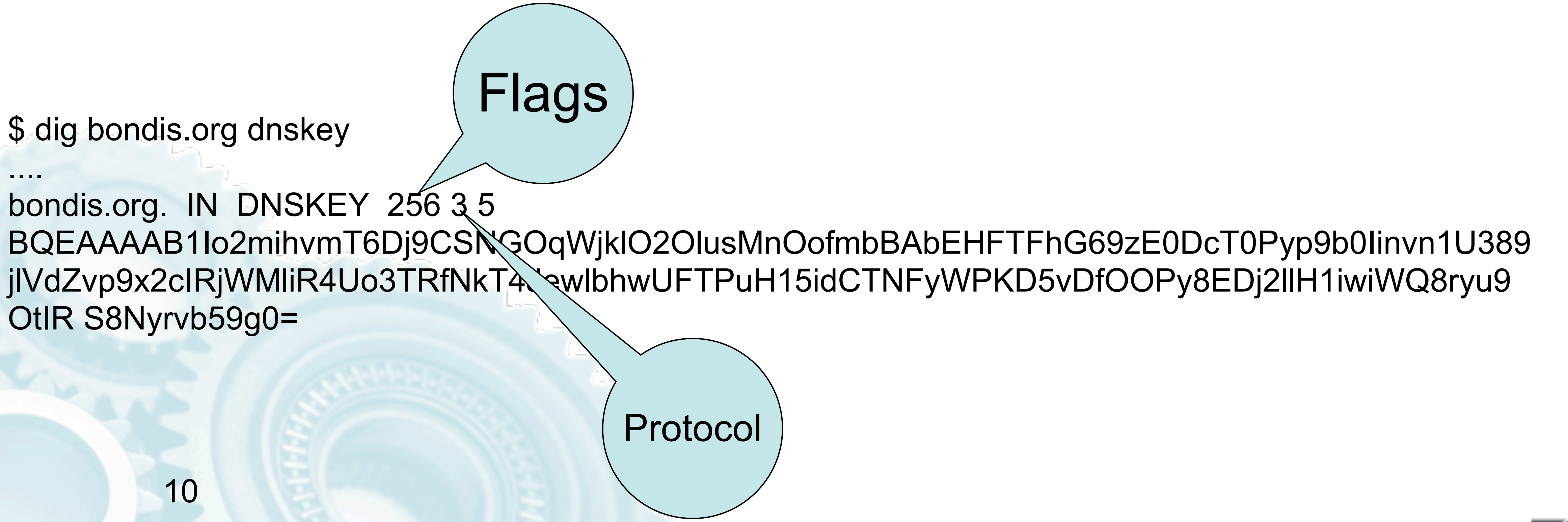
- Public key cryptography
  - –choice of algorithms: RSA/DSA/GOST
- Data digests
  - –SHA1, SHA2, GOST

Flags

```
$ dig bondis.org dnskey
....
bondis.org.  IN  DNSKEY  256 3 5
BQEAAAAB1Io2mihvmT6Dj9CSNGOqWjkIO2OlusMnOofmbBAbEHFTFhG69zE0DcT0Pyp9b0Iinvn1U389
jIVdZvp9x2cIRjWMIiR4Uo3TRfNkT4JewlbhwUFTPuH15idCTNFyWPKD5vDfOOPy8EDj2lIH1iwiWQ8ryu9
OtIR S8Nyrvb59g0=
```

Keys

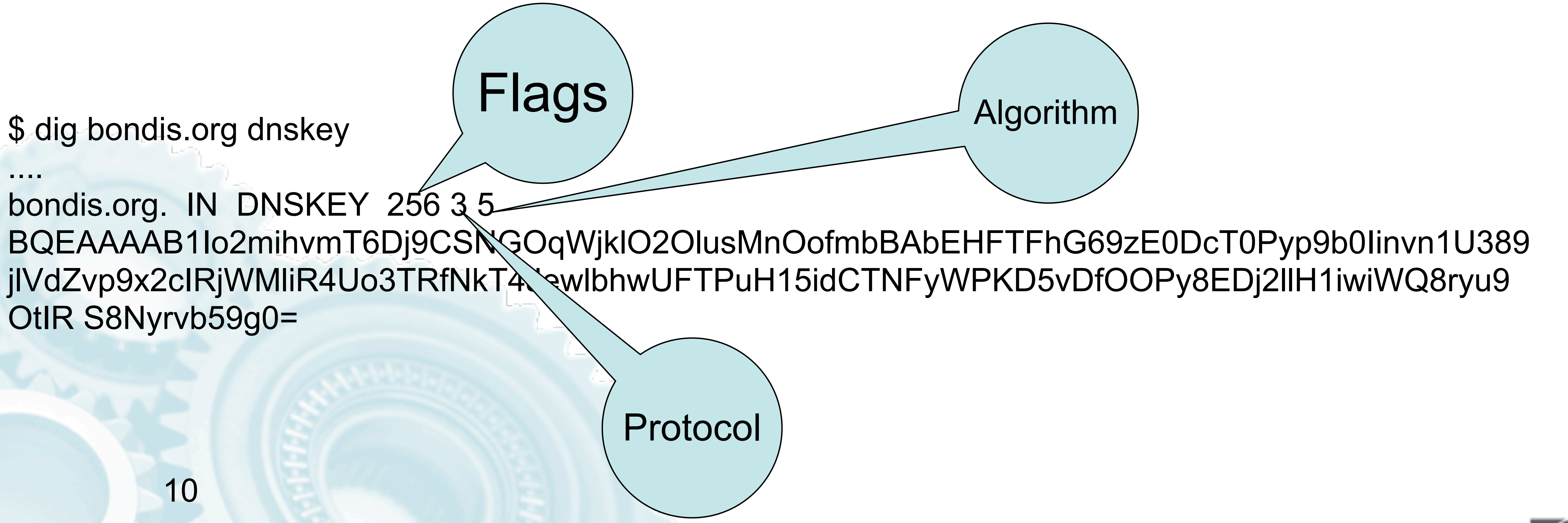
- Public key cryptography
  - choice of algorithms: RSA/DSA/GOST
- Data digests
  - SHA1, SHA2, GOST



```
$ dig bondis.org dnskey
....
bondis.org.  IN  DNSKEY  256 3 5
BQEAAAAB1Io2mihvmT6Dj9CSNGOqWjkIO2OlusMnOofmbBAbEHFTFhG69zE0DcT0Pyp9b0Iinvn1U389
jIVdZvp9x2cIRjWMIiR4Uo3TRfNkT4dewIbhwUFTPuH15idCTNFyWPKD5vDfOOPy8EDj2lIH1iwiWQ8ryu9
OtIR S8Nyrvb59g0=
```

Keys

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



```
$ dig bondis.org dnskey
....
bondis.org.  IN  DNSKEY  256 3 5
BQEAAAAB1Io2mihvmT6Dj9CSNGOqWjklO2OlusMnOofmbBAbEHFTFhG69zE0DcT0Pyp9b0Iinvn1U389
jlVdZvp9x2cIRjWMliR4Uo3TRfNkT4dewlbhwUFTPuH15idCTNFyWPKD5vDfOOPy8EDj2llH1iwiWQ8ryu9
OtIR S8Nyrvb59g0=
```

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 problemtends to be in the whois, not in the DNS

X

NSEC

```
-$ 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

NSEC

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

;; 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. nYwLzUsk5Q.....
```

NSEC

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

;; QUESTION SECTION:
;patio.bondis                   IN      A

;; AUTHOR             ION:
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.....
```

previous

NSEC

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

;; QUESTION SECTION:
;patio.bondis                    IN      A

;; AUTHOR              ION:
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.....
```

previous

next

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

```
$  dig isc0.org +dnssec +noall +answer +authority

; <<>> DiG 9.6.1-P1 <<>> isc0.org +dnssec +noall +answer +authority
;; global options: +cmd
org.                    872     IN      SOA     a0.org.afilias-nst.info. noc.afilias-nst.info. 2009765707 1800 900 604800 86400
org.                    872     IN      RRSIG   SOA 7 1 900 20110929095701 20110908085701 56472 org.
DaeMBz24QcHdzTQrjE7SdzJ42SKgNBK2sFSZaWNRzwskT2QghgbUcywf
2GxSFf6cChEsFe4hULXzWWDHqMcipiIlAjT78UMfZ8o5XHFXw458M7FT bb+41u0OX75WtoCXXHa8+zrXGn9csa7QuE29c/
JQhg/Ynv9ylAnww36U fJc=
h9p7u7tr2u91d0v0ljs9l1gidnp90u3h.org. 872 IN RRSIG NSEC3 7 2 86400 20110929095701 20110908085701 56472 org.
GmtpVsYkxJ1yRmt8vWsuHmbWBJCJhuGaRvoKccdDX8B/gO1Q+cUw8jG2 lH24MV4J4vipBvqvbI72g/
1DNFdOPW2Vqn3aIctA+8co9wImHr/5tNHY HcCwF79x/wm38nFbhxxI7XDWPfvTMy+YbjCeSddxIPdegggBRHPZOLj5
QQA=
h9p7u7tr2u91d0v0ljs9l1gidnp90u3h.org. 872 IN NSEC3 1 1 1 D399EAAB H9R9S3ARGOL56DI1SIA1K4AORTQ8FGPN NS
SOA RRSIG DNSKEY NSEC3PARAM
tc8i66k7jila0sgib7tjeic8vftrevko.org. 872 IN RRSIG NSEC3 7 2 86400 20110926183026 20110905173026 56472 org.
E3DwrbG9RdbfaQcu0nDyylhYAP44Ezo48qwUO95wXVQPkgkdJnTgPz5P
aecBljmbG4RIY7sa4SMwy6WPo3cpVPd7tcVOy5uJfqkEQJhOP8eYfaGf BpvlrBMPTo3KefFoEjQ0RscN0ZWIR+/
rwlpZdA4R9yP7u+YU0AxOq6eb /bU=
tc8i66k7jila0sgib7tjeic8vftrevko.org. 872 IN NSEC3 1 1 1 D399EAAB TCEKMSLUSATMEGL10541FLRRD7CNAL2J A
RRSIG
vaiuqvth0uj0nkst7dkbscpig5lcg2op.org. 872 IN RRSIG NSEC3 7 2 86400 20110922155643 20110901145643 56472 org.
eyXNpLjjD/B3c9/V1Dfhyf5jJu1cwHc40V+zvVHYgKsNCsndZLXYiV/1 T33Lc5ka6cdCK/FHWy0/
qn7idRvViyOrNDPQ0f8AKmme/Gl1ZvTuHzOZ 3fP0JkQgC2EmHF4m/sPOMPBVPUYwU3fnzh4XtBZJFcnrXSHv7Mg9E9P6
NQo=
vaiuqvth0uj0nkst7dkbscpig5lcg2op.org. 872 IN NSEC3 1 1 1 D399EAAB VARKIF352C7E5J1AGLO6DJ68T9H5N4R1 A
RRSIG
```

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

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
```

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/2I/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
```

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
```

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
```

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
```

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/2I/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
```

Overview of zone signing

Create key(s)

- standard utilities come with BIND and others
- dnsssec-keygen
- Most common case people create 2 types of keys
  - DNS itself doesn’t care about these key types, purely administrative
  - KSK/SEP, ZSK

Sign zone

- Use cli tools that ship with BIND and others
  - dnssec-signzone
- Use automated processes
  - BIND 9.7+
  - zkt
  - opendnssec

Serve the signed zone

- Make sure all NS are DNSSEC enabled
- Don’t forget signatures have an expiry date

More details

- See online resources
  - https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources

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)

Getting our hands dirty

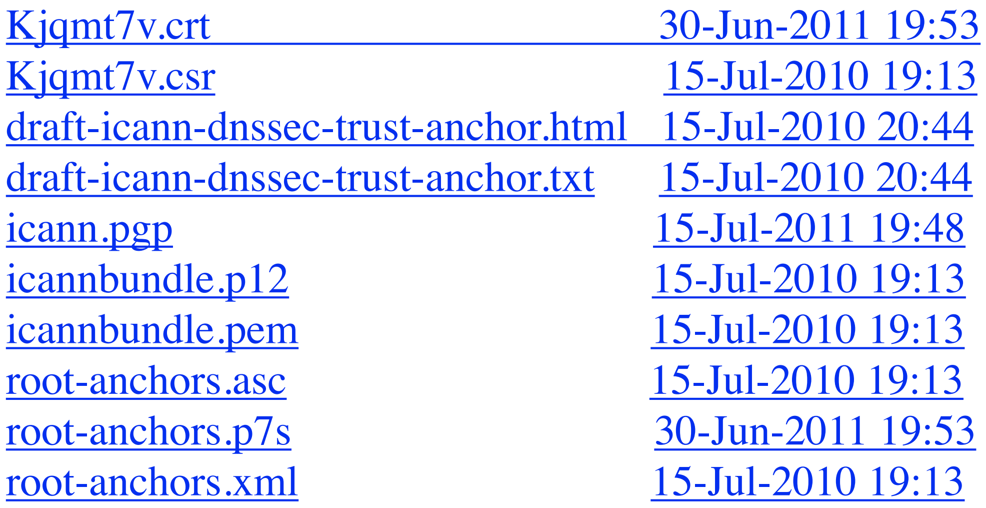
- First make sure DiG is ready
  - compile BIND using

    ```
    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 most convenient is the combination of the PGP signature with the xml file...

even if 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
      - –RFC5011
- Make sure DNSSEC is enabled

DLV

- Useful under some circumstances
  - –frequent use of islands of security
  - –testing
- What is it?
  - –early deployment aid
- how does it work?

Enabling DLV

- enable it with
  - dnssec-lookaside auto
- You can register your own DNSSEC keys with ISC's DLV registry
  - https://dlv.isc.org/

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

When things break

- Things don’t break...