

Troubleshooting DNSSEC Visually

ESCC/Internet2 Joint Techs

July 14, 2010

Casey Deccio

Sandia National Laboratories



Outline

- **Motivation**
- **Visualizing DNSSEC**
- **Future Work**



Outline

- **Motivation**
- Visualizing DNSSEC
- Future Work



DNS Query and Response

casey@rome:~\$ dig www.sandia.gov

```
; <<>> DiG 9.6.1-P3 <<>> www.sandia.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25307
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 2
```

```
;; QUESTION SECTION:
www.sandia.gov.      IN      A
```

```
;; ANSWER SECTION:
```

```
www.sandia.gov.      3593   IN      CNAME   sahp1305.sandia.gov.
sahp1305.sandia.gov. 3593   IN      A        132.175.81.4
```

```
;; AUTHORITY SECTION:
```

```
sandia.gov.          3593   IN      NS       NS1.CA.sandia.gov.
sandia.gov.          3593   IN      NS       NS9.sandia.gov.
sandia.gov.          3593   IN      NS       NS2.CA.sandia.gov.
sandia.gov.          3593   IN      NS       NS8.sandia.gov.
```

```
;; ADDITIONAL SECTION:
```

```
NS8.sandia.gov.      3593   IN      A        198.102.153.28
NS9.sandia.gov.      3593   IN      A        198.102.153.29
```

```
;; Query time: 4 msec
;; SERVER: 127.0.0.1#5353(127.0.0.1)
;; WHEN: Mon Apr 26 12:04:46 2010
;; MSG SIZE rcvd: 178
```

DNSSEC Query and Response

```
casey@rome:~$ dig +dnssec www.sandia.gov
```

```
; <<>> DiG 9.6.1-P3 <<>> +dnssec www.sandia.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10600
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.sandia.gov.                IN      A

;; ANSWER SECTION:
www.sandia.gov. 3252 IN CNAME sahp1305.sandia.gov.
www.sandia.gov. 3252 IN RRSIG CNAME 7 3 3600 20100518100446 20100418100446 64298 sandia.gov.
aBCBrkcGw4ejj+HFrXuR/oxygP30Vurs20Aej/F1Bu4ahHsvYNuWVJ94
21hKS8Ylu/xbX2UJRrLq390d8OT2vQF9wkVI8IVMViLGdxp1fVTzES+6
XtMHvEMxavuGv9fkHk3Kyt5RNrWwJ1ZquhdsTfzJwTpS9f6u7K5B24Au
MOHRI5FscQhy85dfMMCOYn7Xa0mqam8mgy1k88xy8zSFQ/hTitMgN6HM
bd2P/nLYnxMXXnjbllqPe9nzUPFjK4jbQVJsEAkPhOJ+k66cFBN/GlyJ
B3i5wjbHgXSS3XmkBlrTGjpTVRgnj7ARgMNOEV4pj6WHUHkM3k2TF/SK oiRY7g==
sahp1305.sandia.gov. 3252 IN A 132.175.81.4
sahp1305.sandia.gov. 3252 IN RRSIG A 7 3 3600 20100518100446 20100418100446 64298 sandia.gov.
nk85TnprSqAPrQyJ8kUE0KM/9MVBCJd0j5XlvJTpn0OdmCnQEC/pyPI7
2HyXGJ1MituQLLP7yDGRubrbFwljkX9DCRvrK1xSGmj+CH2zrFrs30cu
tE+w24IuaK3RDL6nVVPZ0pcpjUSBpHja0G4VMiPHbkafyOsl7q101Jd
Ot8Z5FAaEWxCc0rtkKKA3NlmQ64S2RdEYCV1PRO1fvumiCzLE/oJ/vNN
nthmmw8F14zV73jxnYuEZaKLCz5DI3LKyHhBXff0q2Z62WR637knH52o
8Gow1gvlQztFDrzAfbYlNd+UGxlGh0/vaxnROp5JVC1WKK3MjOnNhZbk E5pO6Q==
7yYXSg==
```



What happens if something goes wrong?

```
casey@rome:~$ dig +dnssec www.medicare.gov
```

```
; <<>> DiG 9.6.1-P3 <<>> +dnssec www.medicare.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 40029
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.medicare.gov.      IN      A

;; Query time: 1085 msec
;; SERVER: 127.0.0.1#5353(127.0.0.1)
;; WHEN: Mon Apr 26 13:56:14 2010
;; MSG SIZE  rcvd: 45
```

Manual Troubleshooting (dig)

casey@rome:~\$ dig +dnssec @ns1cms.rdcms.eds.net. **www.medicare.gov**

;; ANSWER SECTION:

www.medicare.gov. 900 IN A 146.123.140.204

www.medicare.gov. 900 IN RRSIG A 5 3 900 20100430184424 20100426183811 39045 medicare.gov.

T1/xOmA+nNEpIcS73wF3iB7+fr/gqhk8HXVL6cnX90jUhN3LWub5snwp OWoIC6eBxbjha1+492SQ4VDQYA8wwmlIF9MFRLrrboo25KUsbJfk0The
440l9heY2Wxm74HXBsJclQEbKvNumx6fRPzmad4jK3RjzLzp4barn282 mmA=

casey@rome:~\$ dig +dnssec +multi @ns1cms.rdcms.eds.net. **medicare.gov** dnskey

;; ANSWER SECTION:

medicare.gov. 1296000 IN DNSKEY 256 3 5 AwEAAcpyc4bhl2jawsXT

GeW8YqUtBudvA0phC/miCBKajTeCXaToPaylzziVlcbVf/1F0vay7KJx LDUGIt
Bo81wMO5

medicare.gov. 1296000 IN DNSKEY 257 3 5 AwEAAchzoM8KoxpaUT

k0gVyODy1YySFmnZW8Nin/PG82BA+t+s1wptKfgBX8ssc68UfitvfnNxO NK2t0C

ULFVKd7GGBInXIGD3LrtgfaGkUBV2XjG9XH2leSxxVvk29ovNdrLYjWs UFP

82hGflrlxkmKiLjeop10gR0pJW2qVMEG9QZQW0nHEbWEeNO1NA7omtX_0b3ZZq6Jfc0=

medicare.gov. 1296000 IN RRSIG DNSKEY 5 2 1296000 20100430202133 20100426194625 35677 medicare.gov.

xU/Y+q7sWM+sjcn9upiz7vUUJZ03YxX+M2Ji89QqMjZSe2eHXbnMQAZh axlpIwHWftrTpTWzCJWO/dFuk7mNkcegC/4l9XoGeTkCL/lnLaseep2j

3RJPSmFXFLOPGvY2v2Vnik45qJweNmZYse083ouOurAUpxCwPJVUzRa/ plmtt6RdzKM4hT3oc4qTEZMaKDku/qEICPaQPz0g2G1Z8Lr86vz+LCp

V3tw4TT5P92wdRTXzvUG+ZonfyYhD4jNgfKhm6hVreHJmon6hPW04lK N1HJIZSbV7KDV5GJo5CHFnxYLRmJtf8YxV4NXqSmOSy8EDgOao1lYbK

cO+9PA==

medicare.gov. 1296000 IN RRSIG DNSKEY 5 2 1296000 20100430202133 20100426194625 39045 medicare.gov.

LRmOwpQoqE5ScCDHHkILhPoxBJaMeV0BYMx8M7lXw96F9oI9ub6MWz+u MZkXmyfkld5UKidKQGU1tqLjglZhOwztRBgYXfTpL7WHP9N0Lcflcs+a

n8pYzDuP0QeucRAHndE7rar3ECt6RCjYJSwELP+96oaBZHqUigael6Zx 4gs=

casey@rome:~\$ dig +dnssec @a.usadotgov.net **medicare.gov** ds

;; ANSWER SECTION:

medicare.gov. 86400 IN DS 26508 7 1 6B998973DAA4C783A7A24B6FC19251FB0CC8064D

medicare.gov. 86400 IN DS 26508 7 2 48704FE4FFF98AD71863FC64751C9B3A0D2B2A73622A84DB19E3A08E CDC912F1

medicare.gov. 86400 IN RRSIG DS 7 2 86400 20100430191703 20100425191703 51998 gov.

Jz14rLZ7r2IaOJHLxDqmIBRvYCH5IPUVh+4kKZit9Rv7wn9oLkcgTXQA rp46Sa0L2FzrEC6fuEDZ6siXKKUfteQ8TaLbnikPuD00yAmYyDUPv

YLwPU0XIG4J5axlylFRu1mJ7843ej/fmmnEfQoq55jz3Oc+hW18KTFB XpA=

By signature analysis:

- ZSK id = 39045

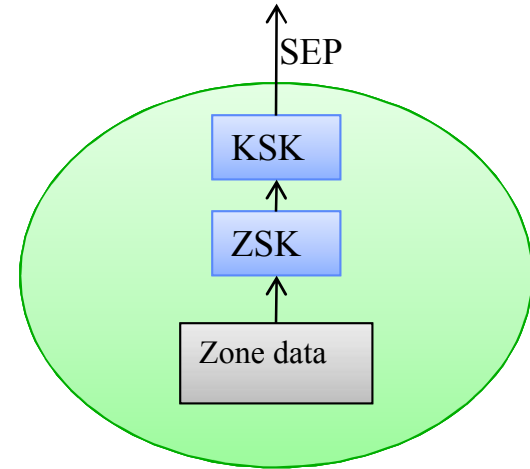
- KSK id = 35677

- DS key tag = 26508

=> DS references DNSKEY 26508 which does not exist

DNSKEY Roles

- **DNSKEY roles:**
 - **ZSK (zone signing key)**
 - signs zone data
 - **KSK (key signing key)**
 - signs only DNSKEY RRset
 - **SEP (secure entry point)**
 - Typically associated with KSK
 - Resolver must ignore SEP flag
 - **Revoked**
 - Revoke bit set and self-signed
- **DNSKEY roles don't necessarily follow attributes**





More Automated Methods

- **Other techniques**
 - dig +sigchase
 - drill -S
- **Methods are textual, more catered toward advanced users**



Outline

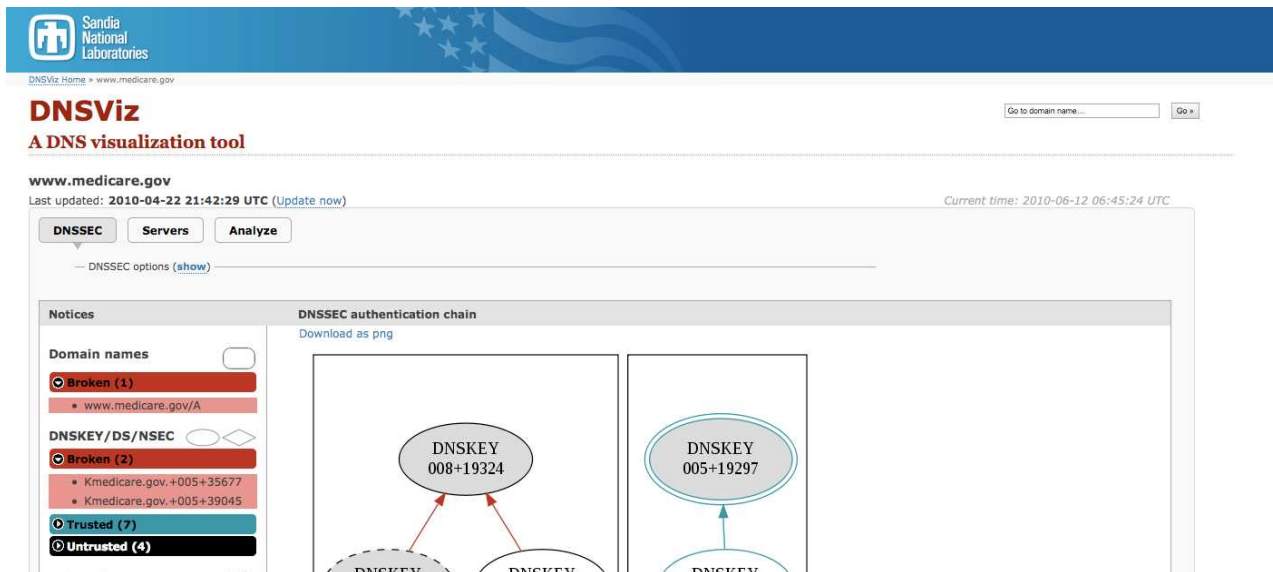
- Motivation
- **Visualizing DNSSEC**
- Future Work

DNSSEC Visualization

“A picture is worth one thousand DNS queries.”

- Loosely adapted from a quote attributed to Chinese proverb

<http://dnsviz.net/>

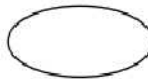


Visualization Components

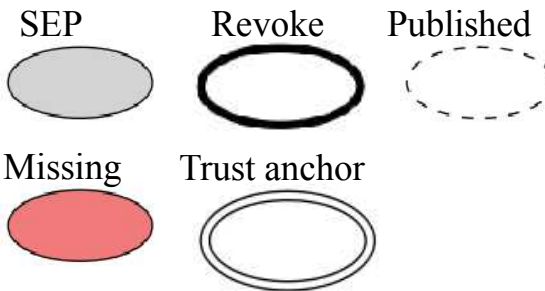
Domain name



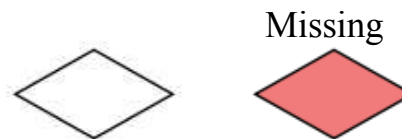
DNSKEY/DS RR



DNSKEY attributes

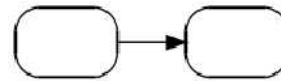


NSEC proving non-existence of
DS RRs (insecure delegation)

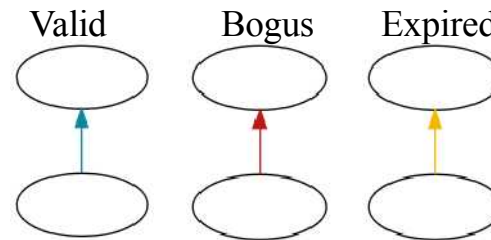


Visualization Components

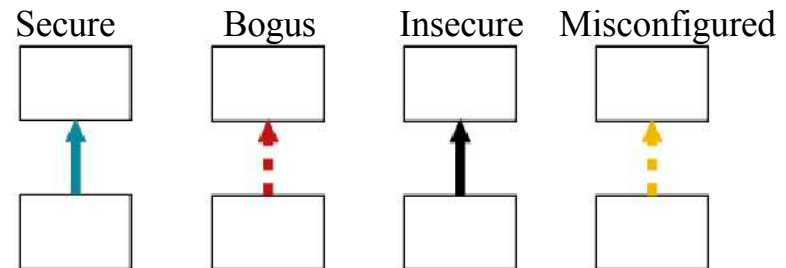
Alias dependency



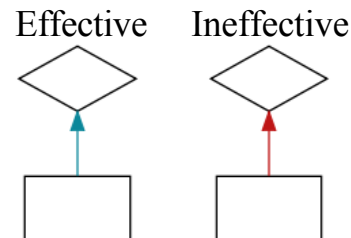
Signature or digest



Delegation



Proof of insecure delegation

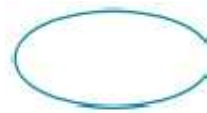




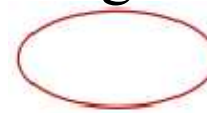
The Bottom Line

- Is there a valid chain of trust from a trust anchor to a node?
- Has the existence of DS RRs been effectively repudiated for insecure delegations?

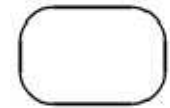
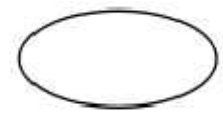
Secure



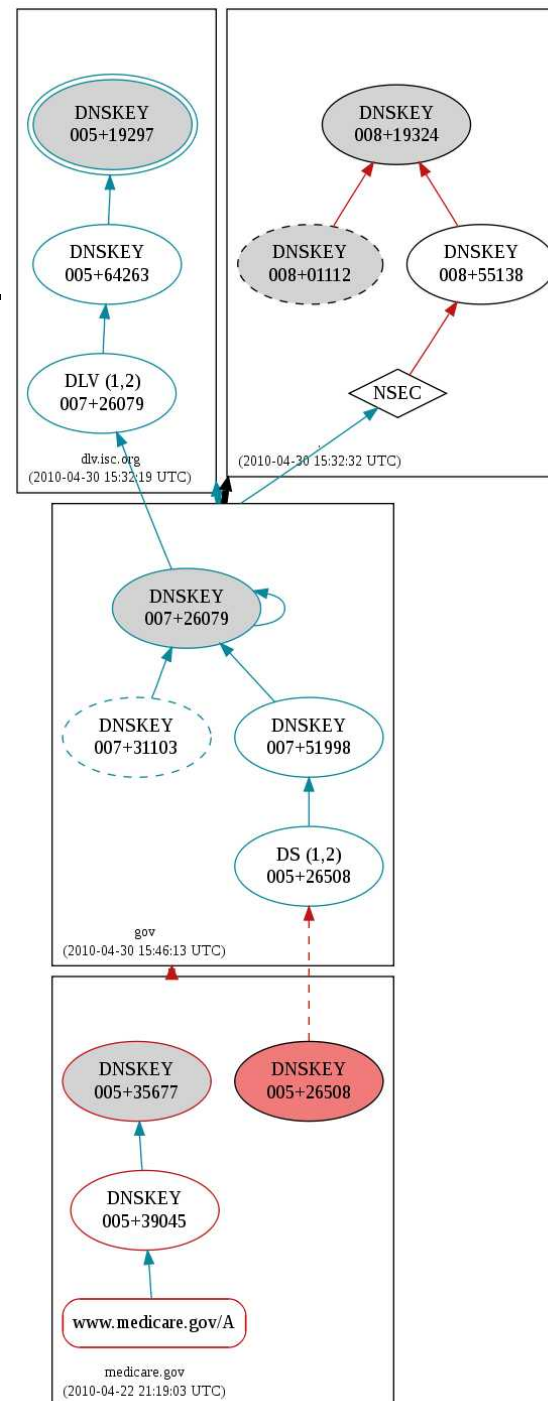
Bogus

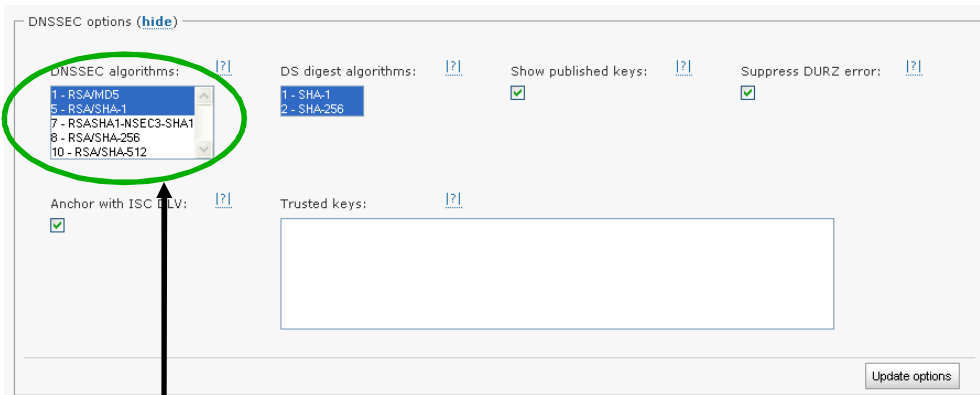


Insecure



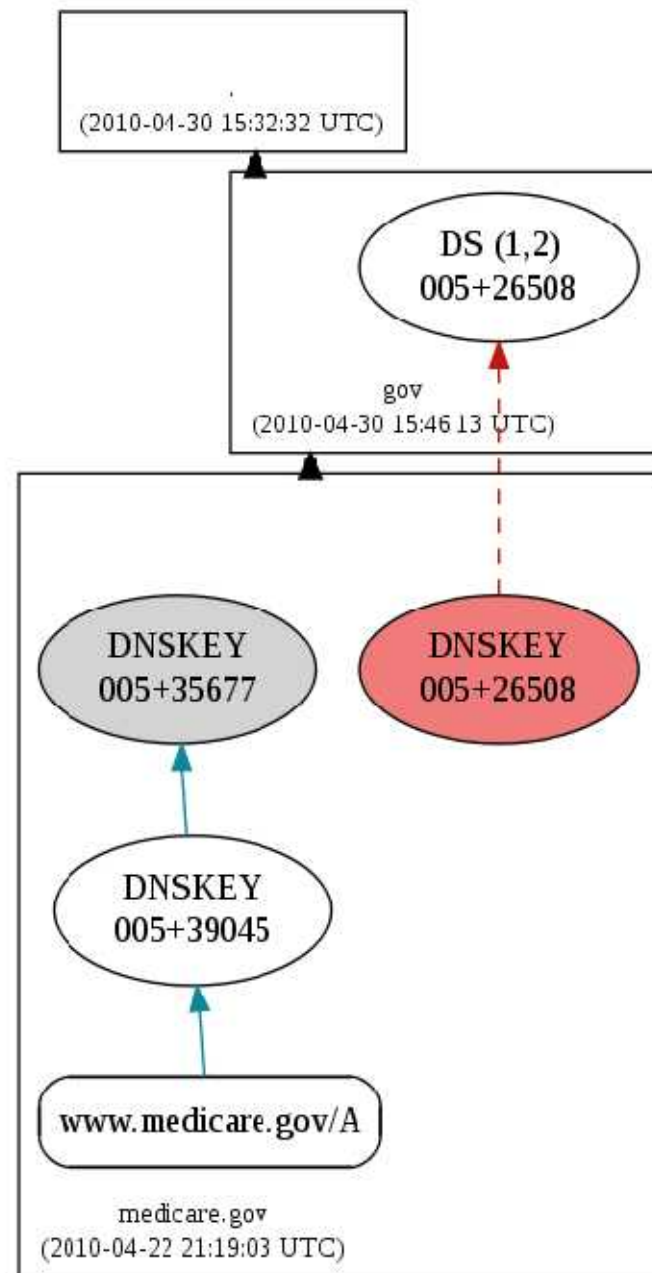
Revisiting medicare.gov:
DS RRs exist, but don't
match any DNSKEY RR

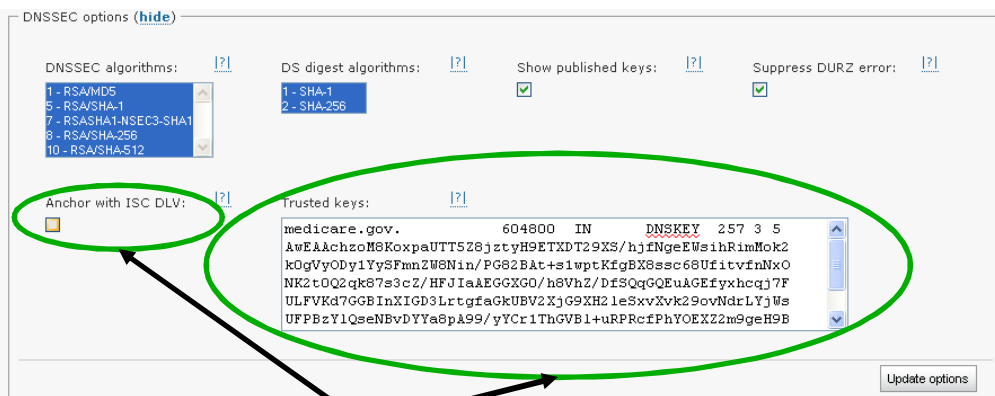




Selective DNSSEC algorithm support (e.g., BIND < 9.6)

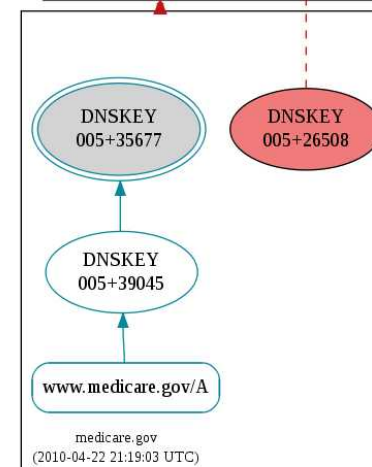
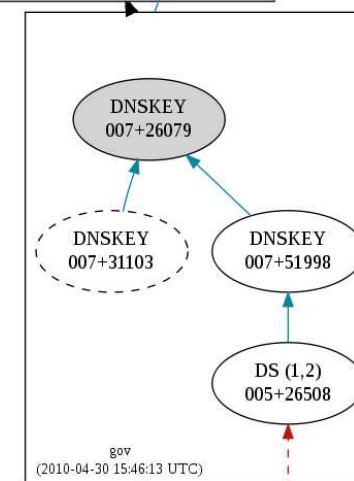
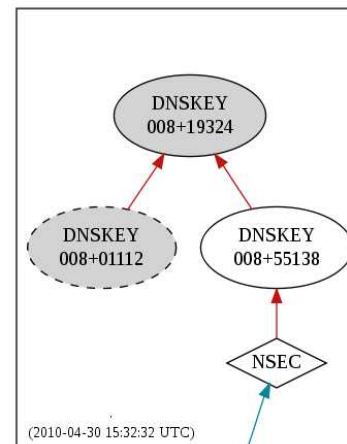
www.medicare.gov/A now “insecure” instead of “bogus”

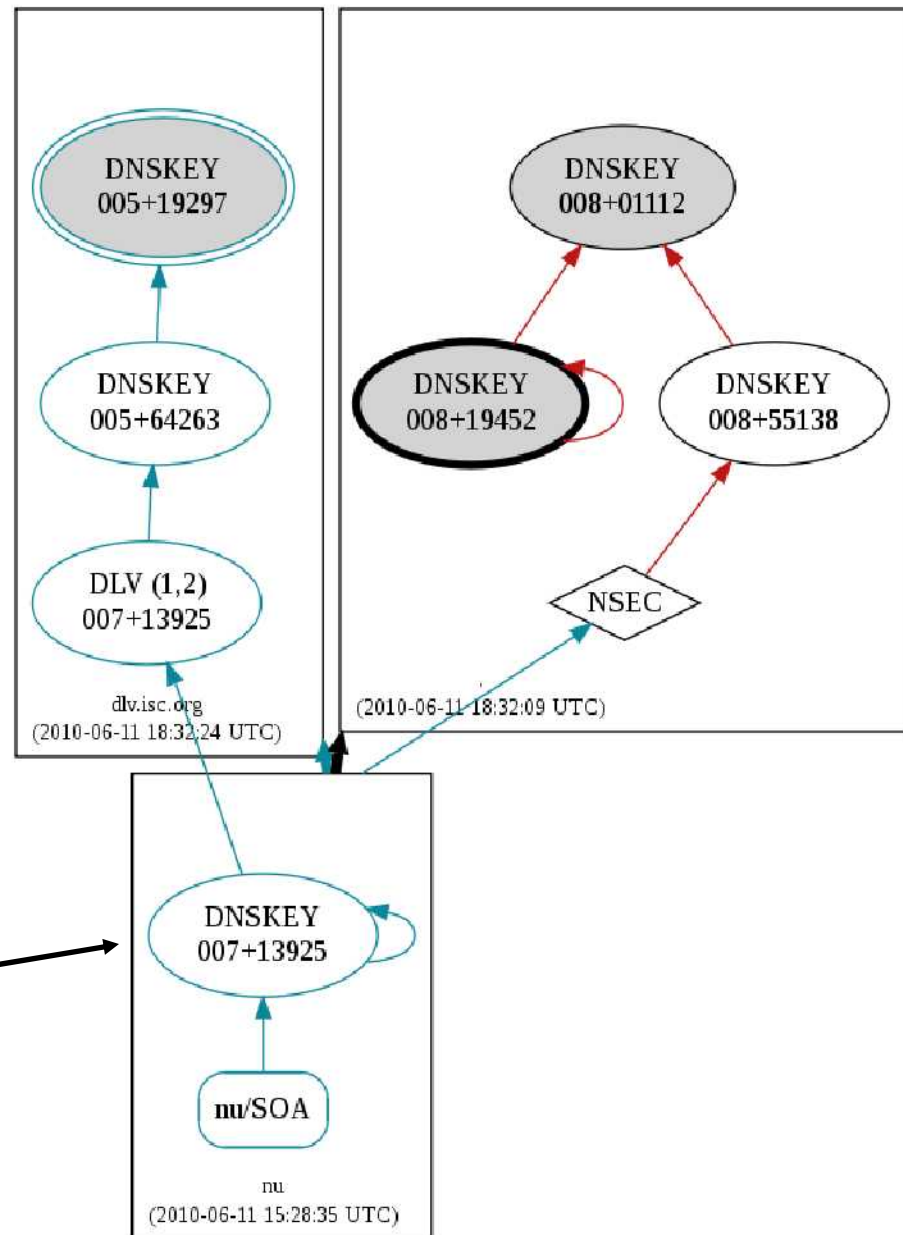




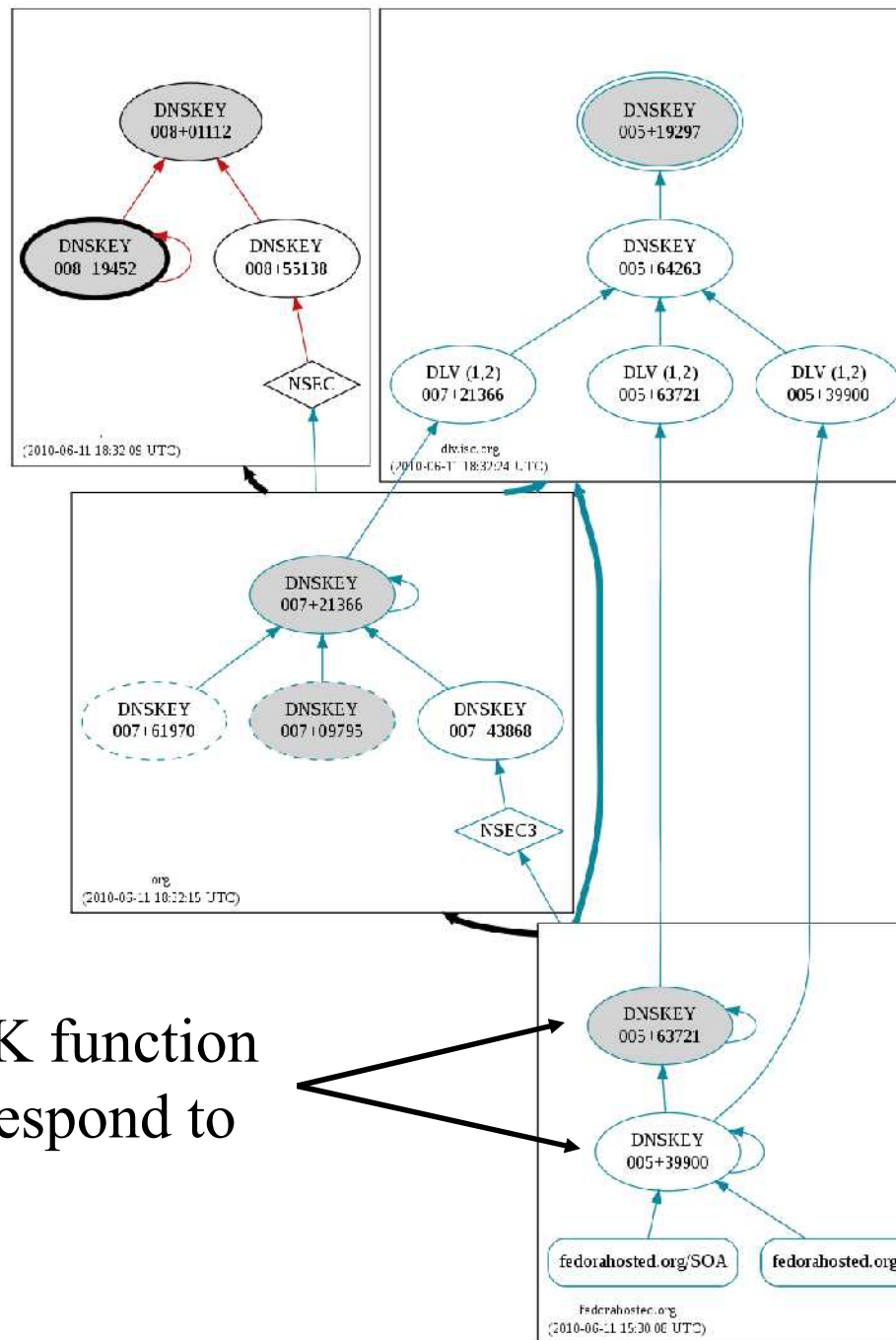
Configurable trust anchors
and ISC DLV support

www.medicare.gov/A now “secure”
instead of “bogus”



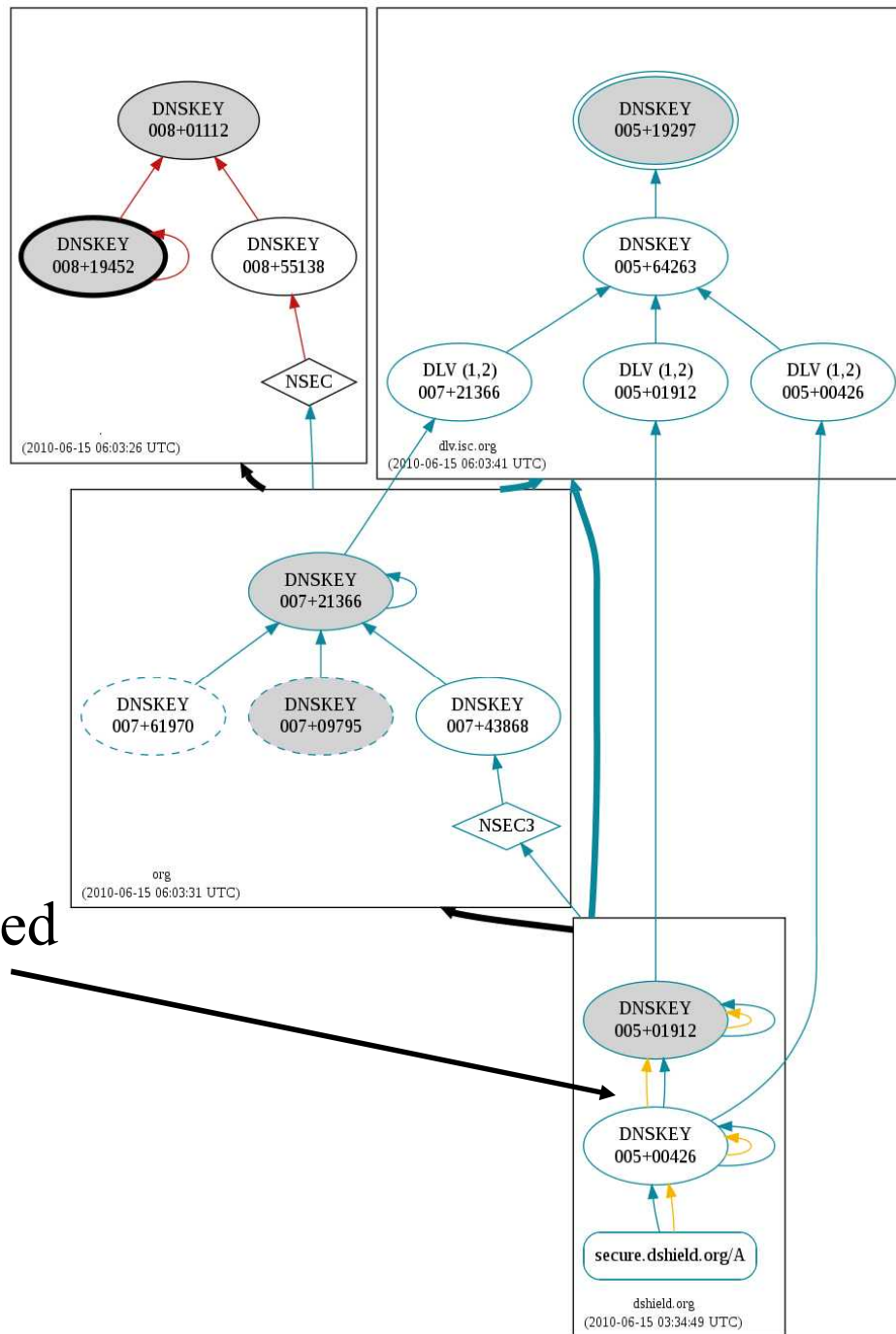


Single DNSKEY,
functioning as
ZSK, KSK, and SEP



Both ZSK and KSK function
as SEPs, each correspond to
a DS (DLV) RR

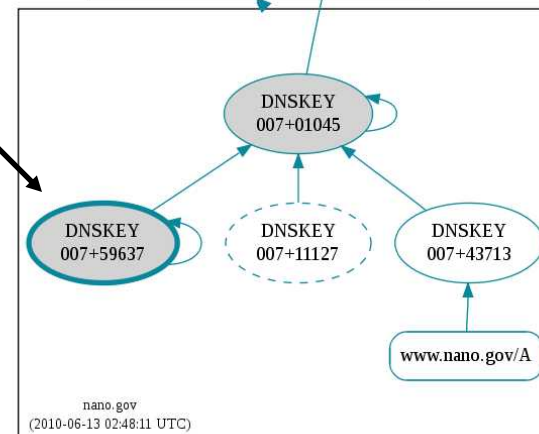
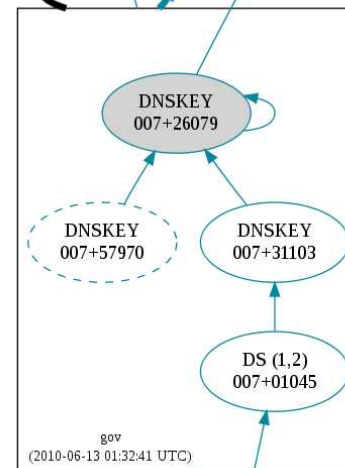
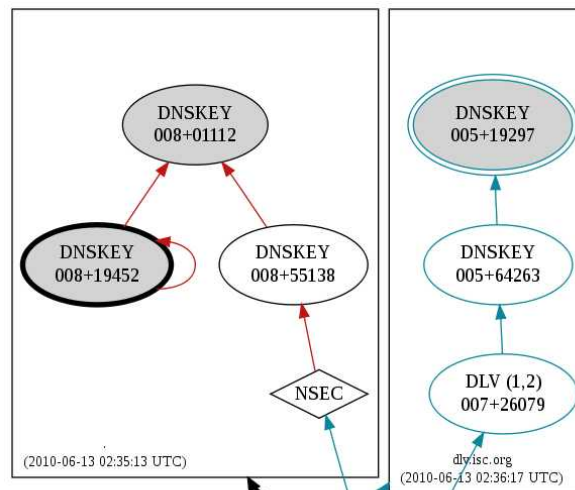


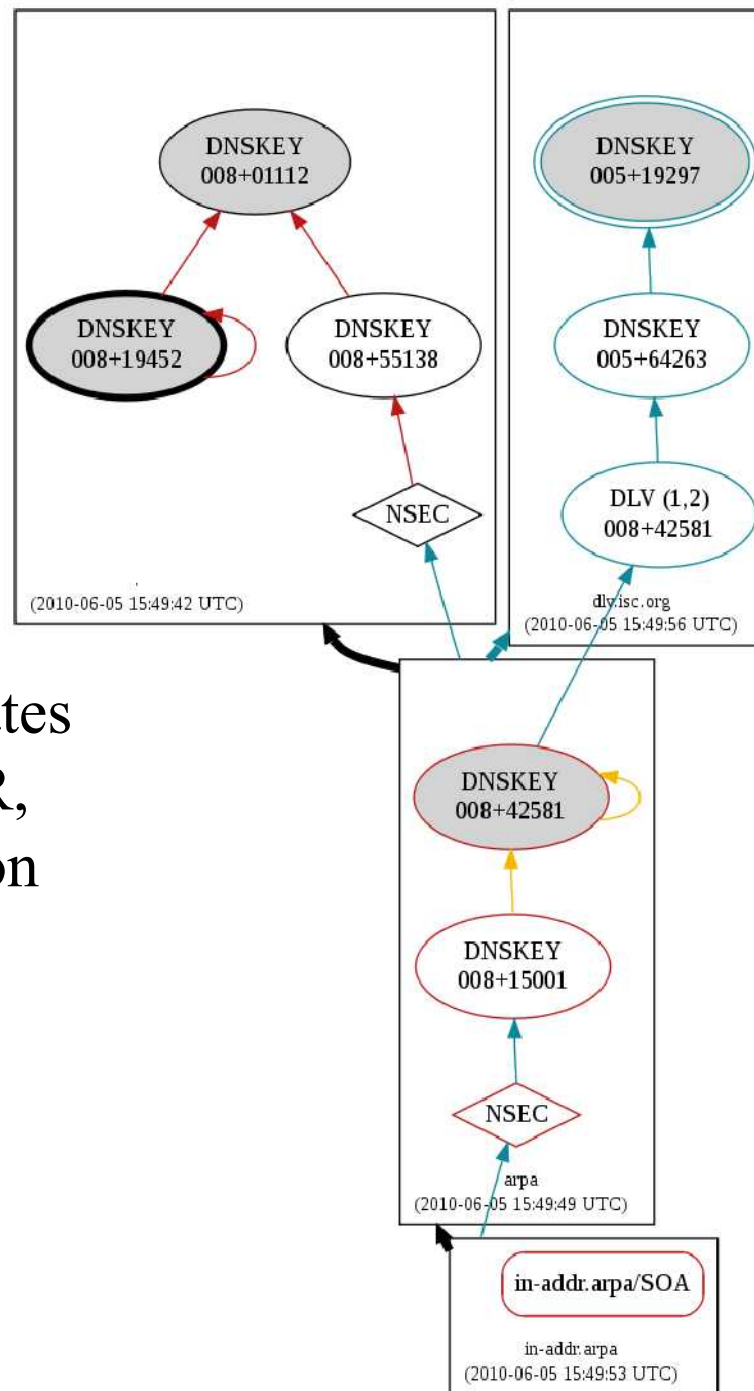


Multiple signatures
across servers; one expired



Revoked DNSKEY:
revoke bit set and self-signed

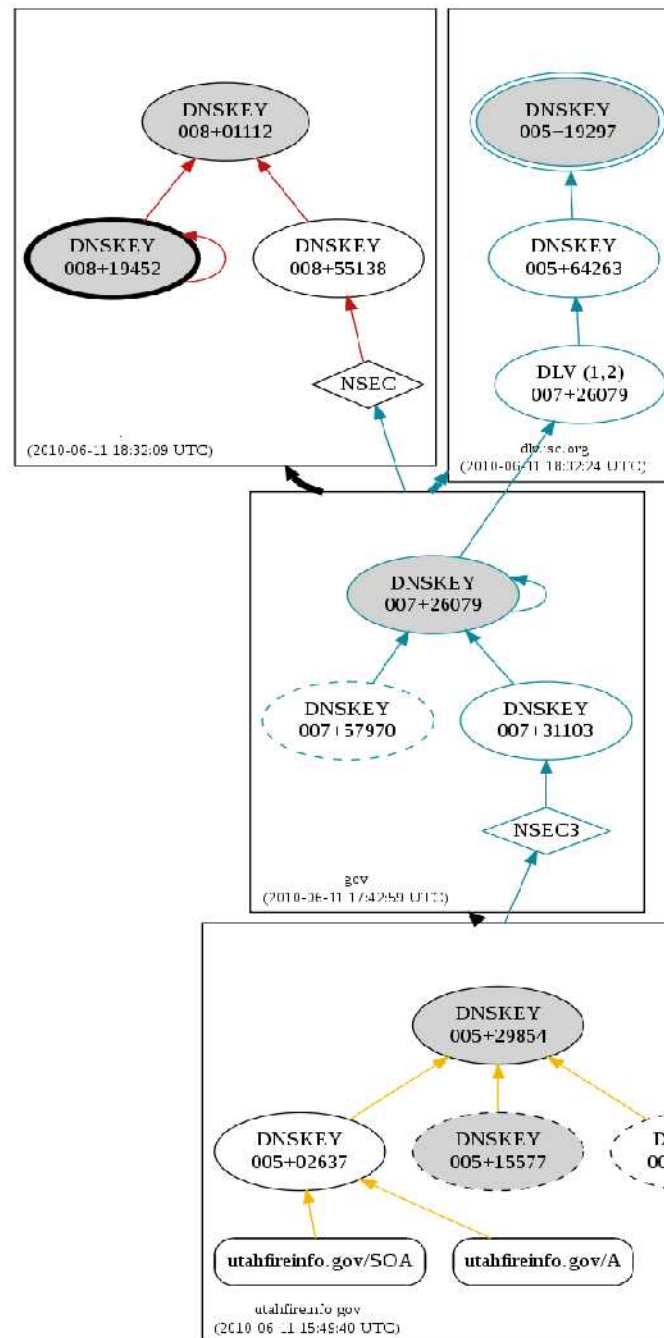




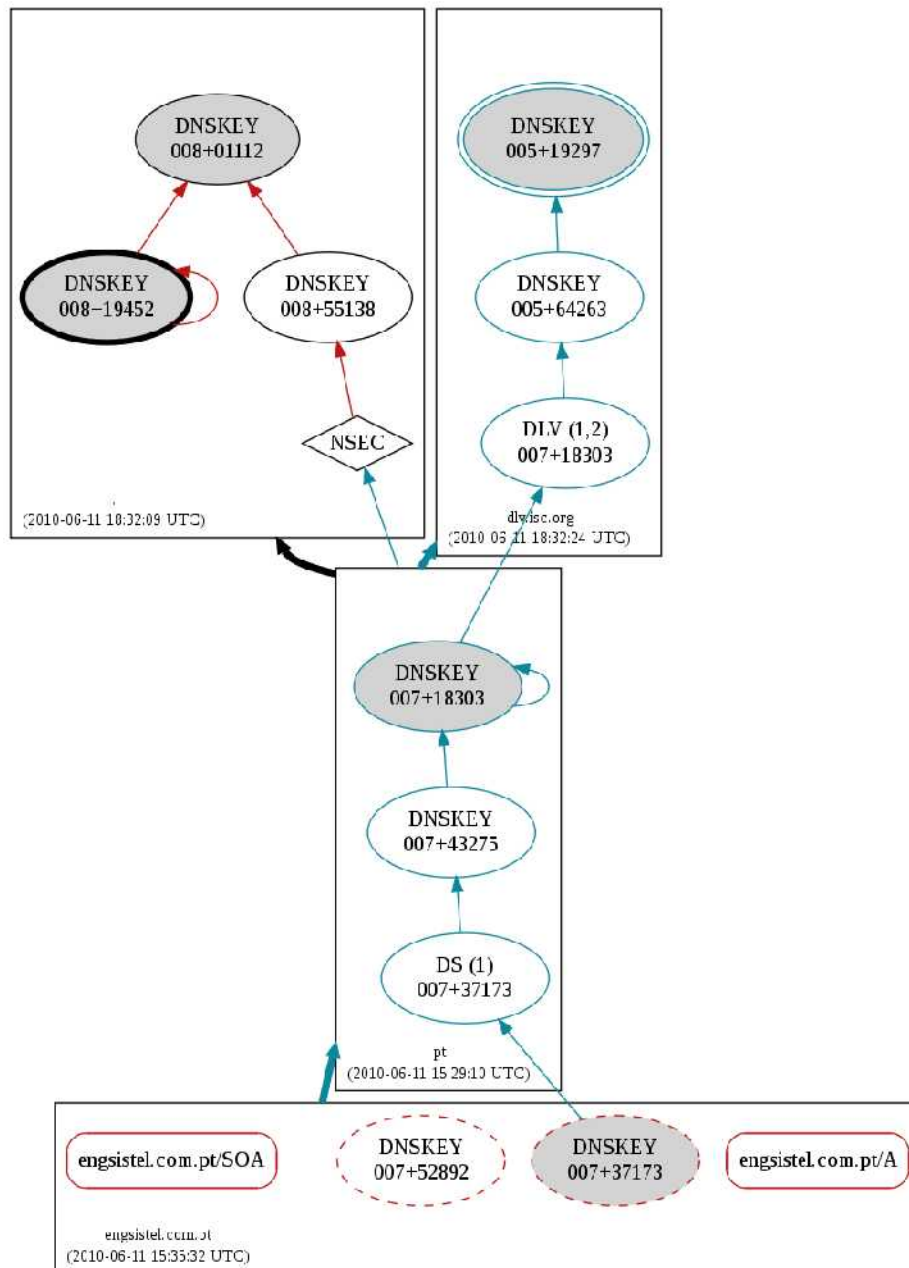
Expired signature: invalidates
NSEC RR covering DS RR,
resulting in bogus validation
below in the hierarchy

in-addr.arpa/SOA
in-addr.arpa
(2010-06-05 15:49:53 UTC)

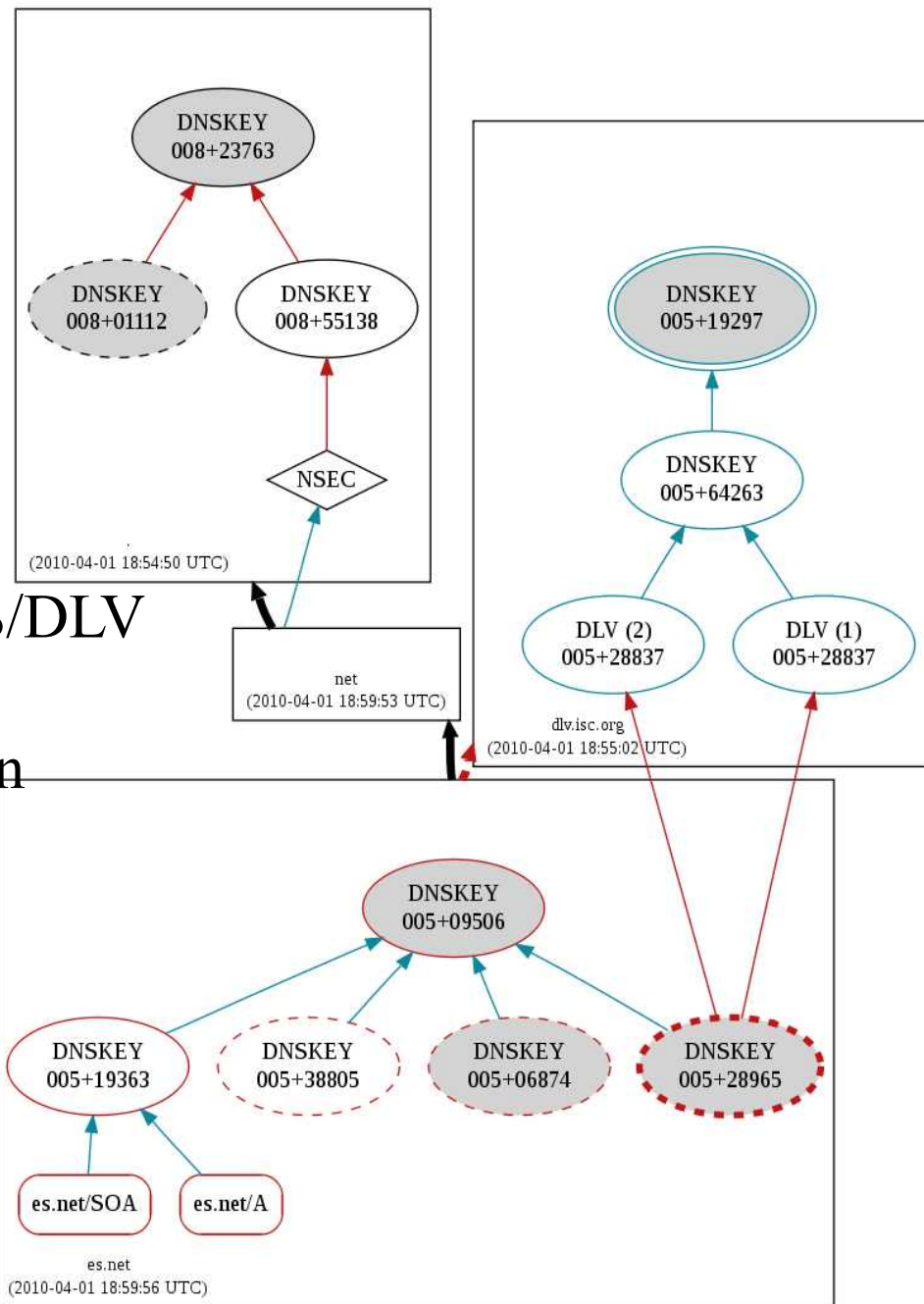
Expired signatures in
island of security: no
effect on security of
names



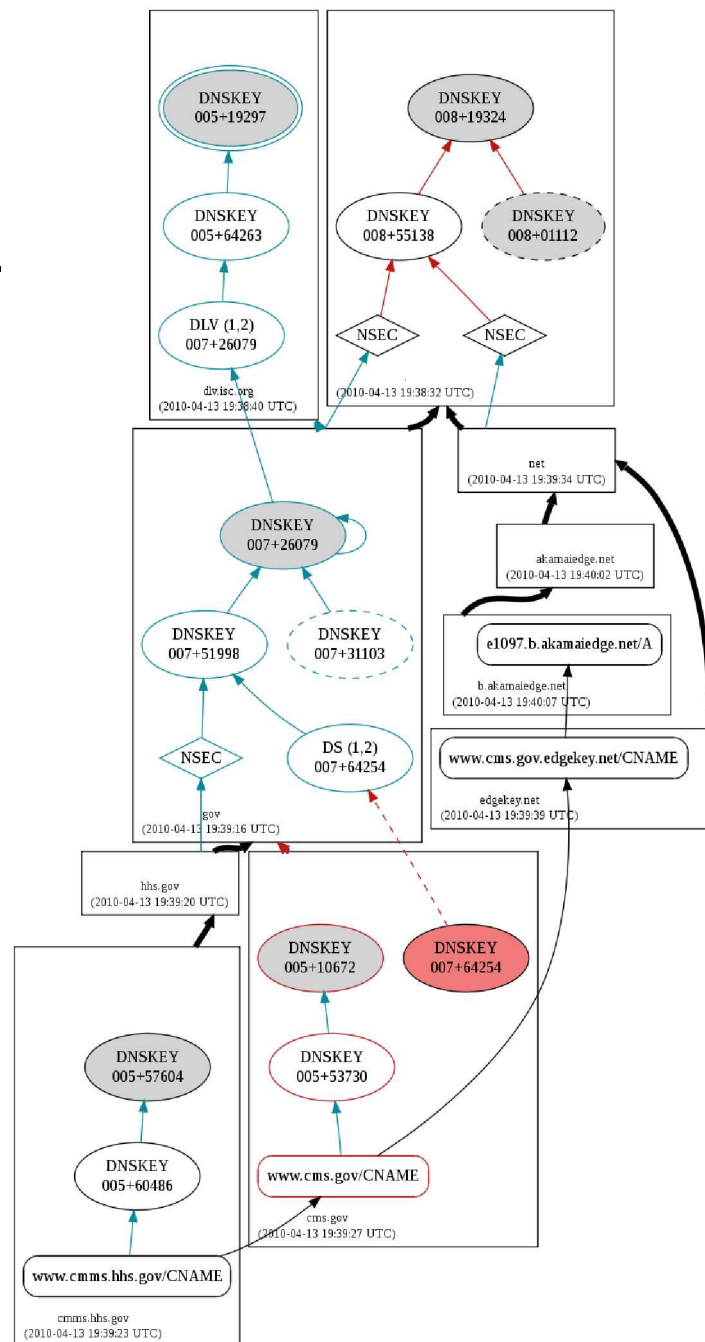
Missing signatures



Bad KSK rollover;
DNSKEY matched with DS/DLV
having previous key tag;
invalid DNSKEY revocation
(missing self-signature)



Dependency complexities



Server status

- Consistency
 - DNSKEY RRset
 - Signature
 - Serial
- PMTU status
- NSEC3 awareness

Servers

68.87.29.164

• (dns101.comcast.org)

Serial: 2010022201

- Low path MTU: Server 68.87.29.164 is attempting to send a payload larger than the supported path MTU. The maximum payload that 68.87.29.164 can send is somewhere between 1328 and 1514 bytes. This limitation may be caused by intervening firewalls or the inability to support IP fragmentation. This size is

cdc.gov.

Servers

198.246.96.61 (icdc-
• us-ns1.cdc.gov, ns1.cdc.gov)
Serial: 288430085

198.246.96.92 (icdc-
• us-ns2.cdc.gov, ns2.cdc.gov)
Serial: 288430085

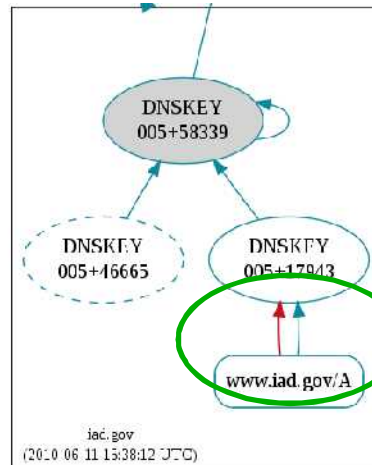
198.246.125.10 (icdc-
• us-ns3.cdc.gov, ns3.cdc.gov)
Serial: 288430085

198.6.1.65
• (auth00.ns.uu.net)
Serial: 288430085

198.6.1.202
• (auth100.ns.uu.net)
Serial: 288430085

- Rogue delegation record: auth100.ns.uu.net appears as a delegation record in gov, but does not exist in the authoritative NS RRset in cdc.gov.

- Missing NSEC3 RRs: cdc.gov is signed with NSEC3, but no NSEC3 RRs were returned by 198.6.1.202.





Outline

- Motivation
- Visualizing DNSSEC
- **Future Work**



Future Work

- **Documentation**
- **Visual history of zone for reference, post-mortem analysis**
- **Regular polling, monitoring/alert services**
- **RESTful interface for queries**



Questions?

`ctdecci@sandia.gov`

`http://dnsviz.net/`