# Visual DNSSEC Troubleshooting with DNSViz

RIPE 60

6 May, 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

# 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
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==
```

# 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 OWoIC6eBxbiha1+492SQ4VDQYA8wwmlIF9MFRLrrboo25KUsbIfk0The
440l9heY2Wxm74HXBsJclQEbKvNumx6fRPzmad4jK3RjzLzp4barn282 mmA=

casey@rome:~$ dig +dnssec @ns1cms.rdcms.eds.net. medicare.gov dnskey
;; ANSWER SECTION:
medicare.gov.          1296000 IN      DNSKEY  256 3 5 AwEAAcpyc4bhl2jawsXT73t
GeW8YqUtBudvA0phC/miCBKajTeCXaToPay1zziVIcbVf/1F0vay7KJx LDUGIti8D
Bo81wMO5
medicare.gov.          1296000 IN      DNSKEY  257 3 5 AwEAAchzoM8KoxpaUTT5
k0gVyODy1YySFmnZW8Nin/PG82BAt+s1wptKfgBX8ssc68UfitvfnNxO NK2t0Q2q
ULFVKd7GGBInXIGD3LrtgfaGkUBV2XjG9XH2leSxvXvk29ovNdrLYjWs UFPBz
82hGflr1xkmKiLjejop10gR0pJW2qVMEG9QZQW0nHEbWEeNO1NA7omtX 0b3ZZq6Jfc0=
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 rp46Sa0L2FzrEC6fuEDZ6siXKKUfteQ8TaLbnikPuD00yAmYyDUpvGUE
YLwPU0XIG4J5axly1FRu1mJ7843ej/FmmnEfqOq55jzf3Oc+hW18KTFB XpA=
```

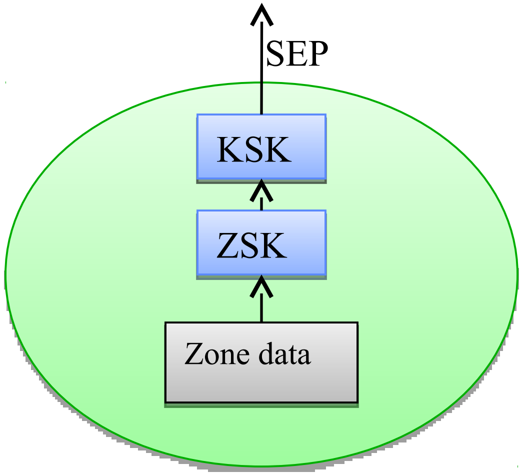
By signature analysis only (key tags unknown):

- ZSK id = 39045
- KSK id = 35677
- DS key tag = 26508

=> Either DNSKEY 26508 is missing or it is simply not being used to sign medicare.gov's DNSKEY RRset

# 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

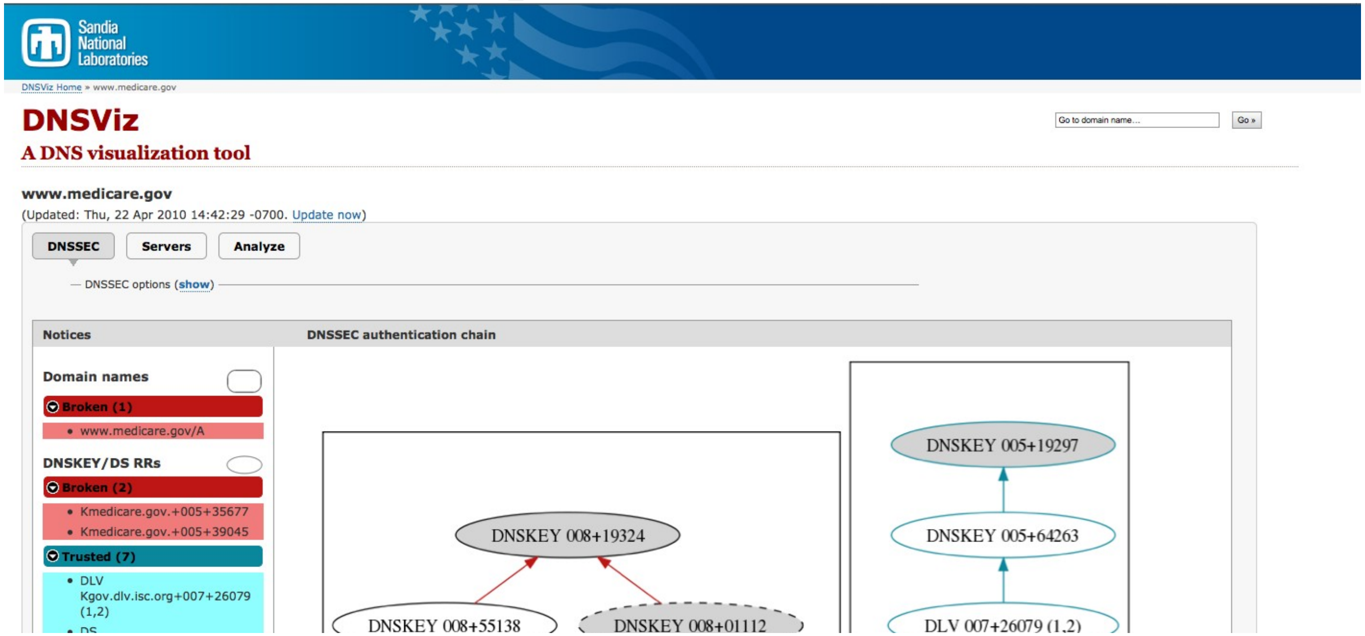
- Motivation
- **Visualizing DNSSEC**
- Future Work

# DNSSEC Visualization

*"A picture is worth one thousand DNS queries."*

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

http://dnsviz.net/



DNSViz Home » www.medicare.gov

**DNSViz**

**A DNS visualization tool**

**www.medicare.gov**

(Updated: Thu, 22 Apr 2010 14:42:29 -0700. Update now)

— DNSSEC options (show)

**Notices**

**Domain names**

Broken (1)

- www.medicare.gov/A

**DNSKEY/DS RRs**

Broken (2)

- Kmedicare.gov.+005+35677
- Kmedicare.gov.+005+39045

Trusted (7)

- DLV Kgov.dlv.isc.org+007+26079 (1,2)
- DS

**DNSSEC authentication chain**

# Visualization Components

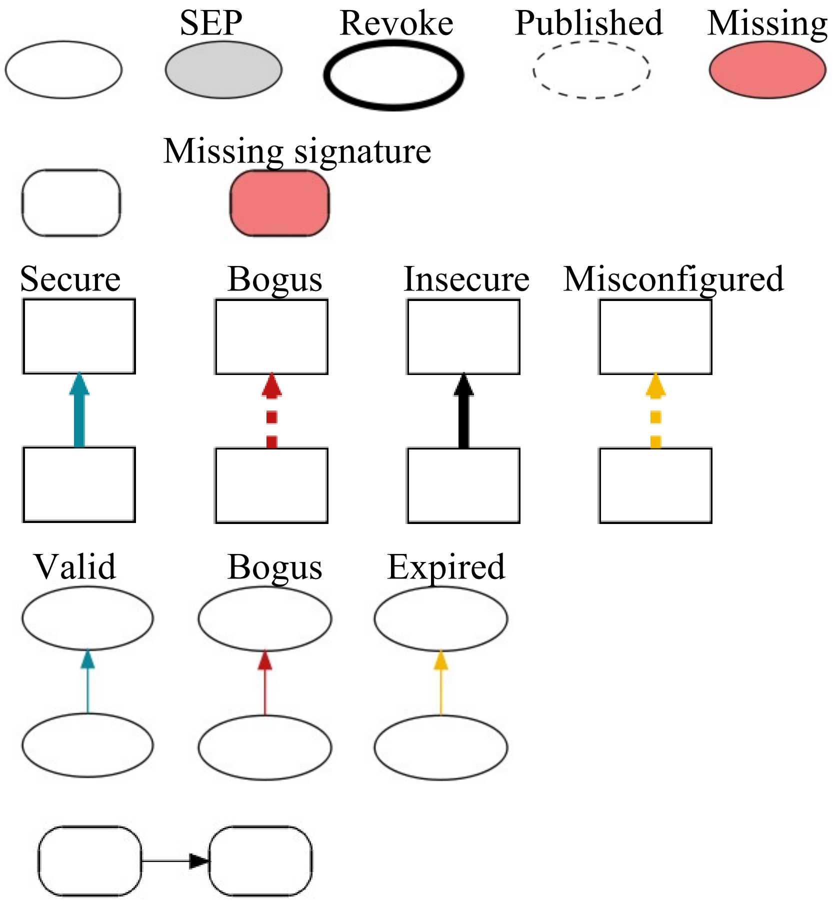
DNSKEY/DS

Domain name

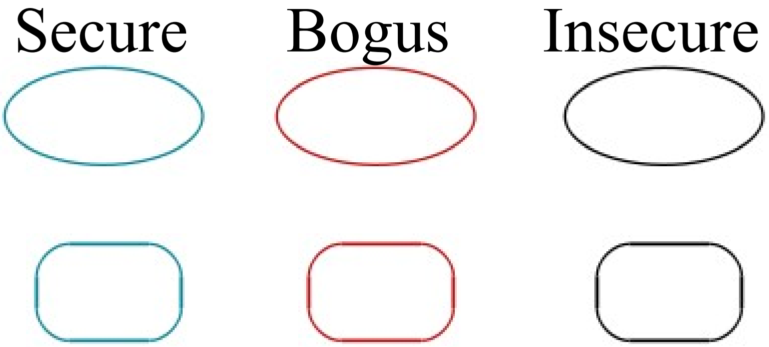
Delegation

Signature or digest

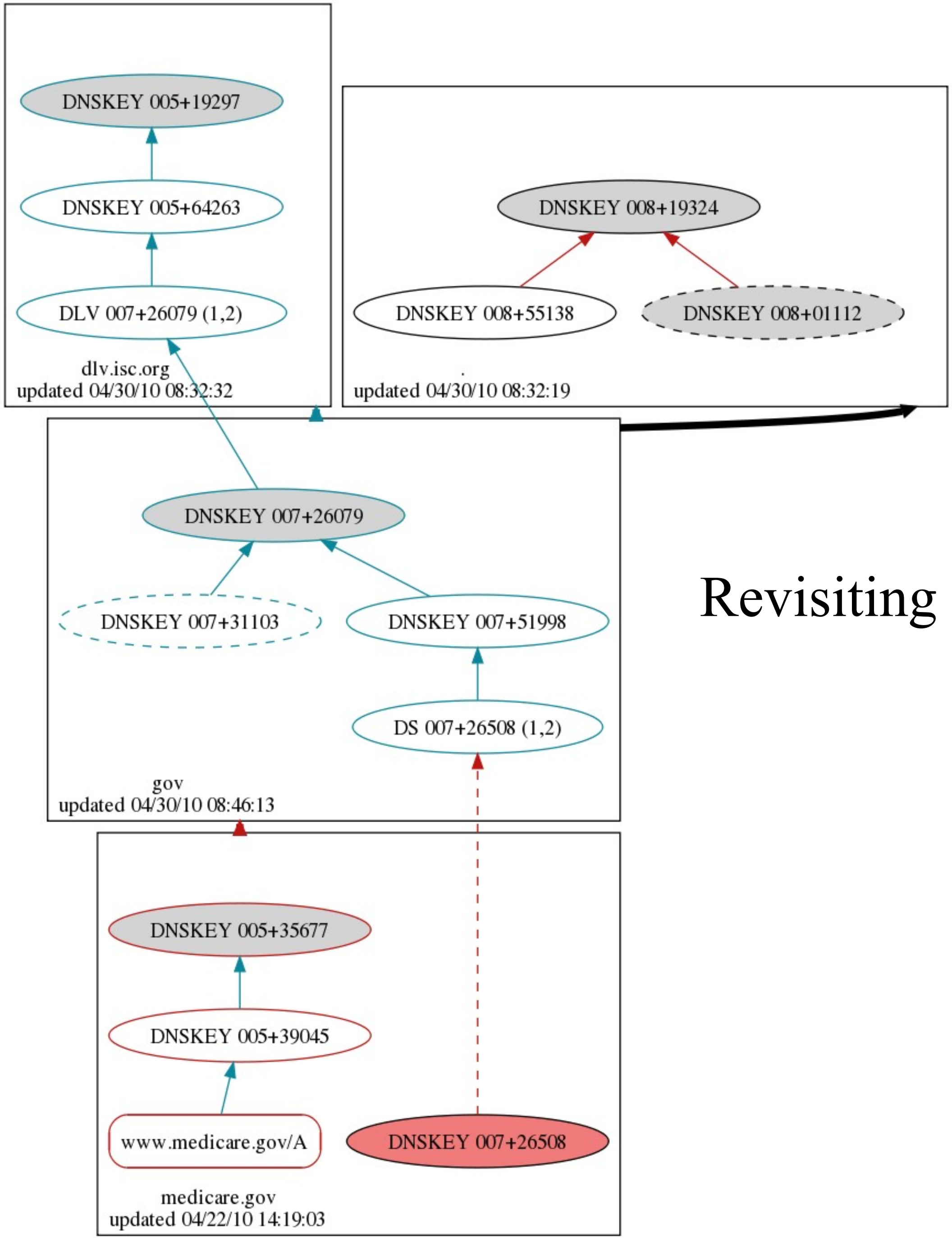
Alias dependency



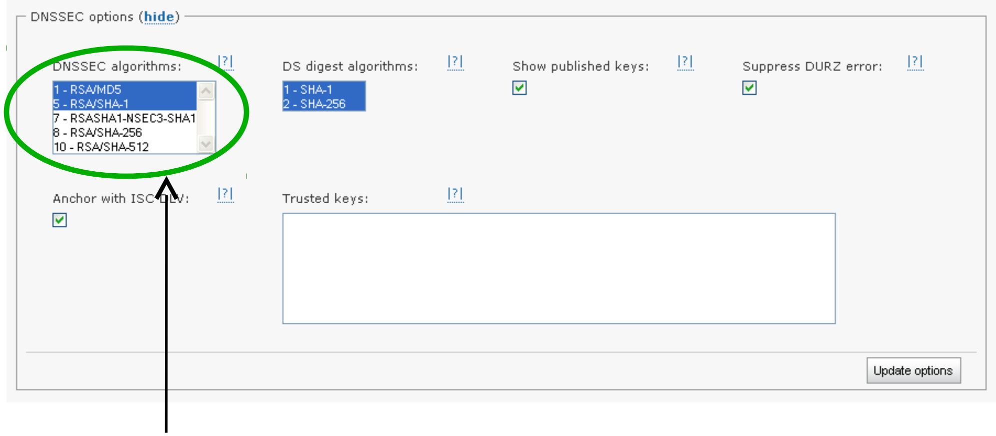
# The Bottom Line



- **Is there a chain of trust to a name or DNSKEY?**
- **Have the existence of DS RRs for insecure delegations been effectively repudiated (NSEC and NSEC3)?**



# Revisiting medicare.gov



DNSSEC options (hide)

DNSSEC algorithms: [?]
1 - RSA/MD5
5 - RSA/SHA-1
7 - RSASHA1-NSEC3-SHA1
8 - RSA/SHA-256
10 - RSA/SHA-512

DS digest algorithms: [?]
1 - SHA-1
2 - SHA-256

Show published keys: [?]
☑

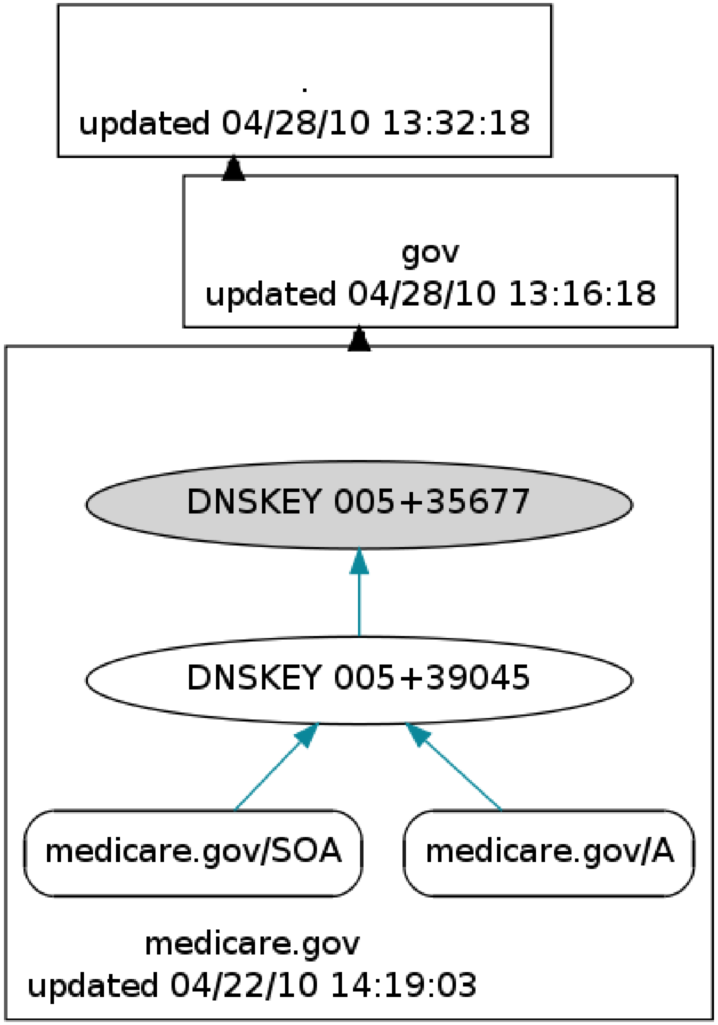
Suppress DURZ error: [?]
☑

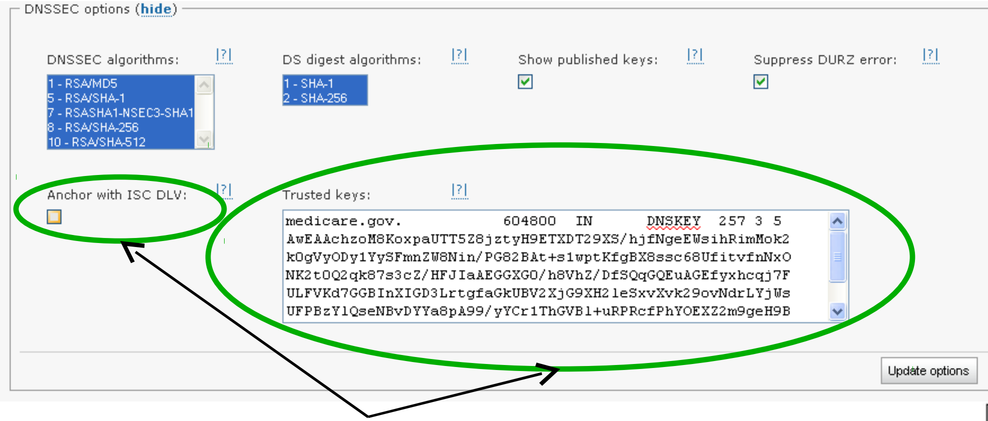
Anchor with ISC DLV: [?]
☑

Trusted keys: [?]

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

**medicare.gov now "insecure" instead of "bogus"**





DNSSEC options (hide)

DNSSEC algorithms: |?|

- 1 - RSA/MD5
- 5 - RSA/SHA-1
- 7 - RSASHA1-NSEC3-SHA1
- 8 - RSA/SHA-256
- 10 - RSA/SHA-512

DS digest algorithms: |?|

- 1 - SHA-1
- 2 - SHA-256

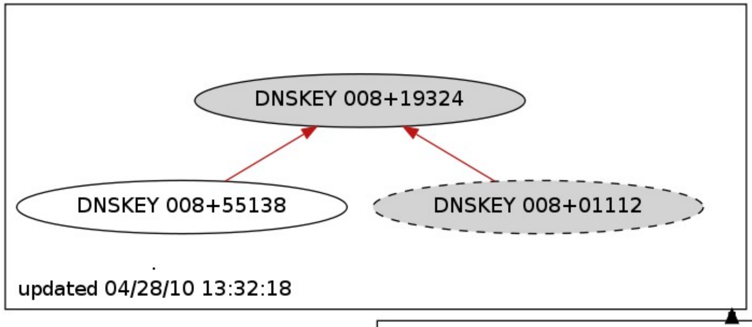
Show published keys: |?| ☑

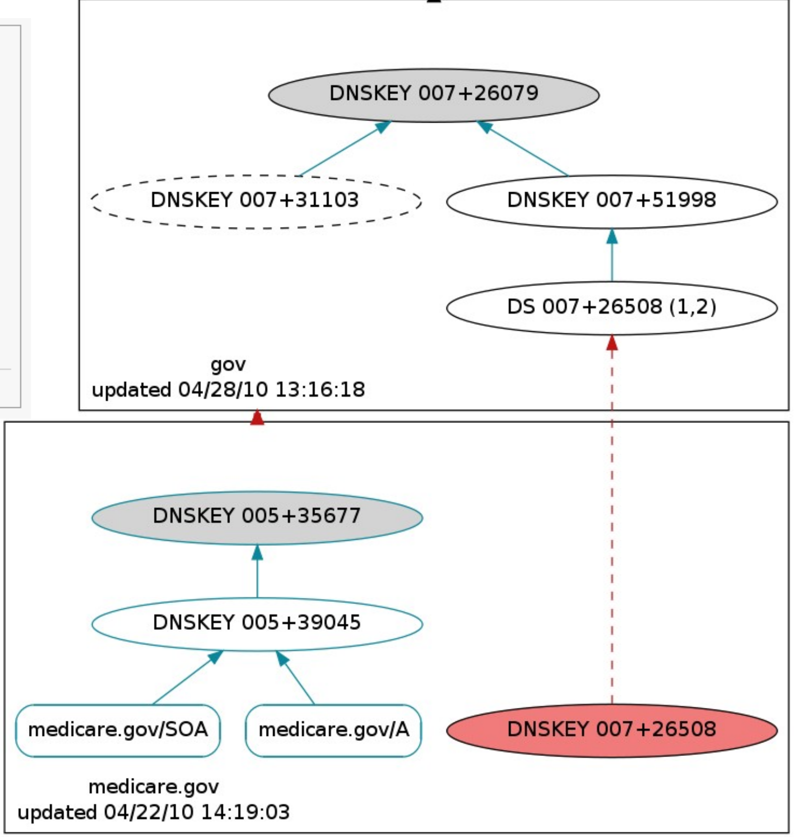
Suppress DURZ error: |?| ☑

Anchor with ISC DLV: |?| □

Trusted keys: |?|

```
medicare.gov.           604800   IN       DNSKEY  257 3 5
AwEAAchzoM8KoxpaUTT5Z8jztyH9ETXDT29XS/hjfNgeEWsihRimMok2
kOgVyODy1YySFmnZW8Nin/PG82BAt+s1wptKfgBX8ssc68UfitvfnNxO
NK2tOQ2qk87s3cZ/HFJIaAEGGXGO/h8VhZ/DfSQqGQEuAGEfyxhcqj7F
ULFVKd7GGBInXIGD3LrtgfaGkUBV2XjG9XH2leSxvXvk29ovNdrLYjWs
UFPBzYlQseNBvDYYa8pA99/yYCr1ThGVBl+uRPRcfPhYOEXZ2m9geH9B
```

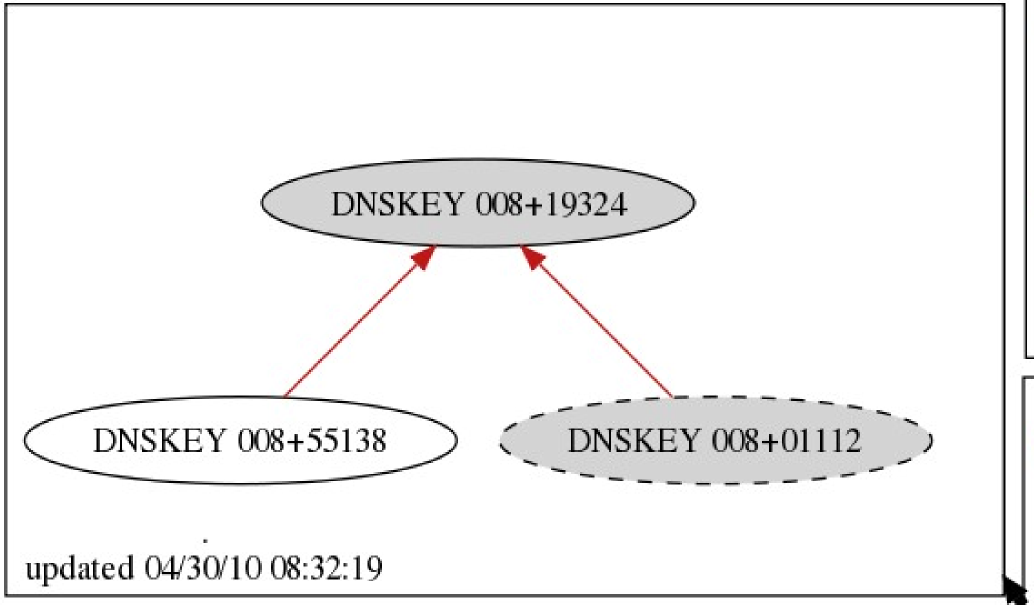


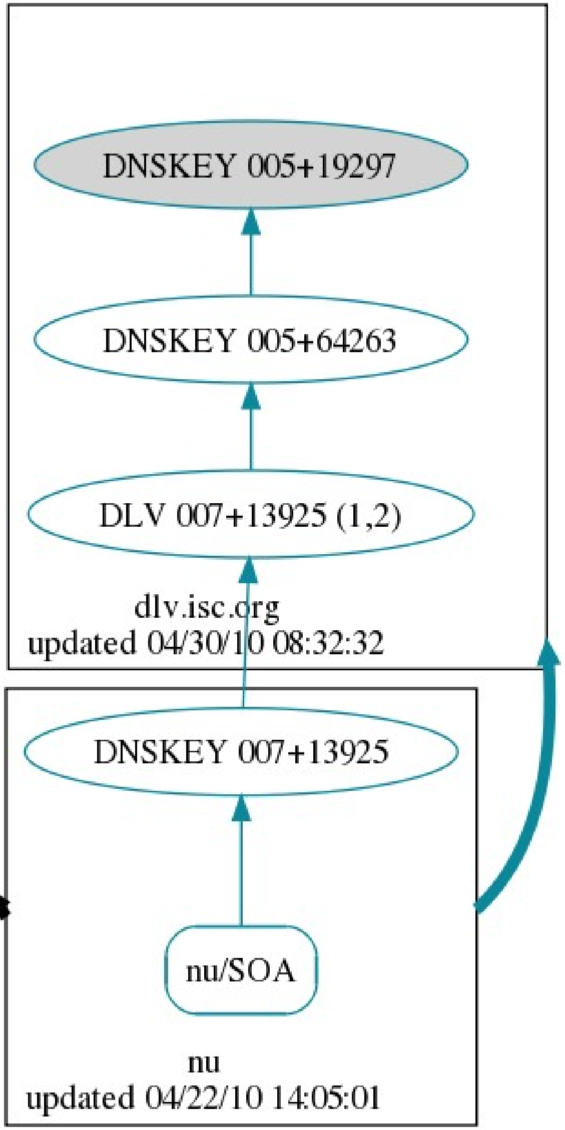


**Configurable trust anchors and DLV support**

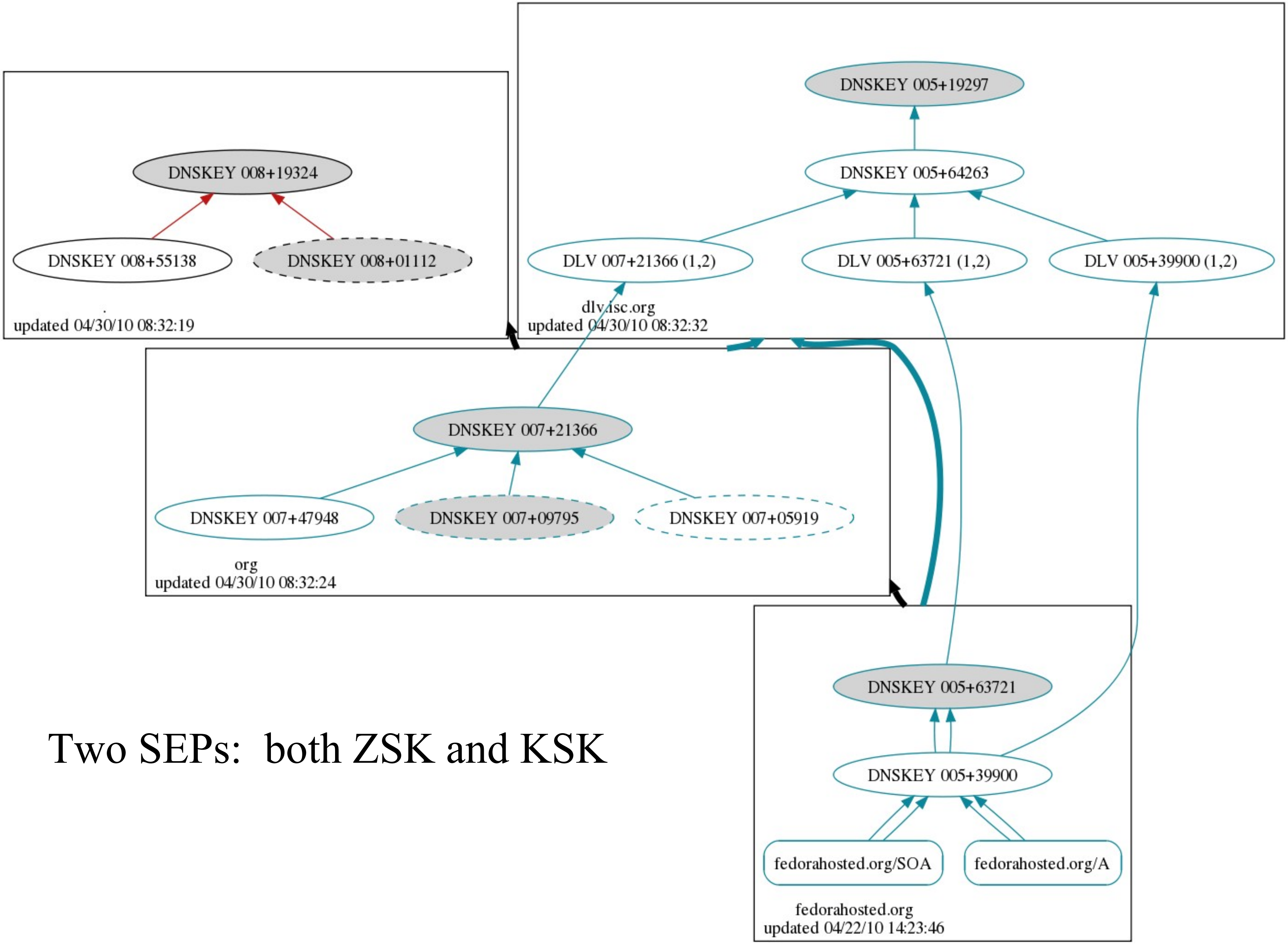
**medicare.gov now “secure” instead of “bogus”**

-

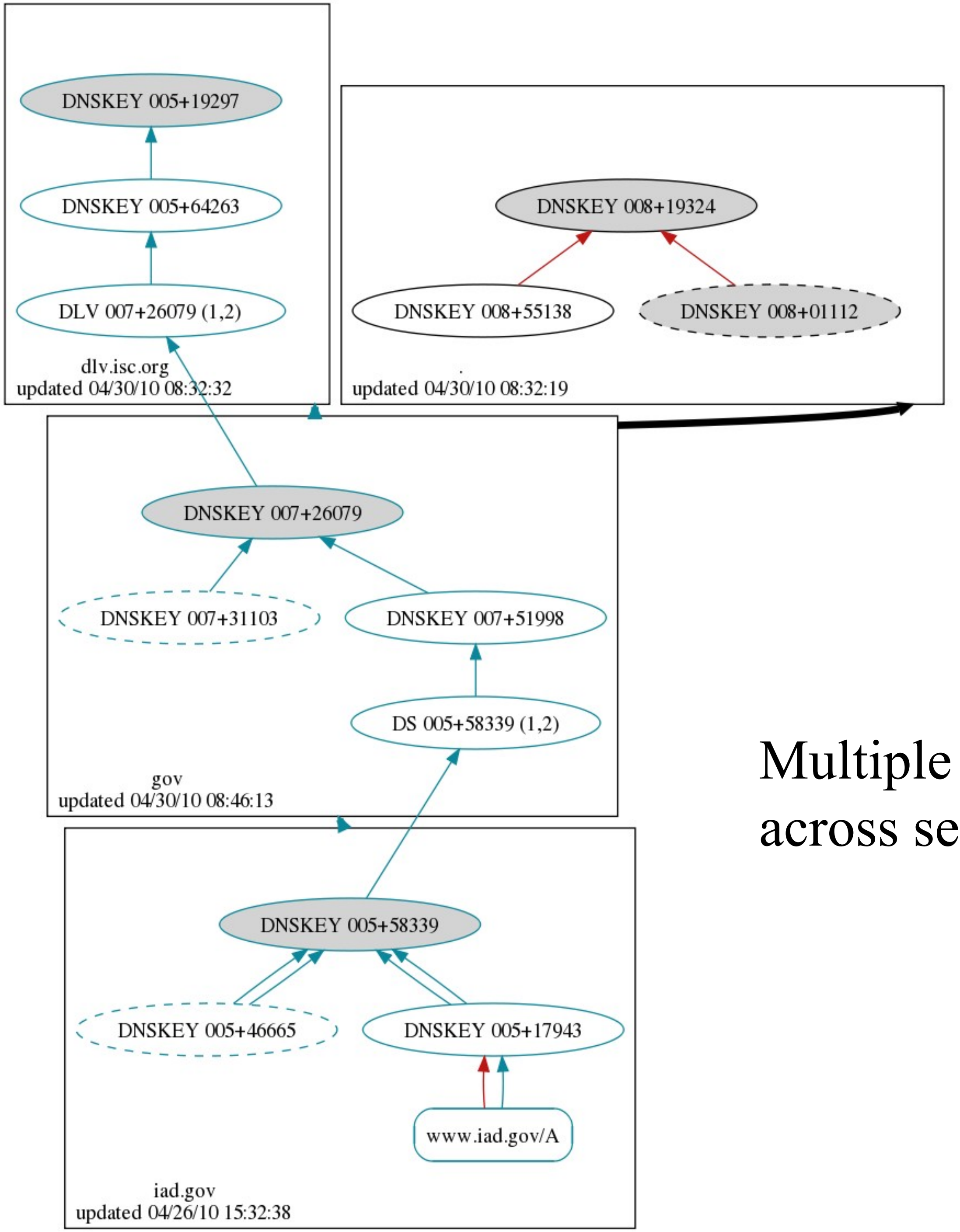




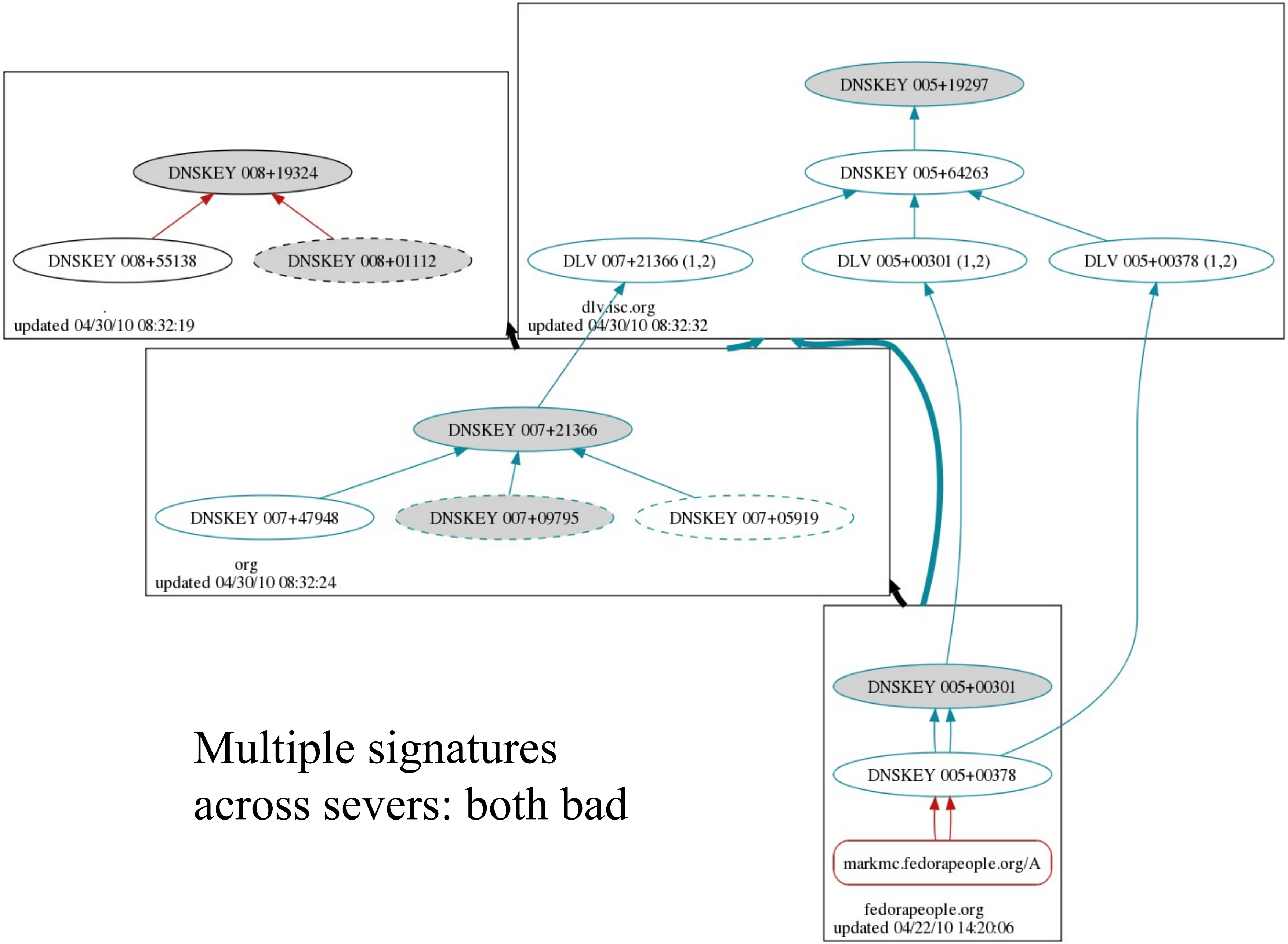
Single DNSKEY: ZSK, KSK, and SEP



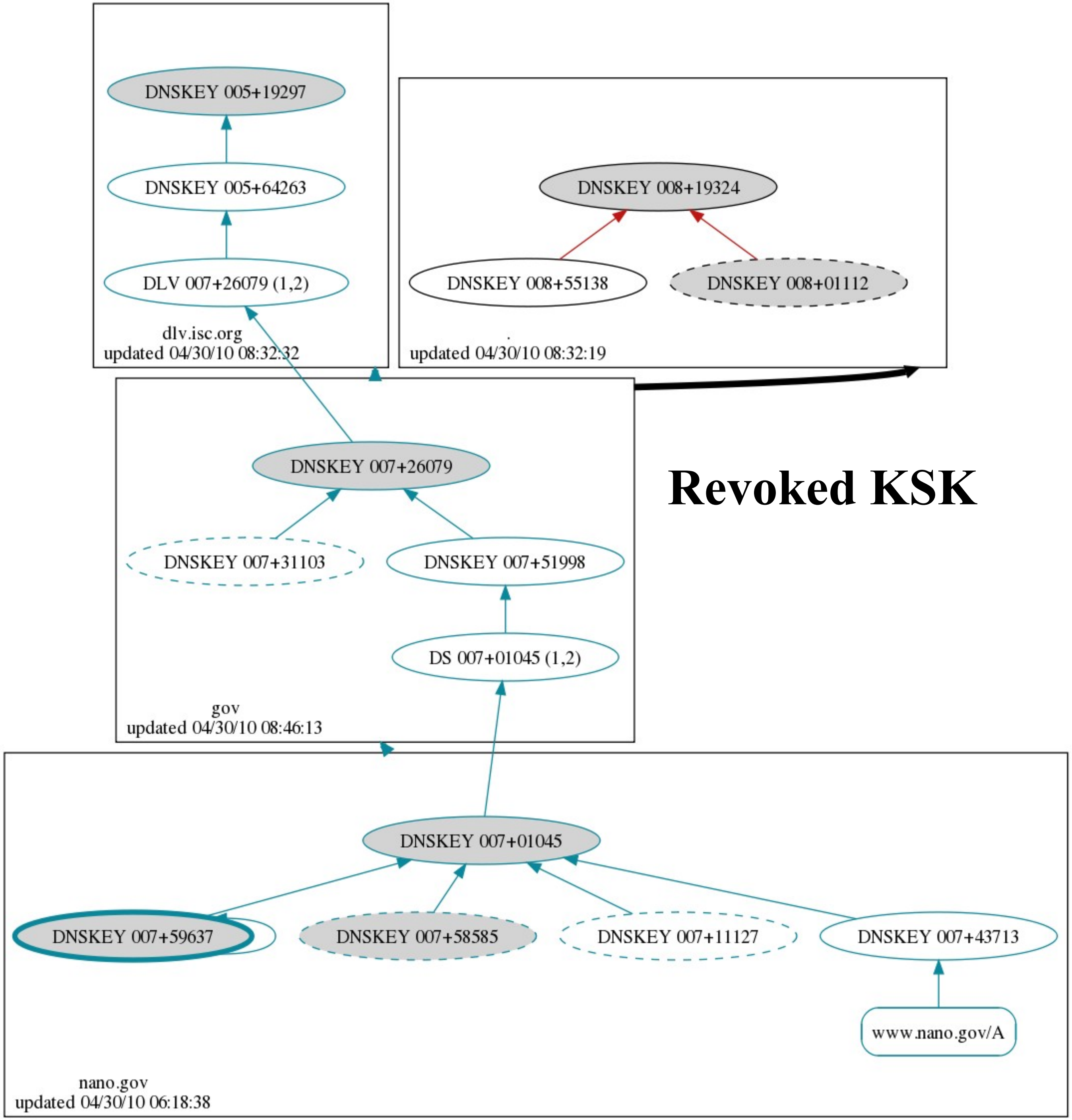
Two SEPs:  both ZSK and KSK



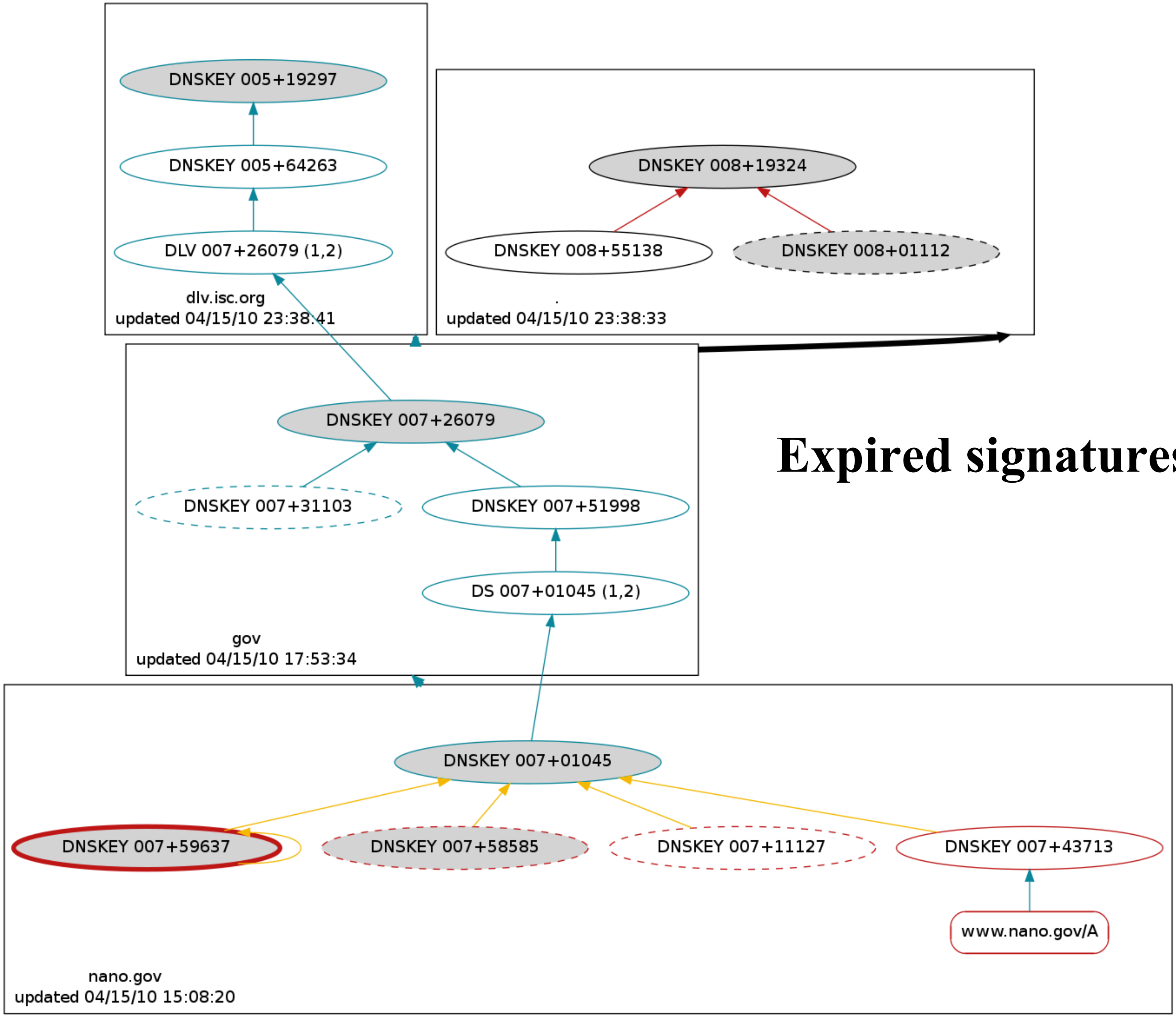
Multiple signatures across severs: one bad



Multiple signatures across severs: both bad


DNSKEY 005+19297
DNSKEY 005+64263
DLV 007+26079 (1,2)
dlv.isc.org
updated 04/30/10 08:32:32
DNSKEY 008+19324
DNSKEY 008+55138
DNSKEY 008+01112
.
updated 04/30/10 08:32:19
DNSKEY 007+26079
DNSKEY 007+31103
DNSKEY 007+51998
DS 007+01045 (1,2)
gov
updated 04/30/10 08:46:13
DNSKEY 007+01045
DNSKEY 007+59637
DNSKEY 007+58585
DNSKEY 007+11127
DNSKEY 007+43713
www.nano.gov/A
nano.gov
updated 04/30/10 06:18:38

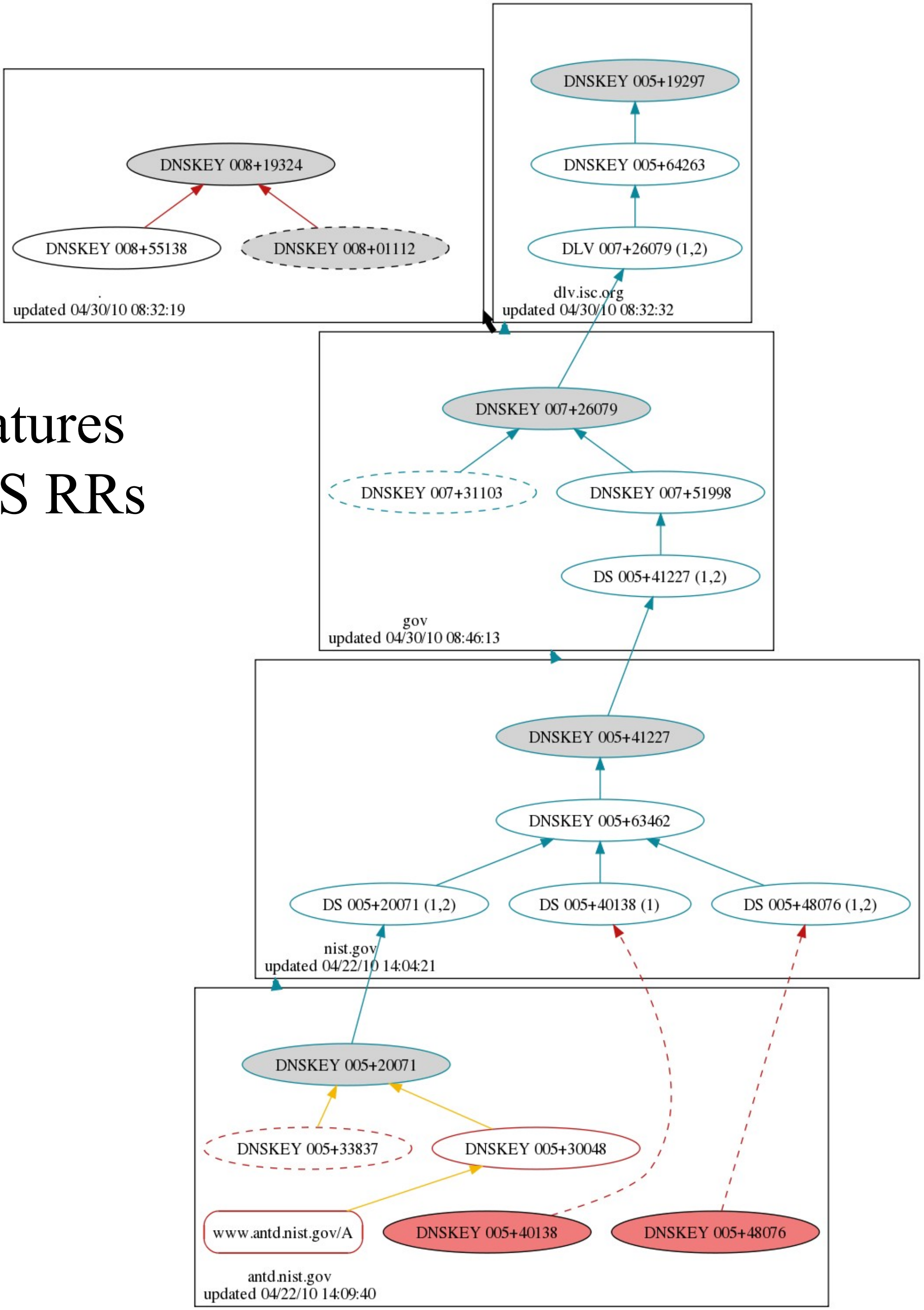
# Revoked KSK



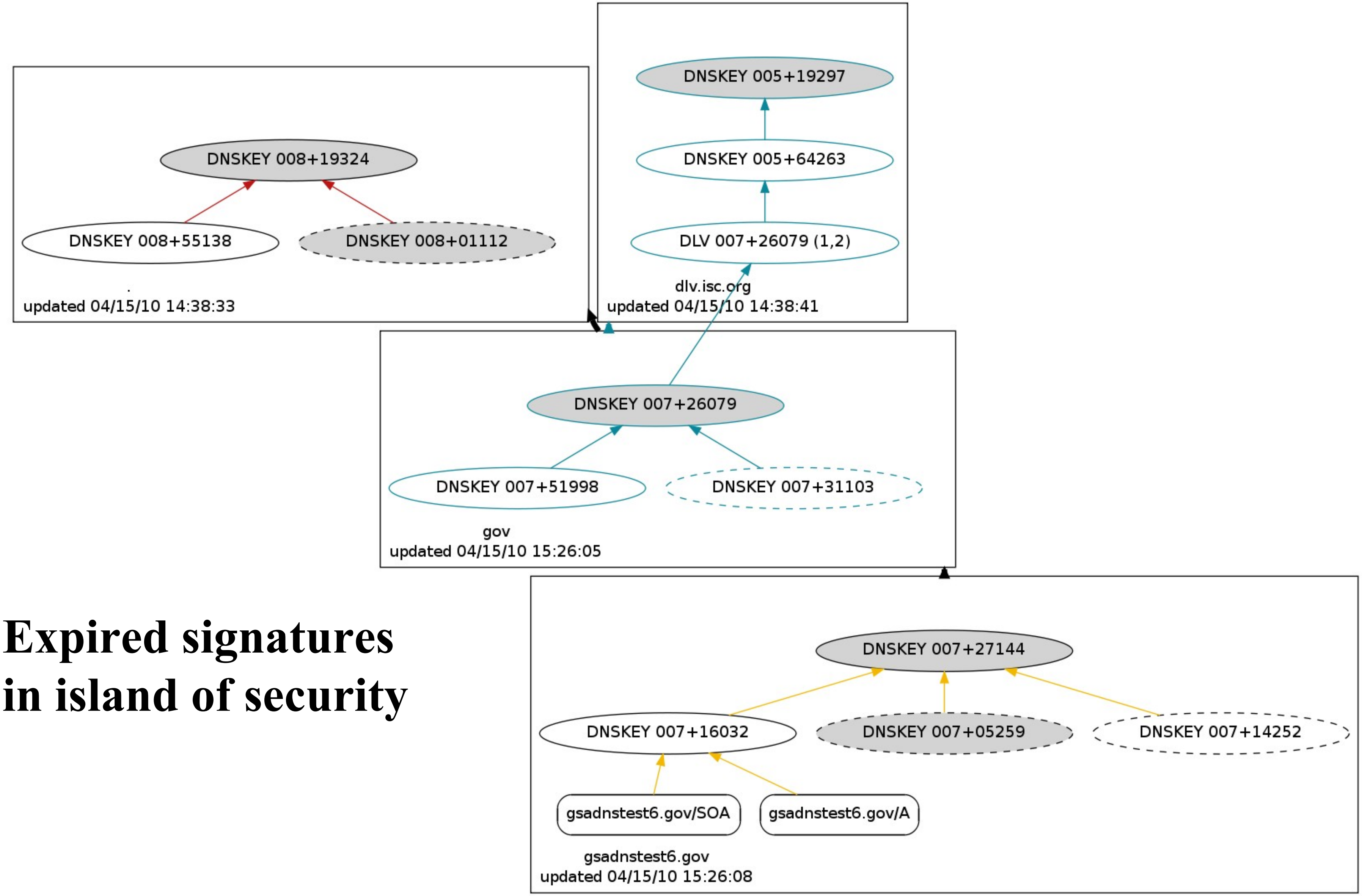
# Expired signatures

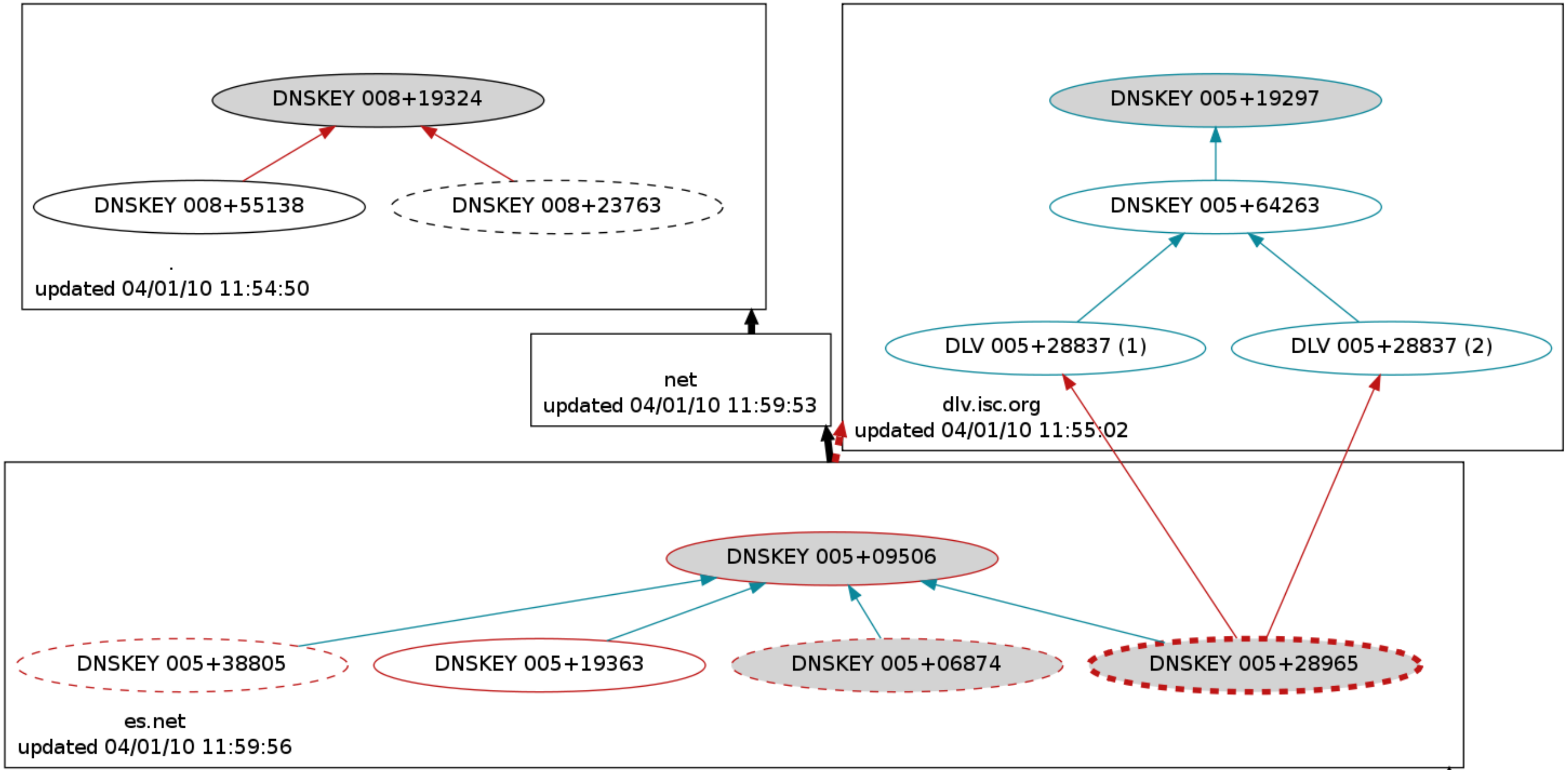
Sandia National Laboratories

Expired signatures
extraneous DS RRs

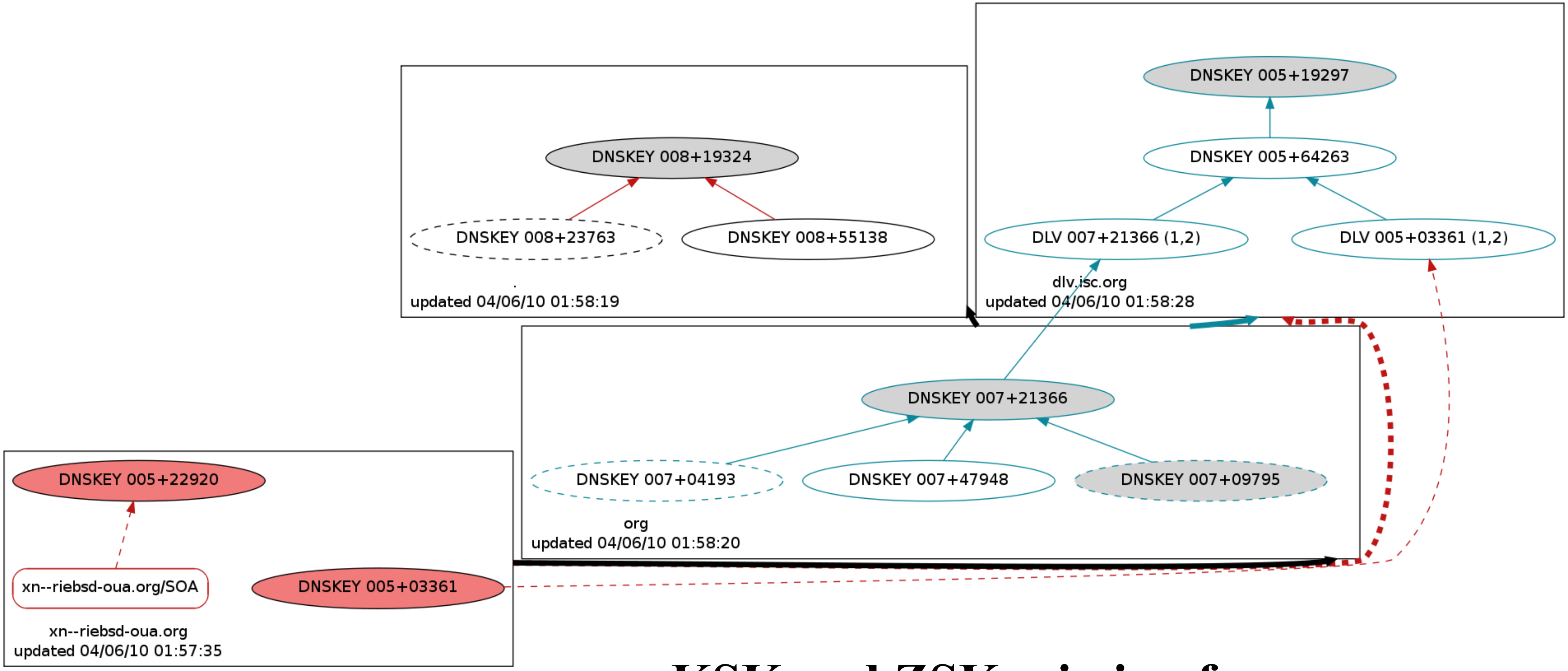


# Expired signatures in island of security

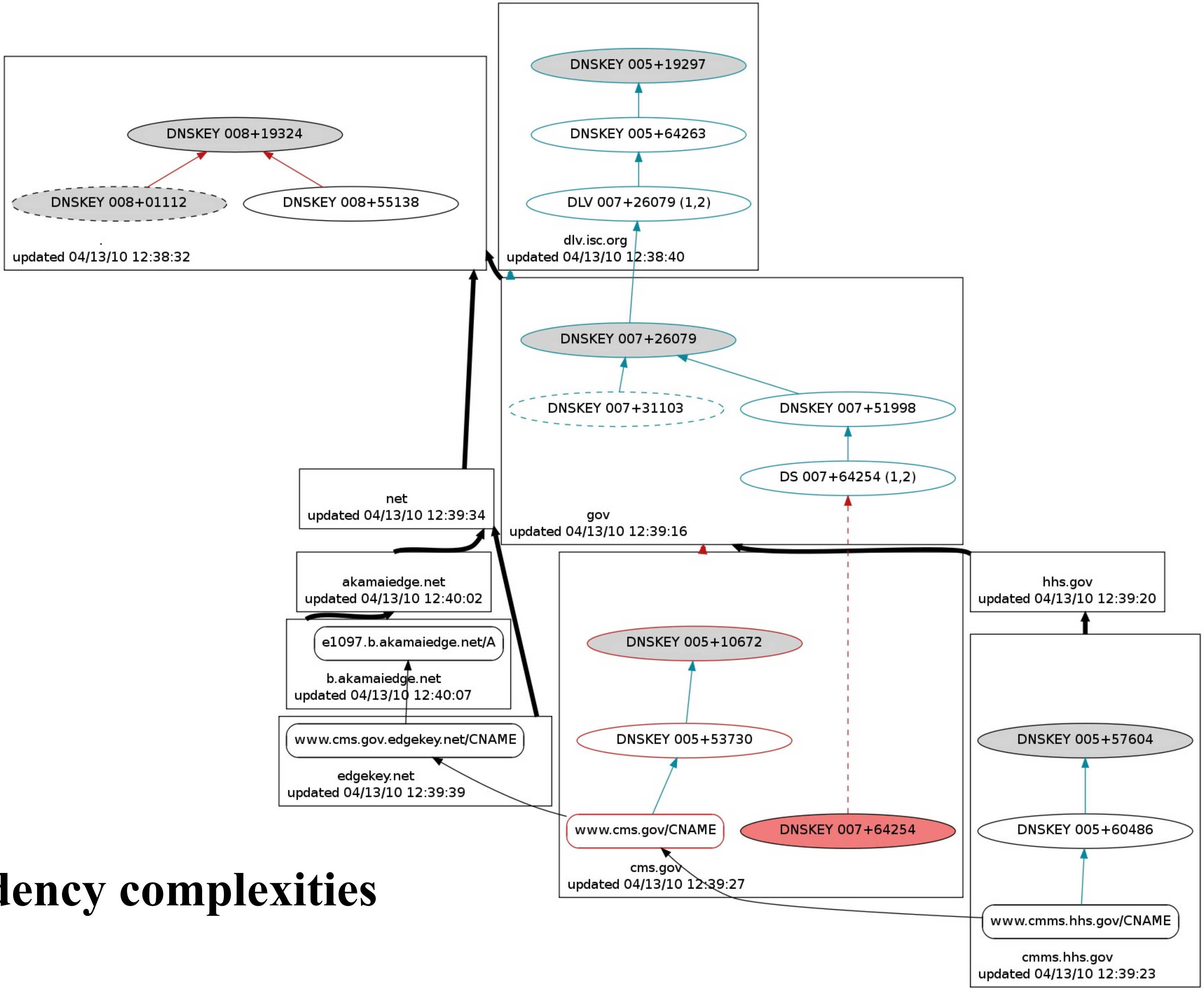




# KSK missing (bad rollover)
# Invalid DNSKEY revocation



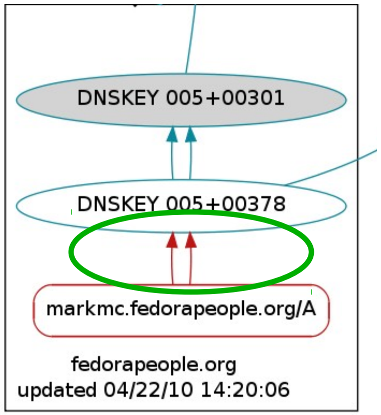
## KSK and ZSK missing from zone (signatures still exist)

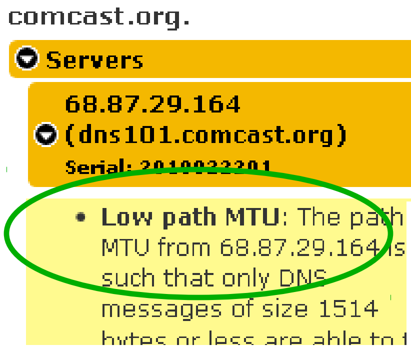


# Dependency complexities

# Server status

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



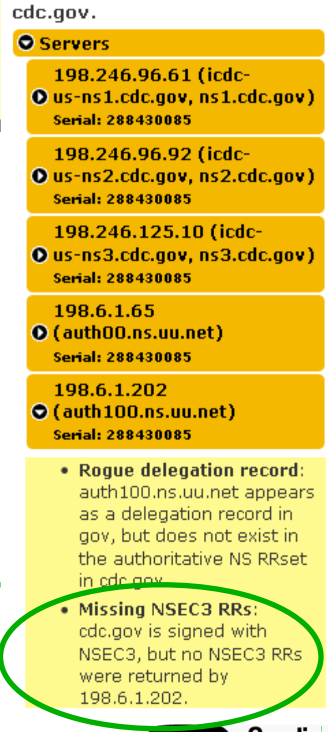


comcast.org.

Servers

68.87.29.164 (dns101.comcast.org)
Serial: 2010022201

- **Low path MTU**: The path MTU from 68.87.29.164 is such that only DNS messages of size 1514 bytes or less are able to t



cdc.gov.

Servers

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

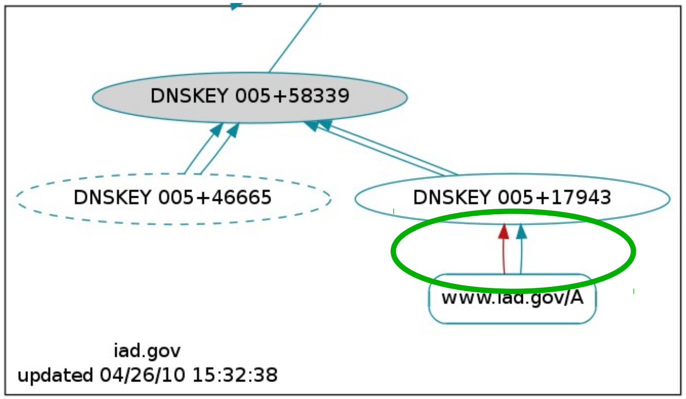
198.246.96.92 (icdc-us-ns2.cdc.gov, ns2.cdc.gov)
Serial: 288430085

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

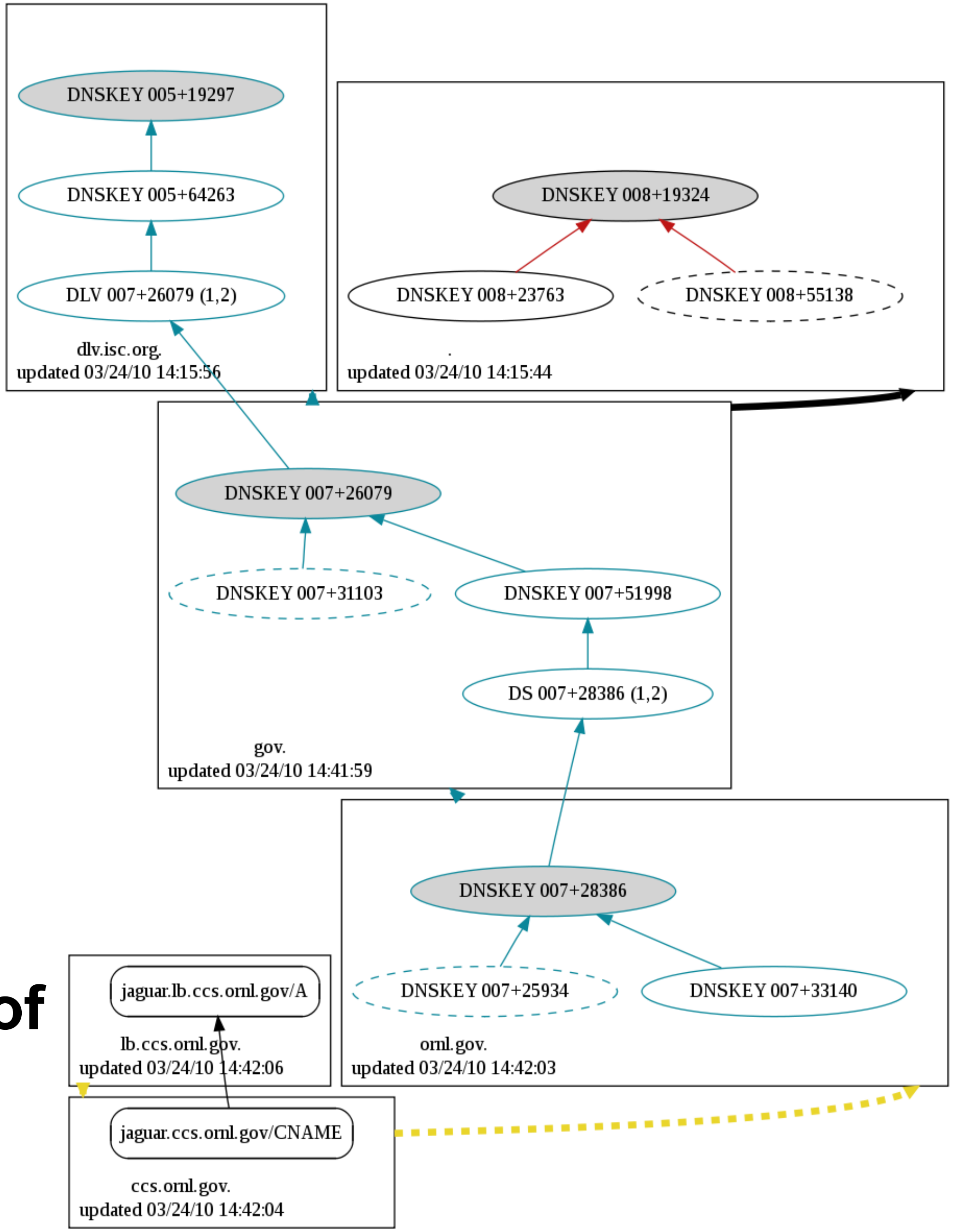
- Better visualization of server dependencies (i.e., to demonstrate subset of servers misconfigured)
- Visual history of zone for reference, post-mortem analysis
- Regular polling, monitoring/alert services

# Questions?

ctdecci@sandia.gov

http://dnsviz.net/

- **Misconfigured delegation: no delegation RRs in parent zone**
- **Impact: Resolver queries server authoritative for both parent child for DS RRs and receives NXDOMAIN, instead of NOERROR (empty answer)**



DNSKEY 005+19297
DNSKEY 005+64263
DLV 007+26079 (1,2)
dlv.isc.org.
updated 03/24/10 14:15:56
DNSKEY 008+19324
DNSKEY 008+23763
DNSKEY 008+55138
.
updated 03/24/10 14:15:44
DNSKEY 007+26079
DNSKEY 007+31103
DNSKEY 007+51998
DS 007+28386 (1,2)
gov.
updated 03/24/10 14:41:59
DNSKEY 007+28386
DNSKEY 007+25934
DNSKEY 007+33140
ornl.gov.
updated 03/24/10 14:42:03
jaguar.lb.ccs.ornl.gov/A
lb.ccs.ornl.gov.
updated 03/24/10 14:42:06
jaguar.ccs.ornl.gov/CNAME
ccs.ornl.gov.
updated 03/24/10 14:42:04