DNSSEC Visualization

NANOG 49

June 15, 2010

Casey Deccio
Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin company, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Outline

- Motivation
- Visualizing DNSSEC
- Future Work

Sandia National Laboratories

Outline

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

Sandia National Laboratories

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
```

Sandia National Laboratories

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 21hKS8YIu/xbX2UJRrLq390d8OT2vQF9wkVl8IVMViLGdxp1fVTzES+6
XtMHvEMxavuGv9fkHk3Kyt5RNrWwJ1ZquhdsTfzJwTpS9f6u7K5B24Au MOHRI5FscQhy85dfMMCOYn7Xa0mqaM8mgy1k88xy8zSFQ/
hTitMgN6HM bd2P/nLYnxMXXnjblIqPe9nzUPFjK4jbQVJsEAkPhOJ+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/9MVBCJd0j5XIvJTpn0OdmCnQEC/pyPI7 2HyXGJ1MItuQLLP7yDGRubrbFwljkX9DCRvrK1xSGmj
+CH2zrFrs30cu tE+w24IuaK3RDL6nVVpZ0pcpjUSBpHja0G4VMiPHbkafyOslL7q101Jd
Ot8Z5FAaEWxCc0rtkKKA3NlmQ64S2RdEYCV1PRO1fvumiCzLE/oJ/vNN
nthmmw8F14zV73jxnYuEZaKLCz5Dl3LKyHhBXff0q2Z62WR637knH52o 8Gow1gvlQztFDrzAfbYLnd+UGxlGh0/
vaxnROp5JVC1WKK3MjOnNhZbk E5pO6Q==
7yYXSg==
```

Sandia National Laboratories

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
```

Sandia National Laboratories

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 AwEAAcpyc4bhl2jawsXT7
miCBKajTeCXaToPay1zziVIcbVf/1F0vay7KJx LDUGIti8DVCksyRoCakgDQsacI
medicare.gov. 1296000 IN DNSKEY 257 3 5 AwEAAchzoM8KoxpaUTT
k0gVyODy1YySFmnZW8Nin/PG82BAt+s1wptKfgBX8ssc68UfitvfnNxO NK2t0Q
ULFVKd7GGBInXIGD3LrtgfaGkUBV2XjG9XH2leSxvXvk29ovNdrLYjWs UFPI
82hGflr1xkmKiLjejop10gR0pJW2qVMEG9QZQW0nHEbWEeNO1NA7omtX 0b
medicare.gov. 1296000 IN RRSIG DNSKEY 5 2 1296000 20100430202133 20100426194625 35677 medicare.gov. xU/Y+q7sWM
+sjcn9upiz7vUUJZ03YxX+M2Ji89QqMjZSe2eHXbnMQAZh axlpIwHWftrTpTWzCJWO/dFuk7mNkcegC/4l9XoGeTkCL/lnLaseep2j
3RJPsmFXFLOPGvY2v2Vnik45qJweNmZYse083ouOurAUpCXwpJVUzRa/ plmtt6RdzKM4hT3oc4qTEZMaKDku/qEICPaPQPz0g2G1Z8Lr86vz+LCp
V3tw4TT5Pf92wdRTXzvUG+ZonfyYhD4jNgFKhm6hVreHJmon6hPWo4lK N1HJIZSbV7KDV5GJo5CHFNxYLRmJtfg8YxV4NXqSmOSy8EDgOao1lYbK
cO+9PA==
medicare.gov. 1296000 IN RRSIG DNSKEY 5 2 1296000 20100430202133 20100426194625 39045 medicare.gov.
LRmOwpQoqE5ScCDHHkILhPoxBJaMeV0BYMx8M7lXw96F9oI9ub6MWz+u MZkXmyfkld5UKidKQGU1tqLJgIZhOwztRBgYXfTpL7WHP9N0LcfIcs+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. Jz14rLZ7r2IaOJHLxDqmIBRvYCH5lPUVh
+4kKZit9Rv7wn9oLkcgTXQA rp46Sa0L2FzrEC6fuEDZ6siXKKUfteQ8TaLbnikPuD00yAmYyDUpvG0E YLwPU0XIG4J5axly1FRu1mJ7843ej/
FmmnEfqOq55jzf3Oc+hW18KTFB XpA=

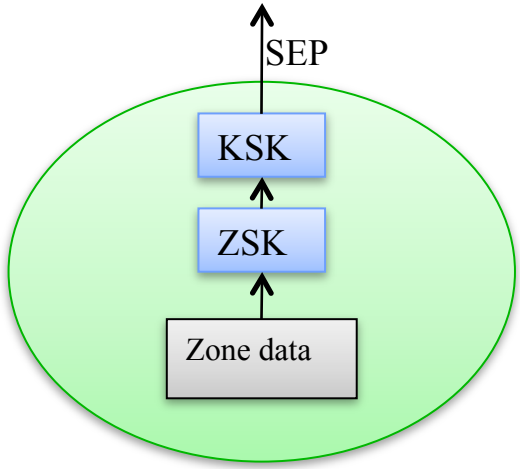
By signature analysis:
- ZSK id = 39045
- KSK id = 35677
- DS key tag = 26508

  => DS references DNSKEY 26508 which does not exist

Sandia National Laboratories

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**



Sandia National Laboratories

More Automated Methods

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

Sandia National Laboratories

Outline

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

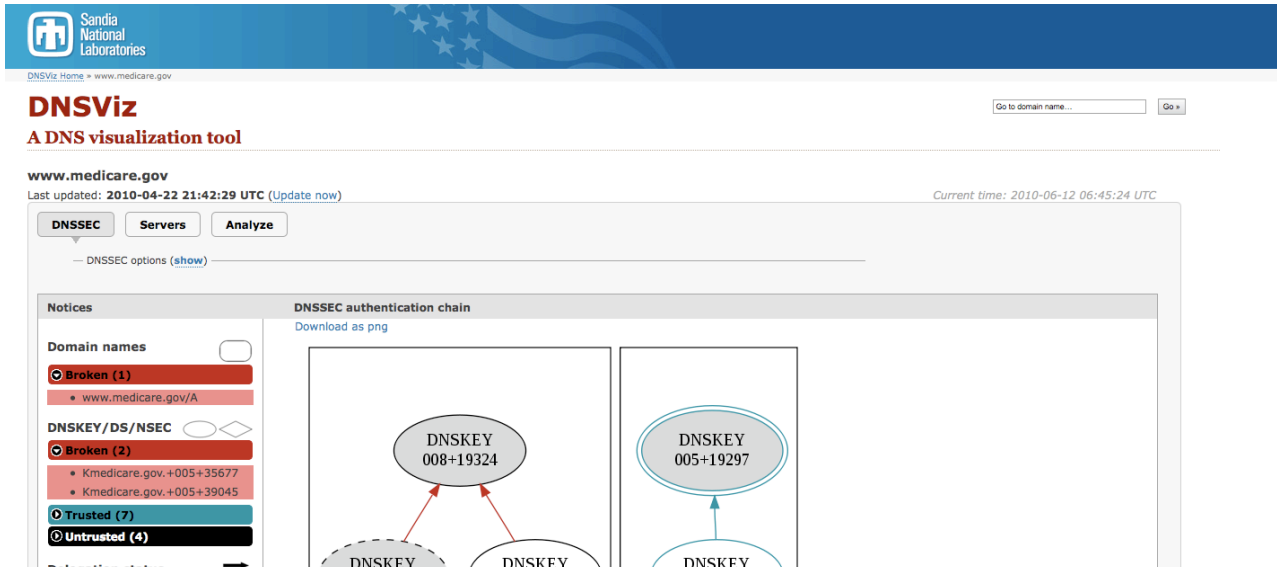
Sandia National Laboratories

DNSSEC Visualization

"A picture is worth one thousand DNS queries."

- **Loosely adapted from a quote attributed to Chinese proverb**

http://dnsviz.net/



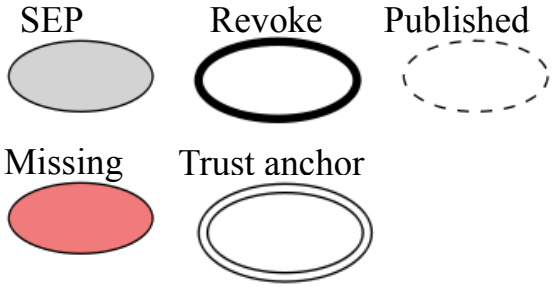
Sandia National Laboratories

Visualization Components

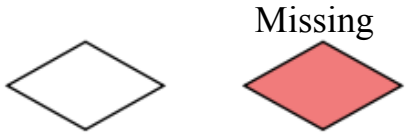
Domain name

DNSKEY/DS RR

DNSKEY attributes



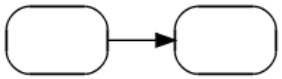
NSEC proving non-existence of DS RRs (insecure delegation)



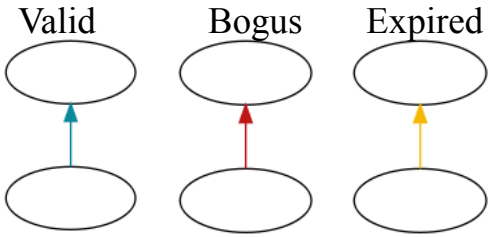
Sandia National Laboratories

Visualization Components

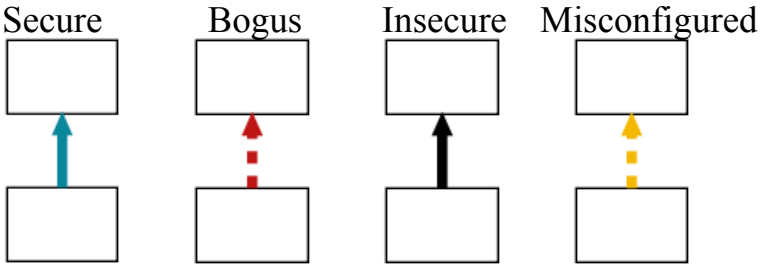
Alias dependency



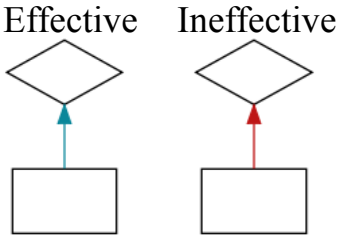
Signature or digest



Delegation



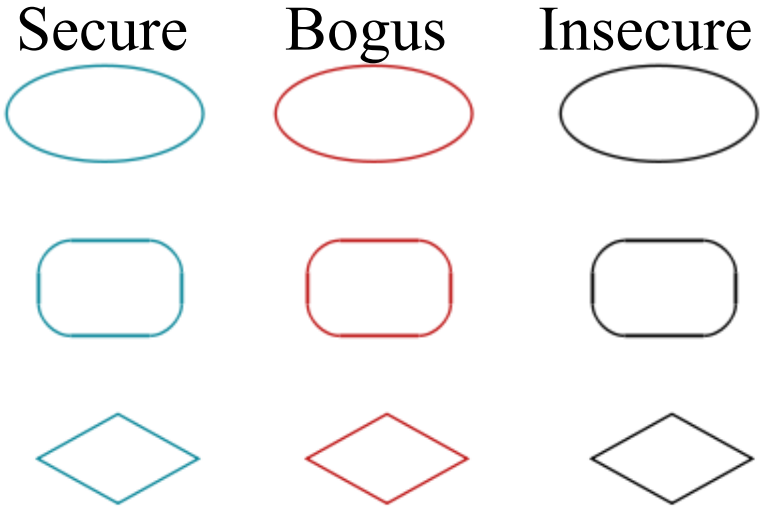
Proof of insecure delegation



Sandia National Laboratories

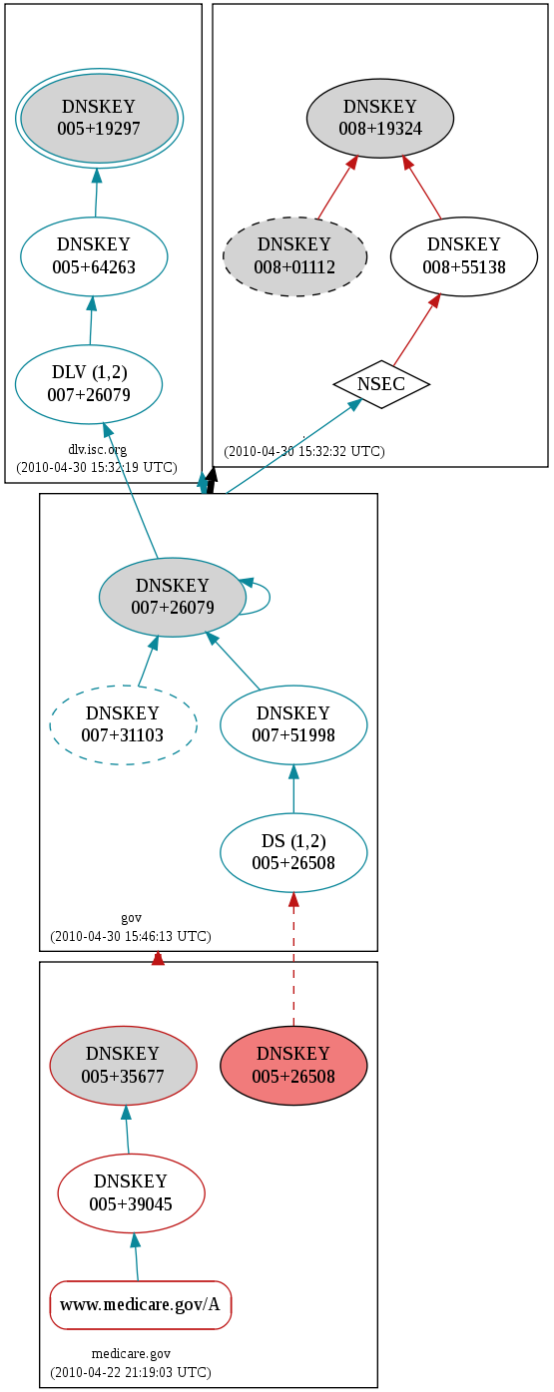
The Bottom Line

- 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?

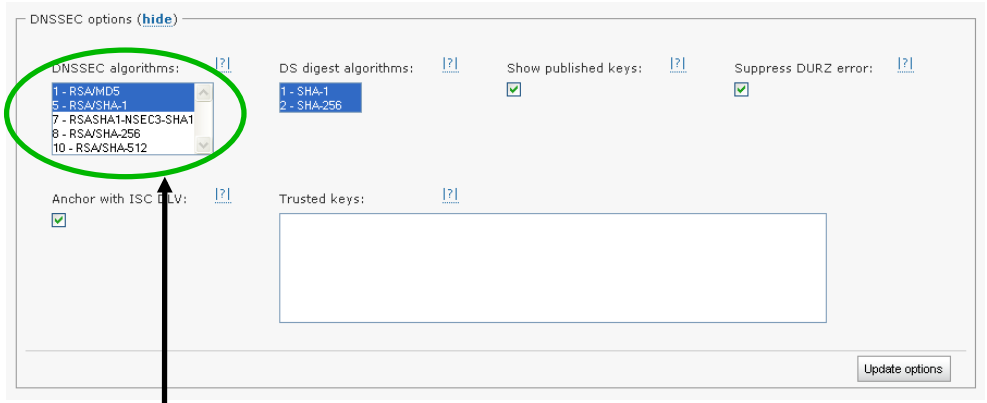


Sandia National Laboratories

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

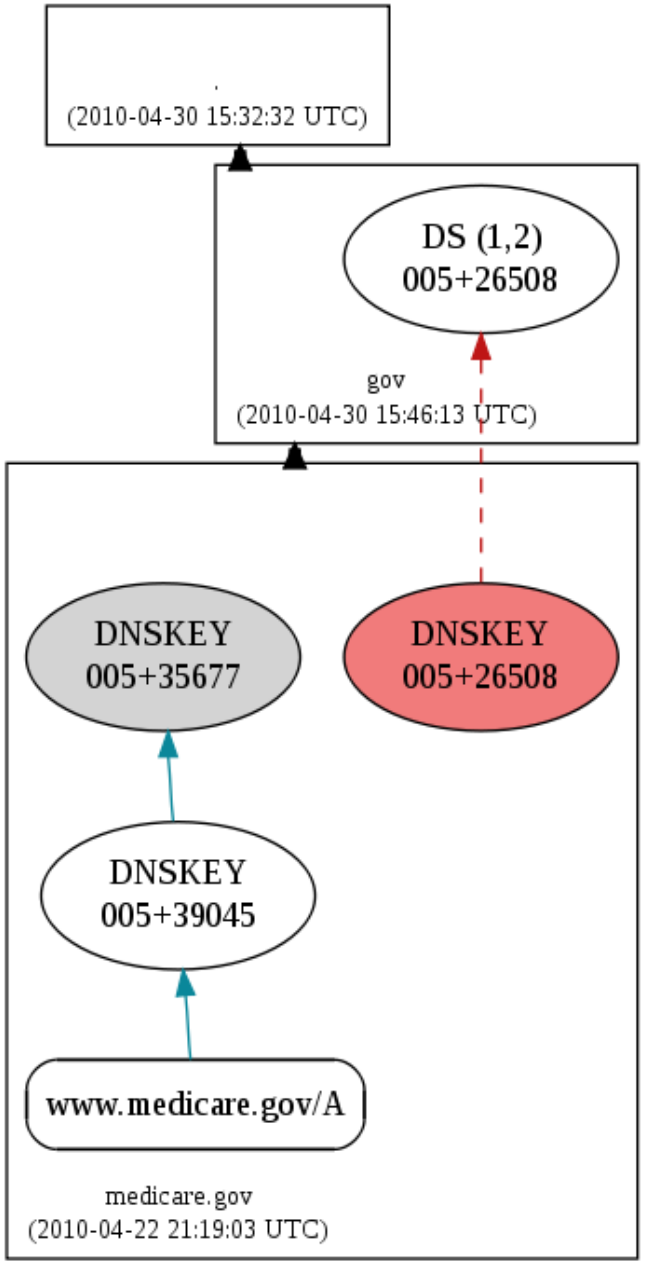


Sandia National Laboratories



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

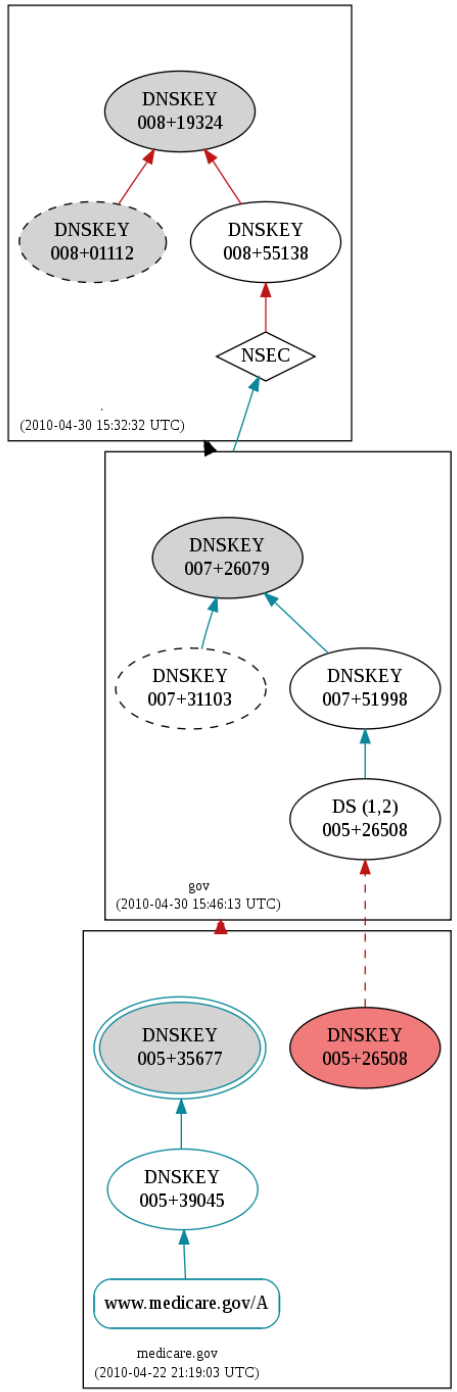
www.medicare.gov/A now "insecure" instead of "bogus"



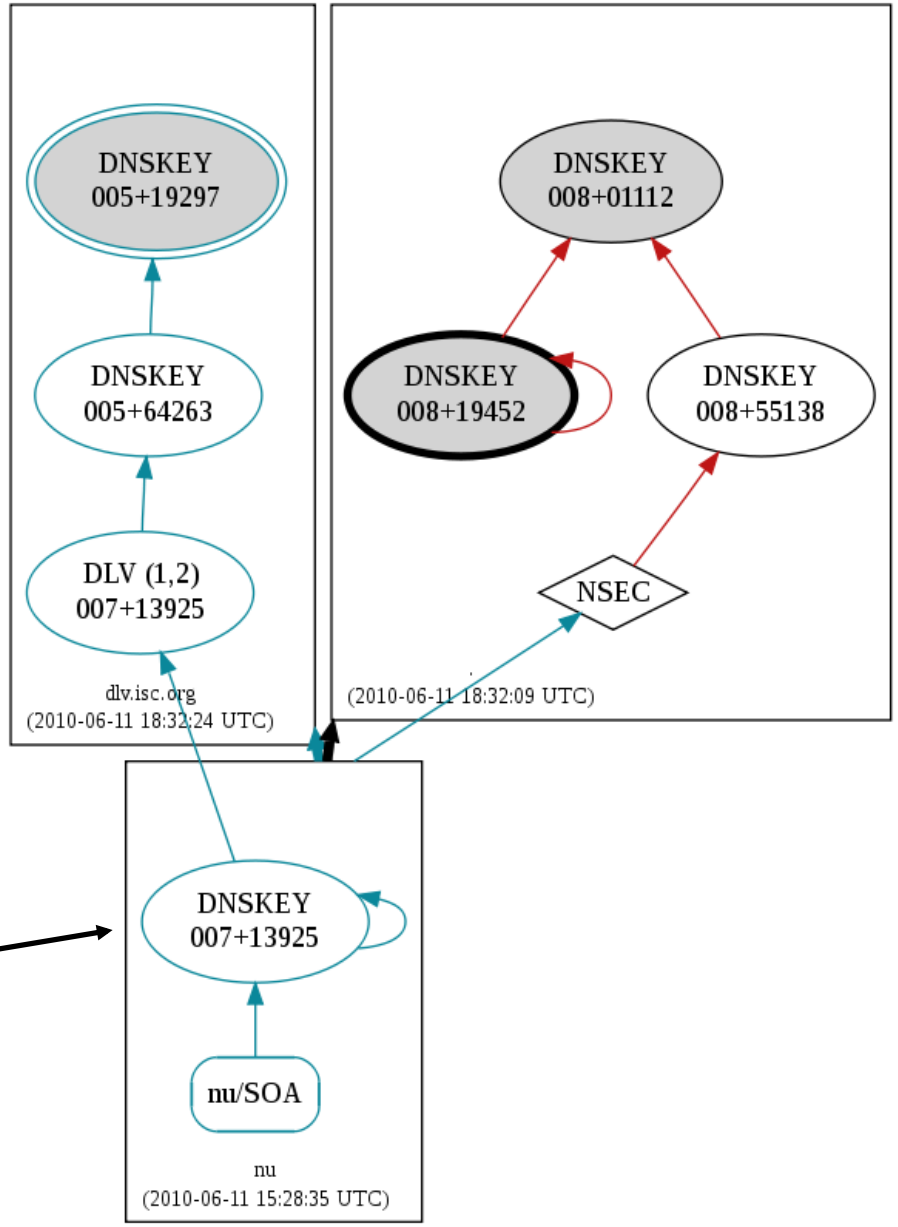
Sandia National Laboratories

Configurable trust anchors
and ISC DLV support

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

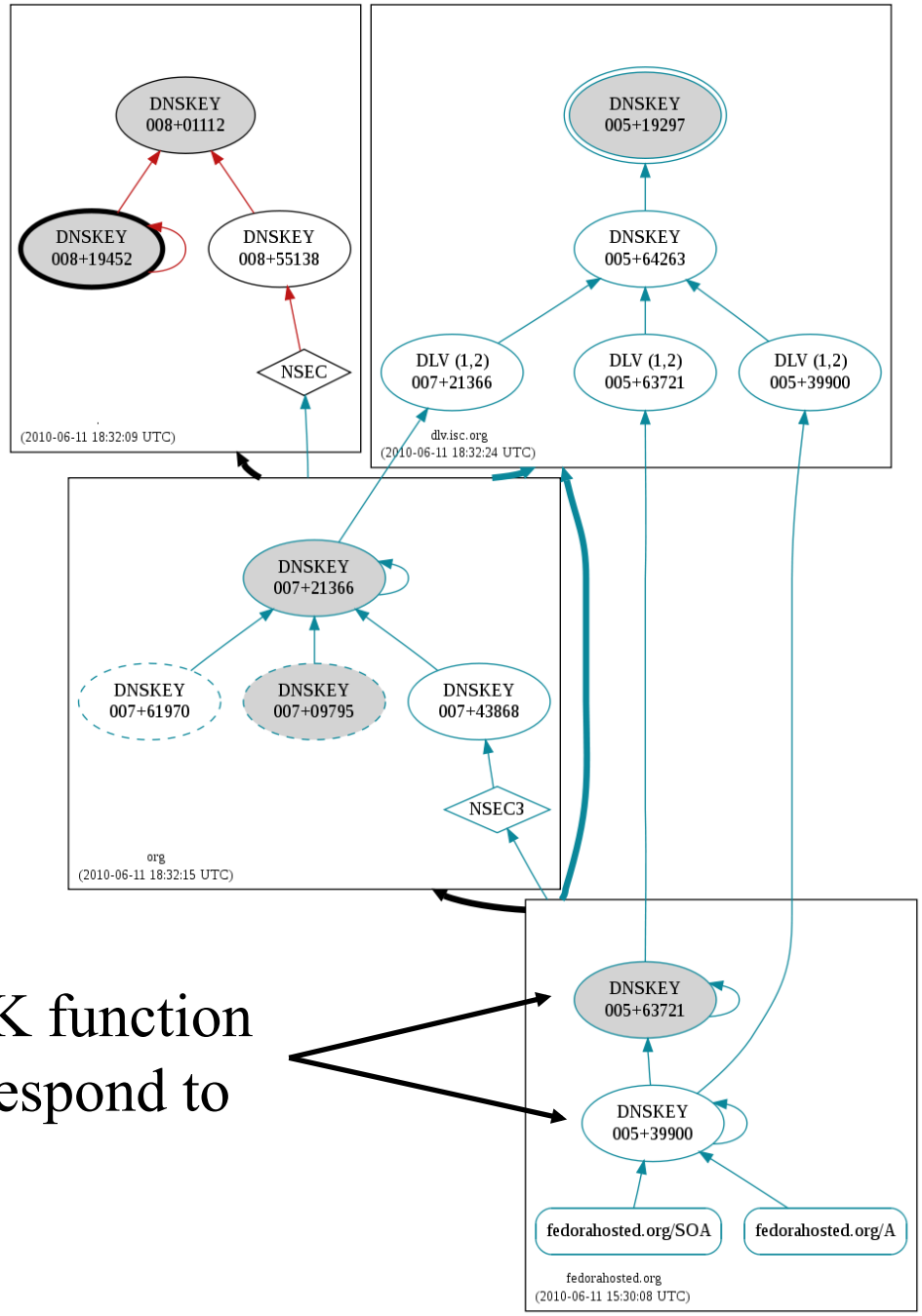


Sandia National Laboratories



Single DNSKEY,
functioning as
ZSK, KSK, and SEP

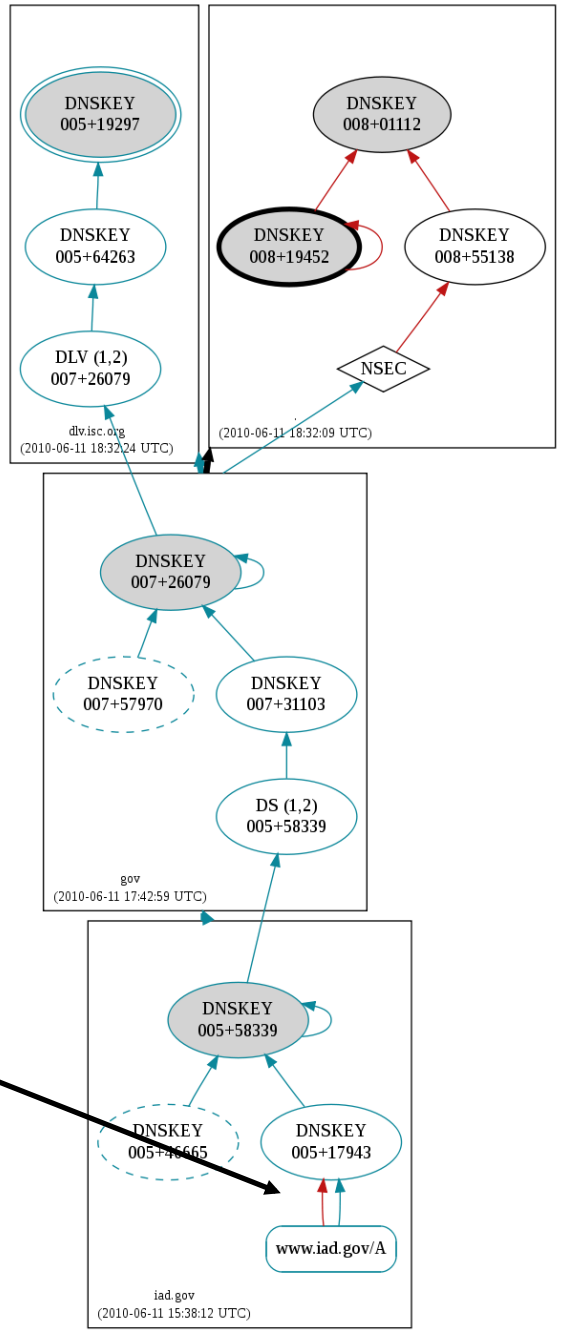
Sandia National Laboratories



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

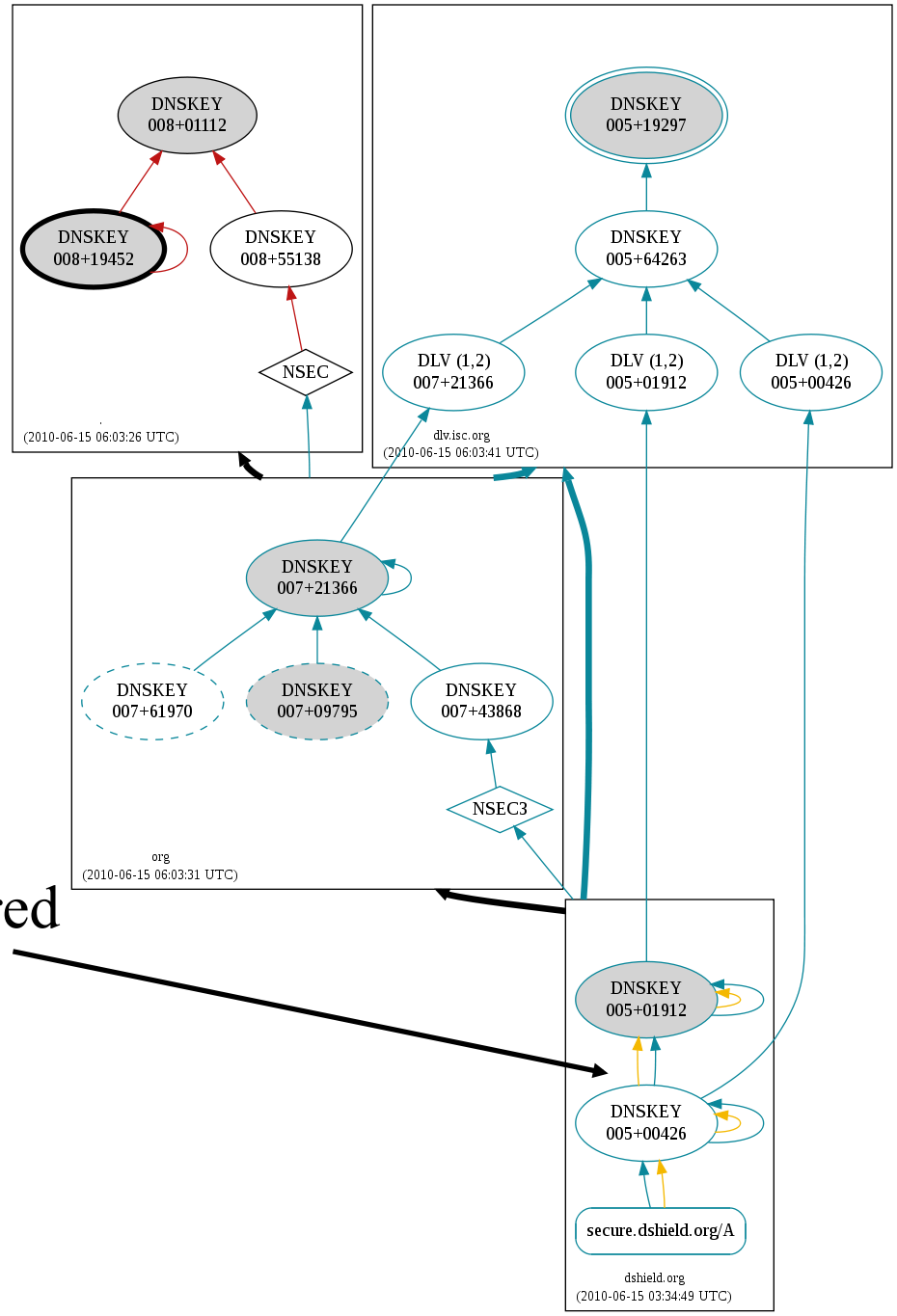
Sandia National Laboratories

Multiple signatures
across severs; one bogus



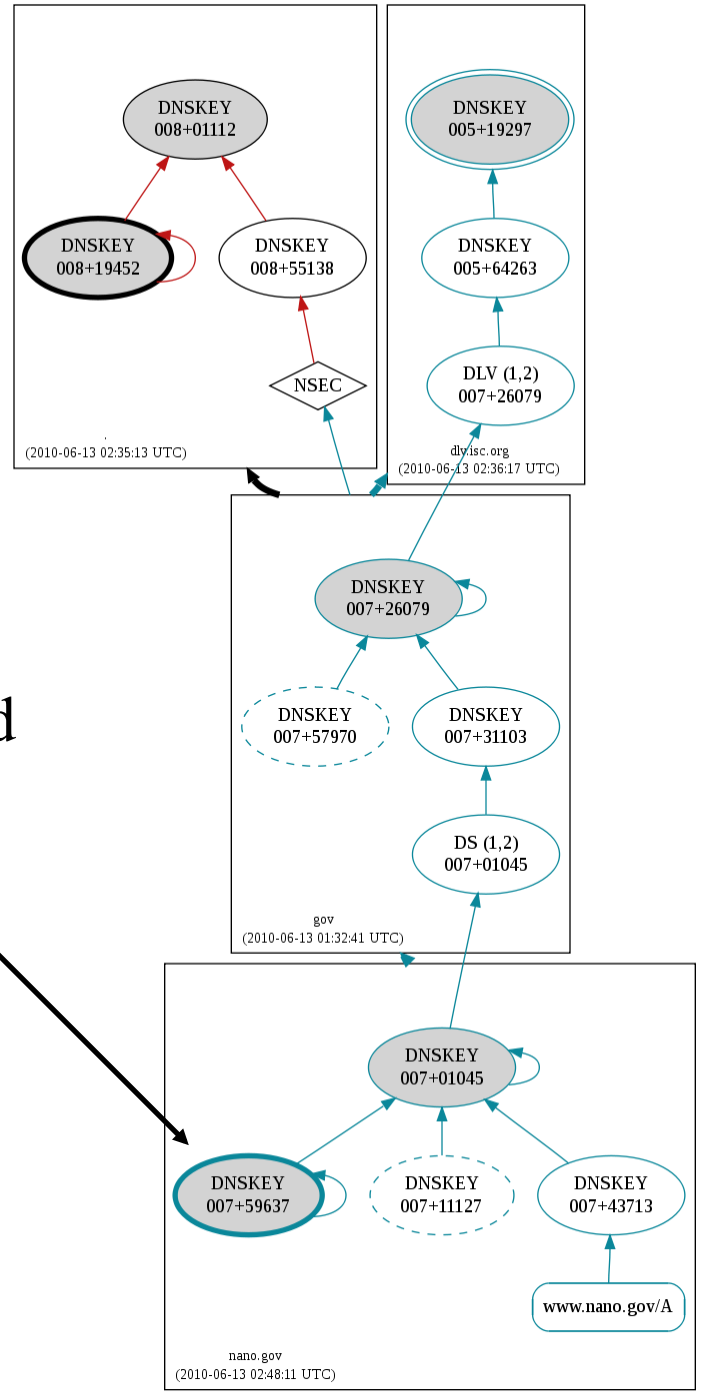
Sandia National Laboratories

Multiple signatures
across severs; one expired



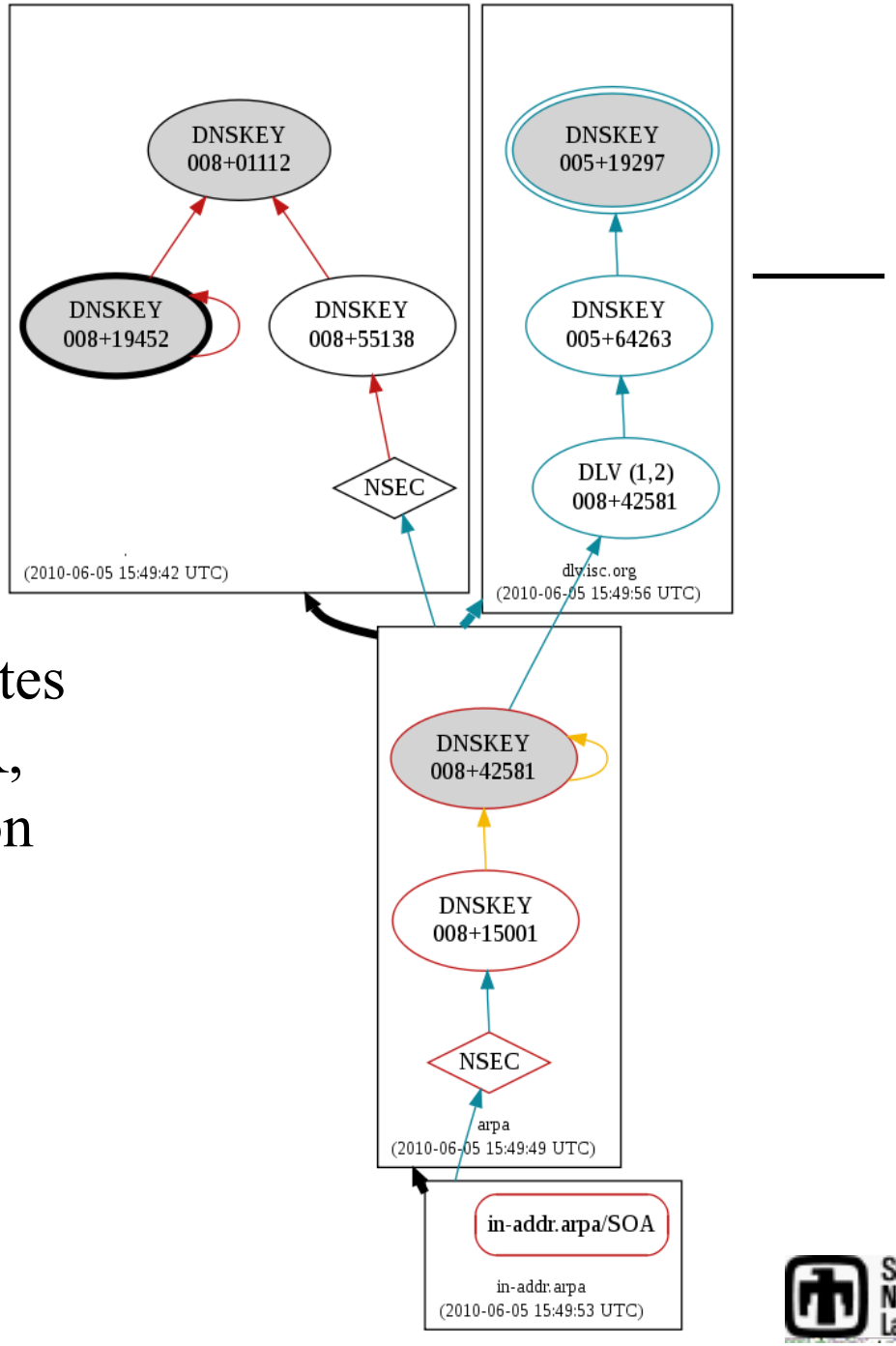
Sandia National Laboratories

Revoked DNSKEY:
revoke bit set and self-signed



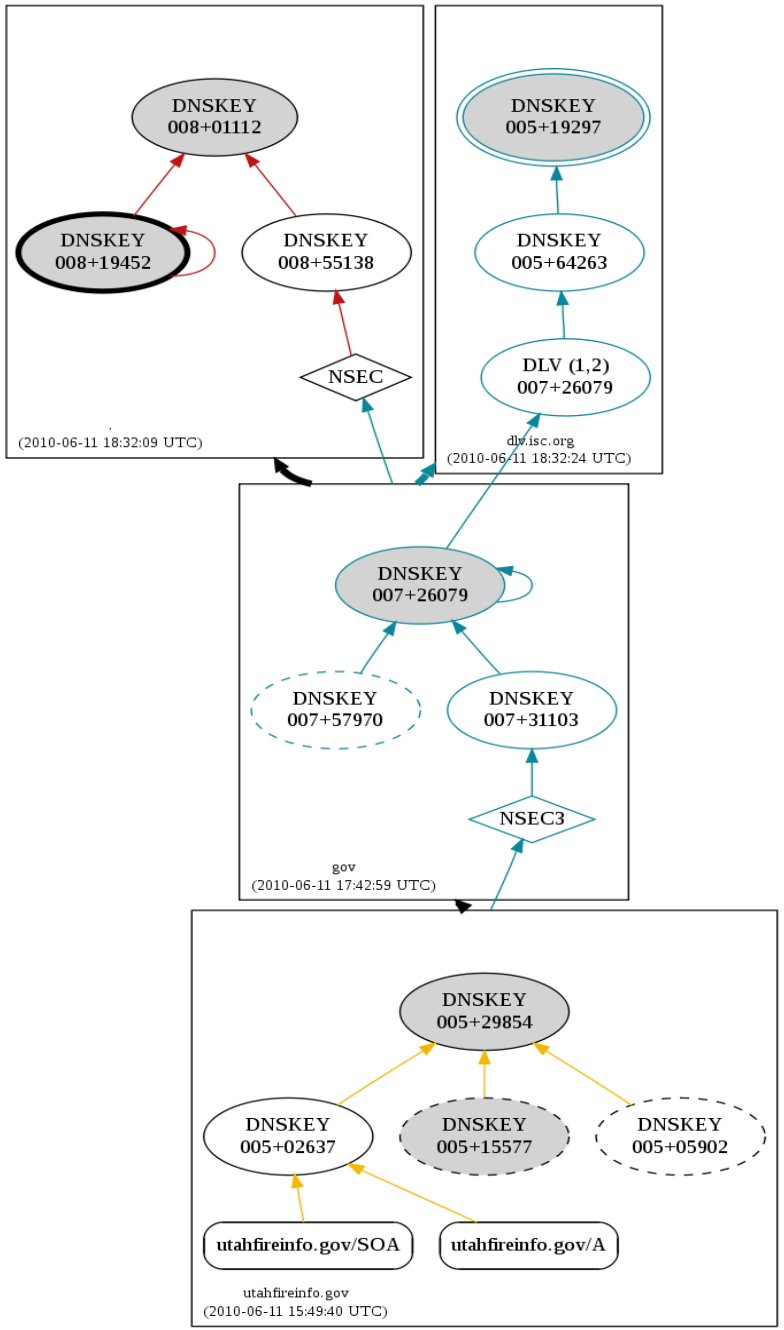
Sandia National Laboratories

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



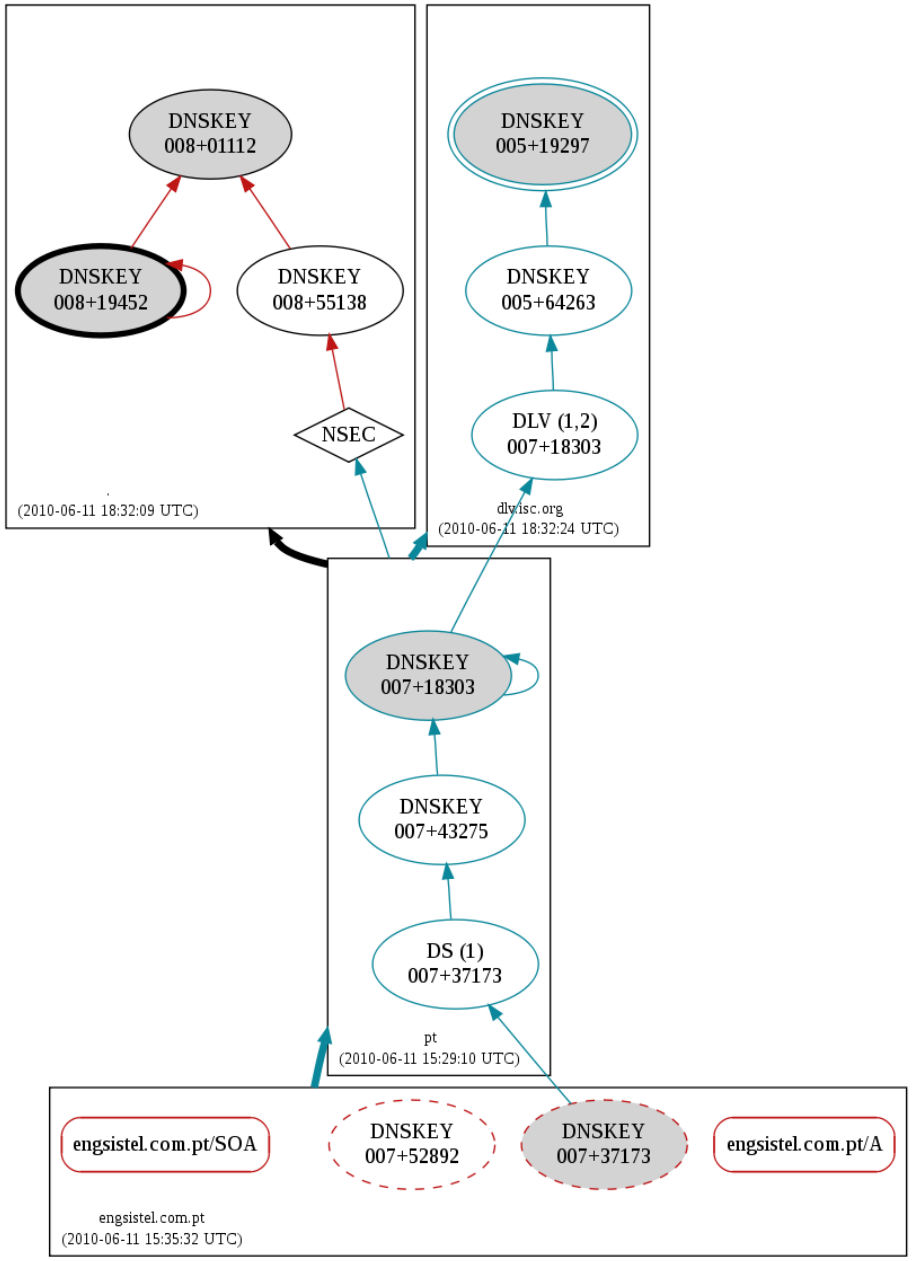
Sandia National Laboratories

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



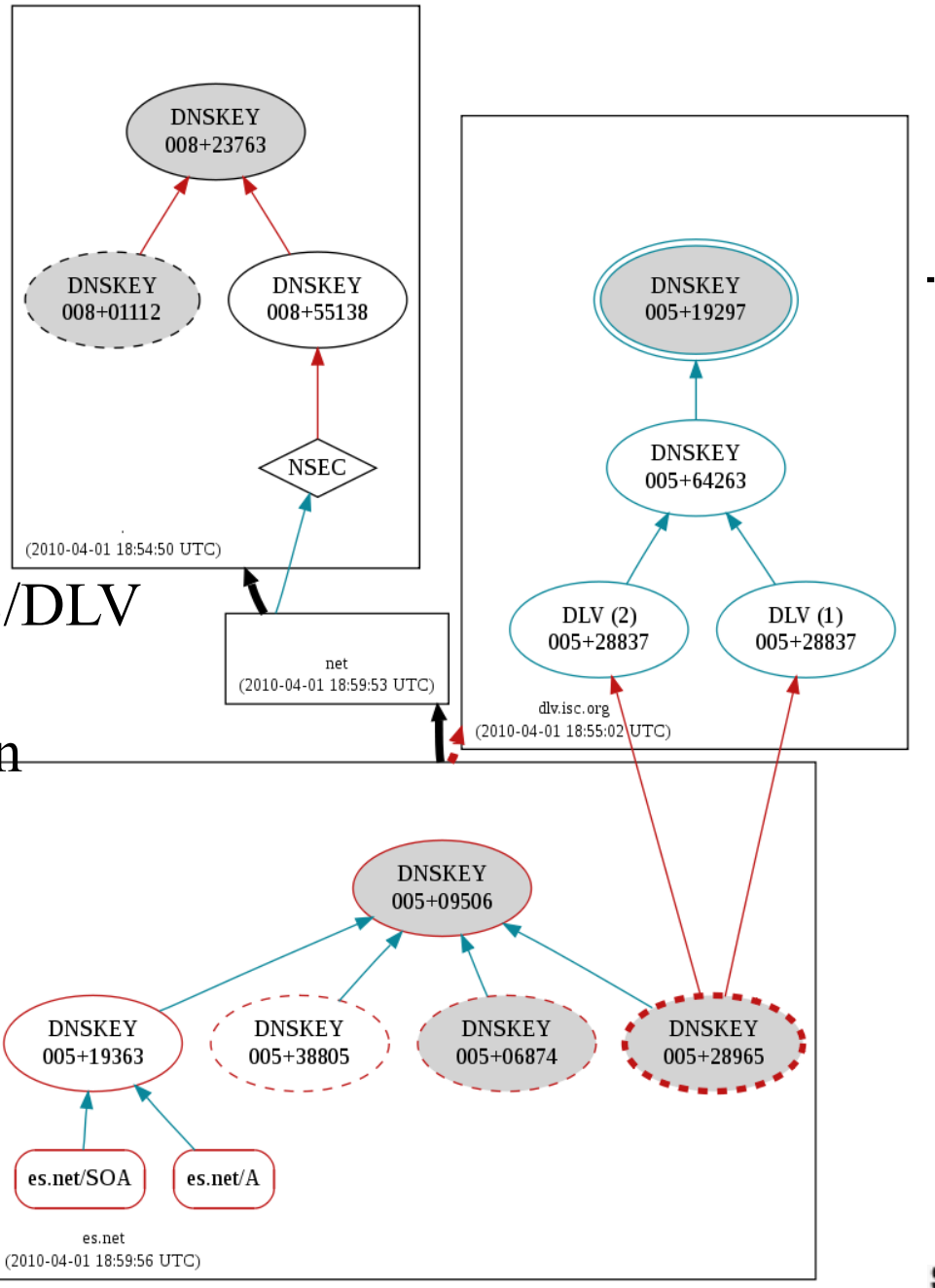
Sandia National Laboratories

Missing signatures



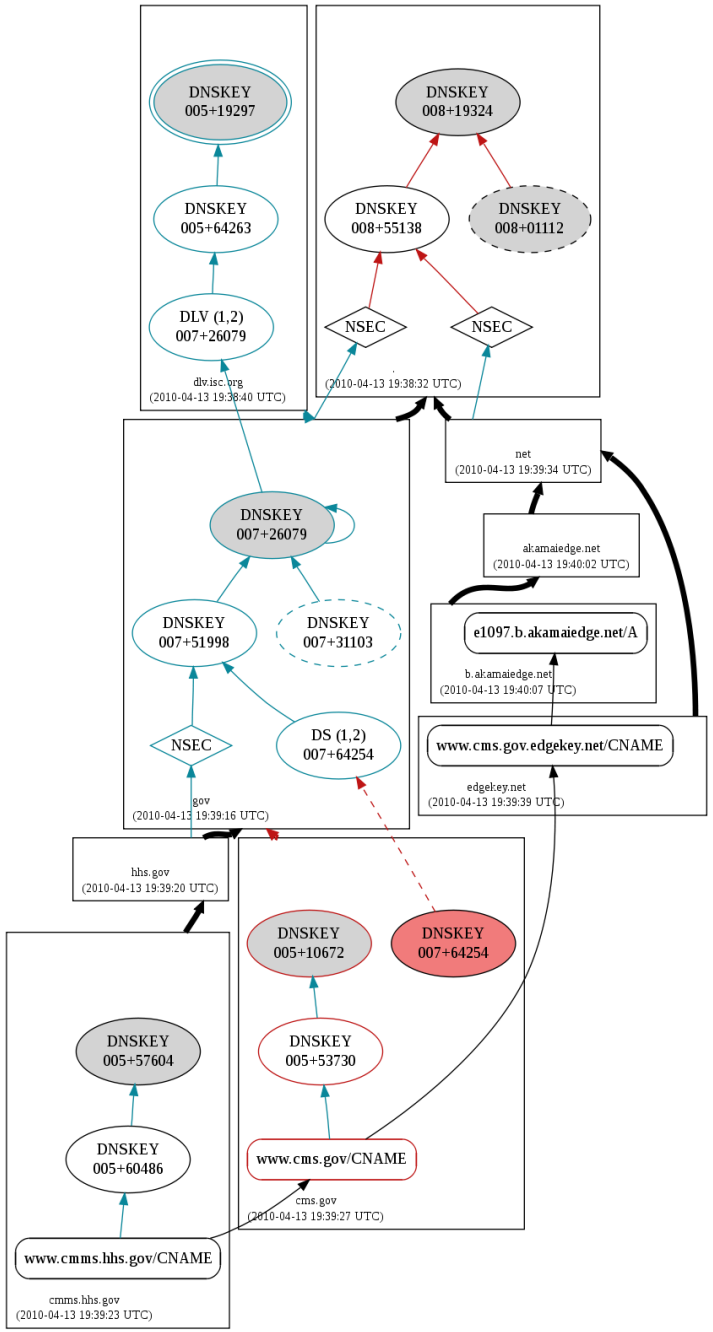
Sandia National Laboratories

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



Sandia National Laboratories

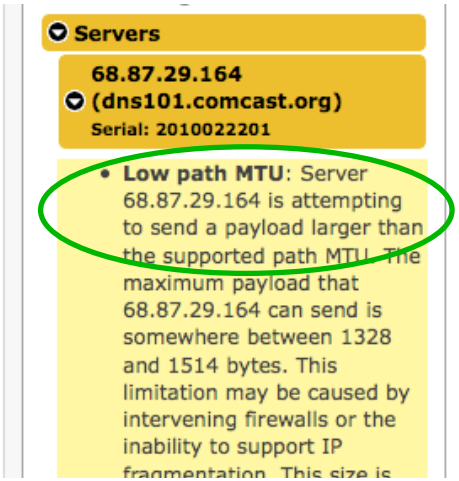
Dependency complexities

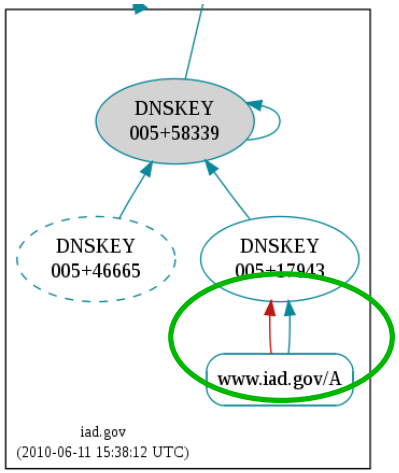


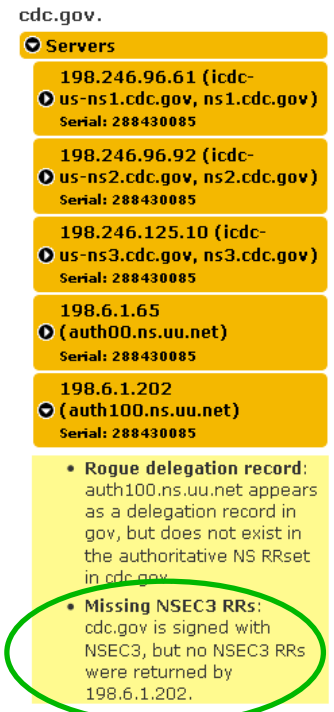
Sandia National Laboratories

Server status

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







Sandia National Laboratories

Outline

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

Sandia National Laboratories

Future Work

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

Sandia National Laboratories

Questions?

ctdecci@sandia.gov

http://dnsviz.net/

Sandia National Laboratories