DNSViz: A DNS Visualization Tool

Casey Deccio

Sandia National Laboratories

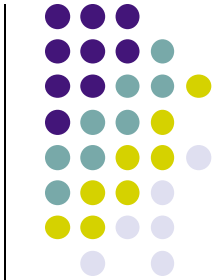
2010 DNS-OARC Workshop (2)

Denver, CO

Oct 14, 2010

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Objectives

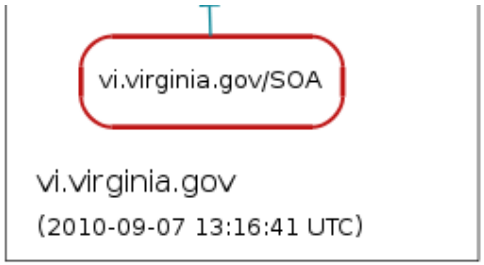


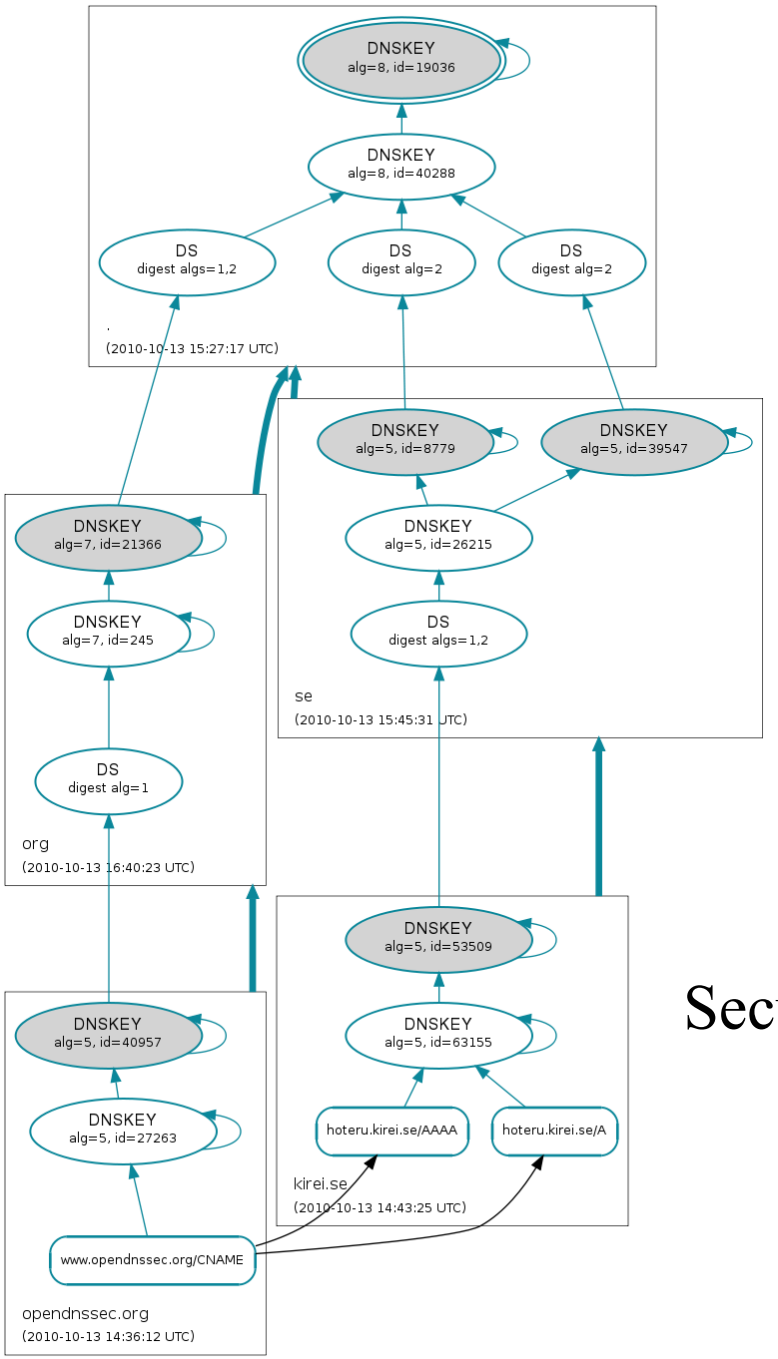
- Help administrators understand DNSSEC
  - Chain of trust
  - Secure/insecure/bogus status
  - Dependencies
- Facilitate DNSSEC troubleshooting
  - Easily identify problems or potential problems related to misconfiguration

Sandia National Laboratories

Insecure

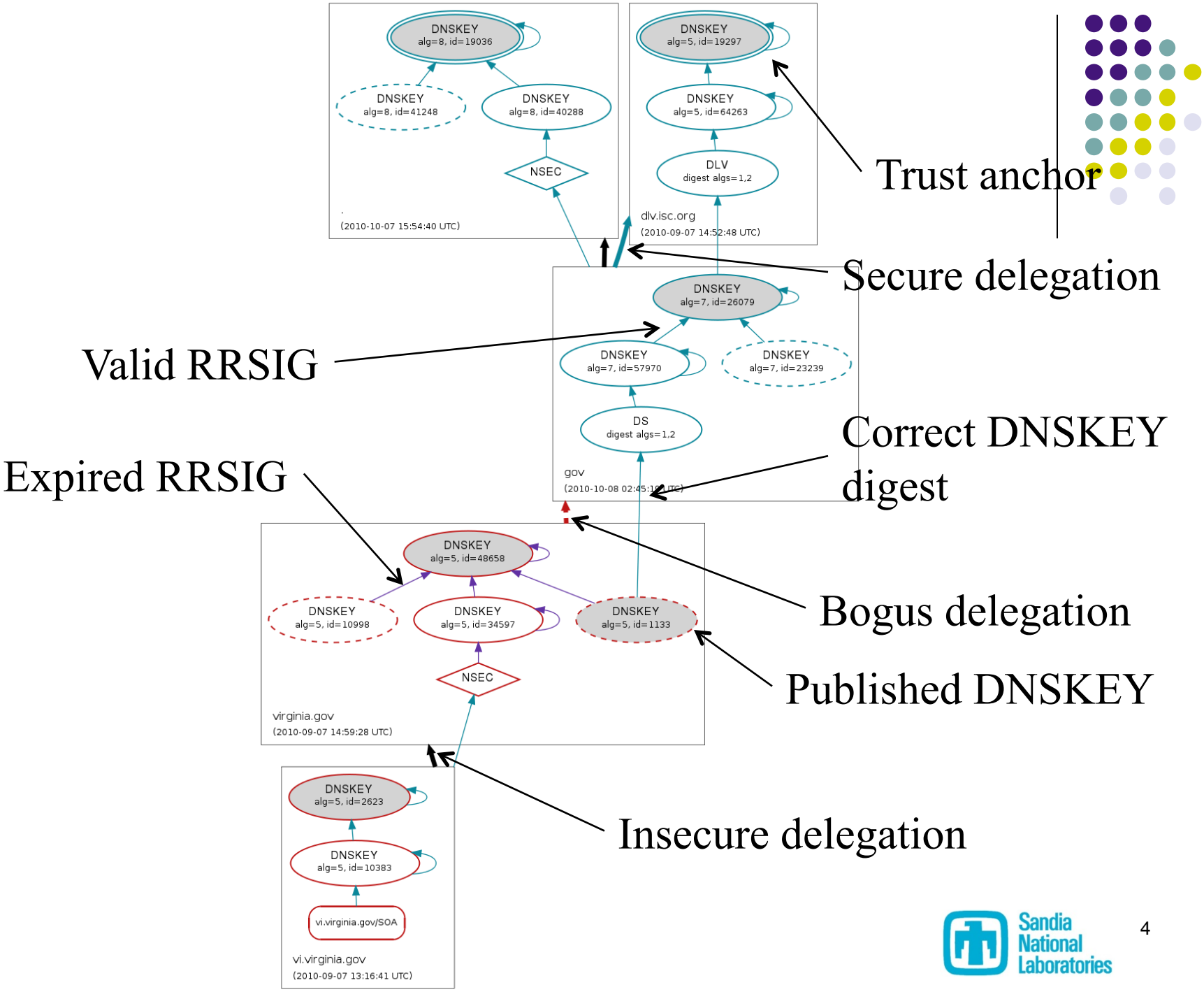
Bogus





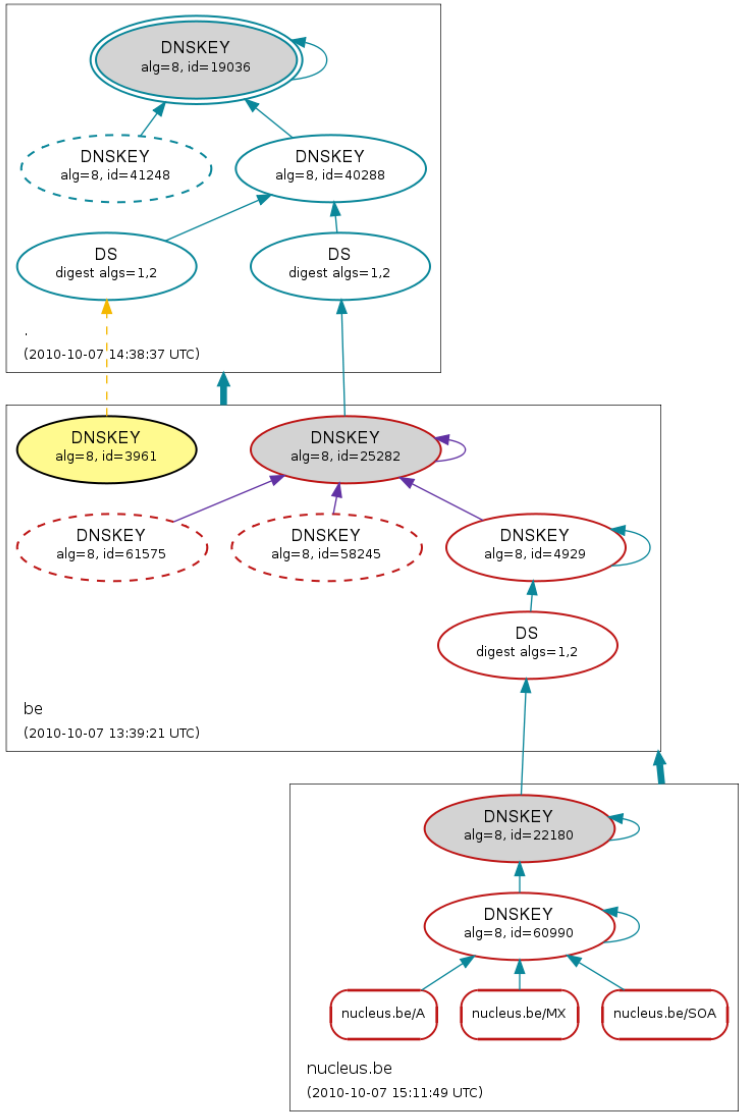
Secure

Sandia National Laboratories


DNSKEY
alg=8, id=19036
DNSKEY
alg=8, id=41248
DNSKEY
alg=8, id=40288
NSEC
.
(2010-10-07 15:54:40 UTC)
DNSKEY
alg=5, id=19297
DNSKEY
alg=5, id=64263
DLV
digest algs=1,2
dlv.isc.org
(2010-09-07 14:52:48 UTC)
Trust anchor
Secure delegation
DNSKEY
alg=7, id=26079
DNSKEY
alg=7, id=57970
DNSKEY
alg=7, id=23239
DS
digest algs=1,2
gov
(2010-10-08 02:45:1
Valid RRSIG
Expired RRSIG
Correct DNSKEY digest
DNSKEY
alg=5, id=48658
DNSKEY
alg=5, id=10998
DNSKEY
alg=5, id=34597
DNSKEY
alg=5, id=1133
NSEC
virginia.gov
(2010-09-07 14:59:28 UTC)
Bogus delegation
Published DNSKEY
DNSKEY
alg=5, id=2623
DNSKEY
alg=5, id=10383
vi.virginia.gov/SOA
vi.virginia.gov
(2010-09-07 13:16:41 UTC)
Insecure delegation

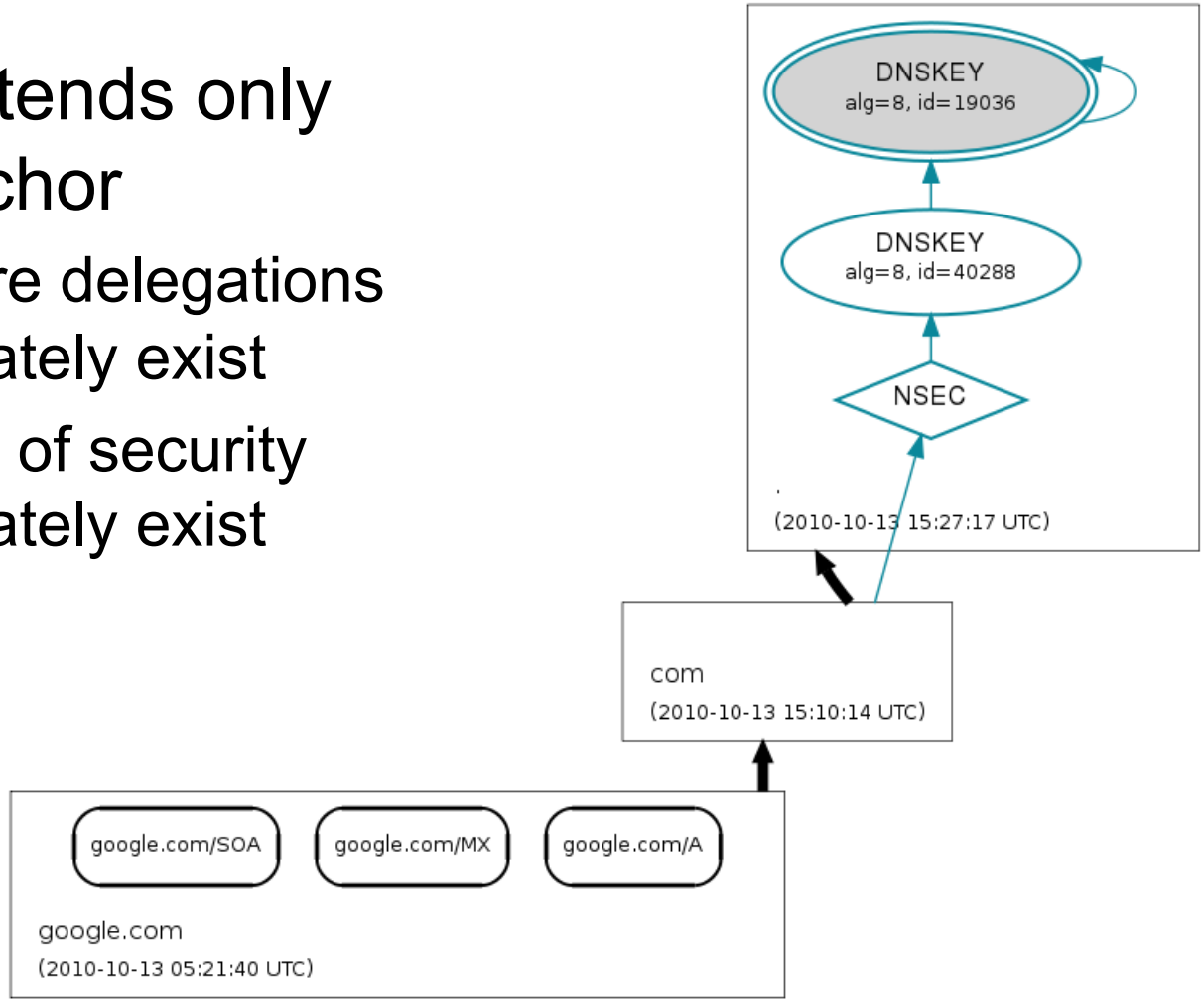
DNSSEC – important points

- A contextual view of a zone configuration is essential
  - Ancestry
  - Dependencies (CNAME, MX, etc.)



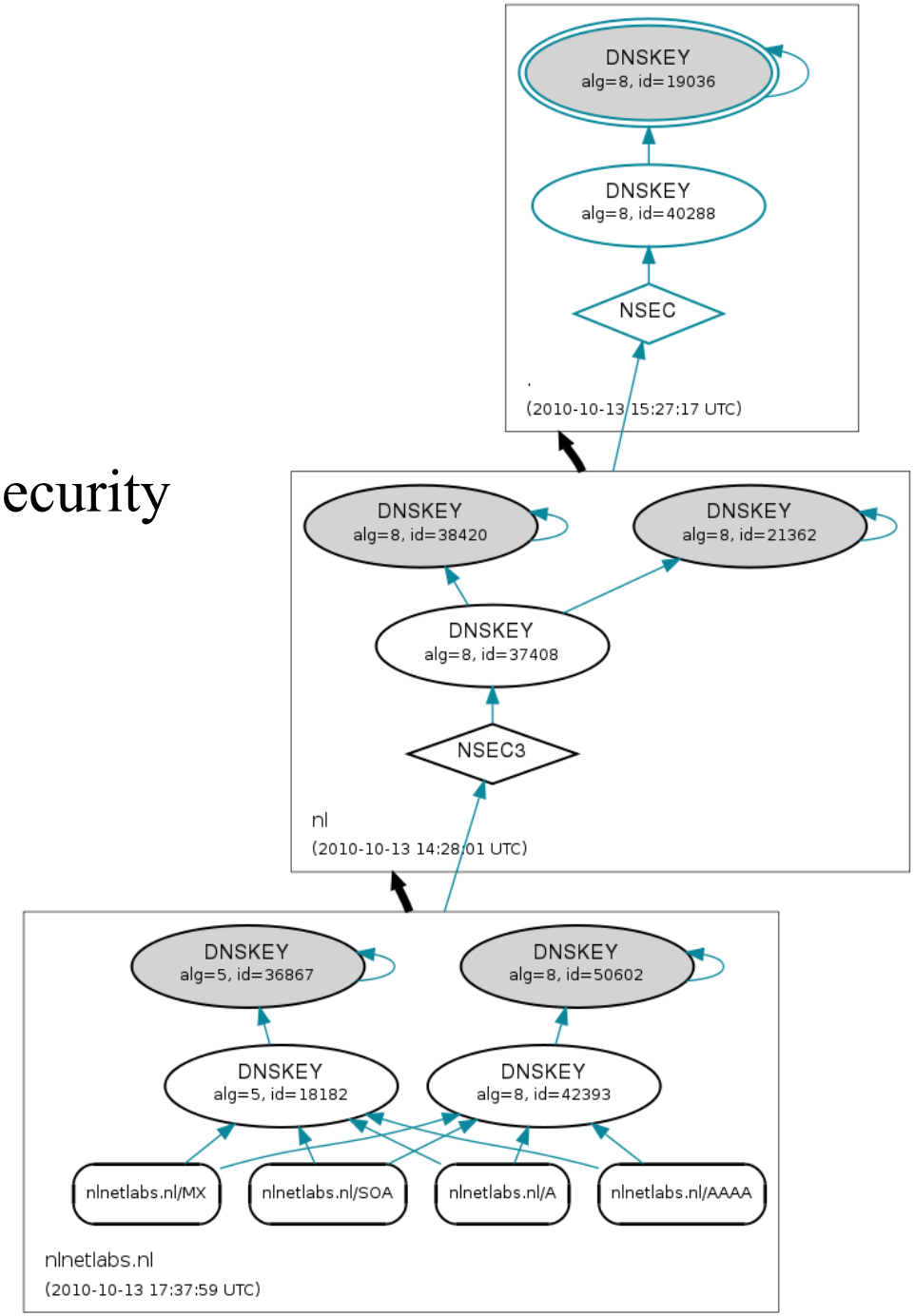
DNSSEC – important points

- Trust extends only from anchor
  - Insecure delegations legitimately exist
  - Islands of security legitimately exist

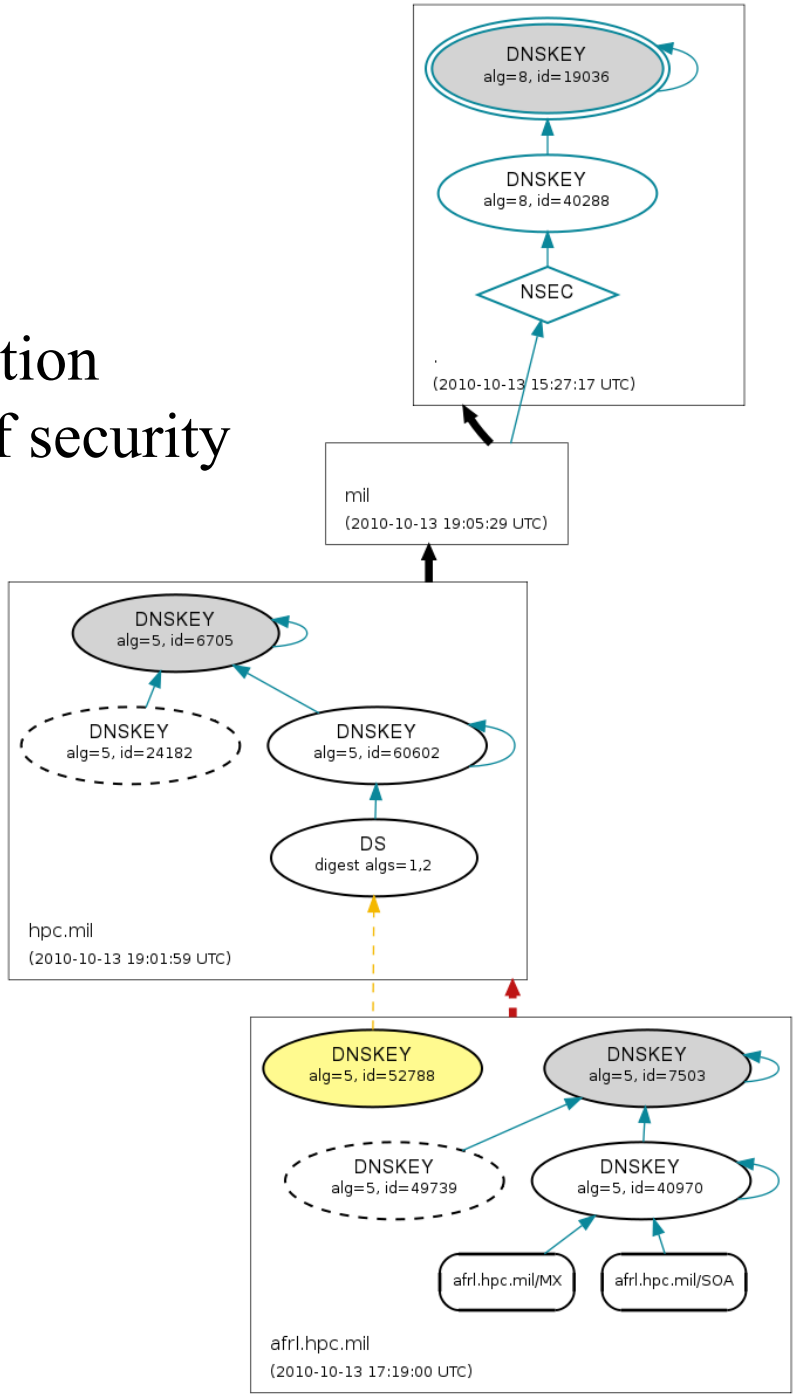


Laboratories

Islands of security

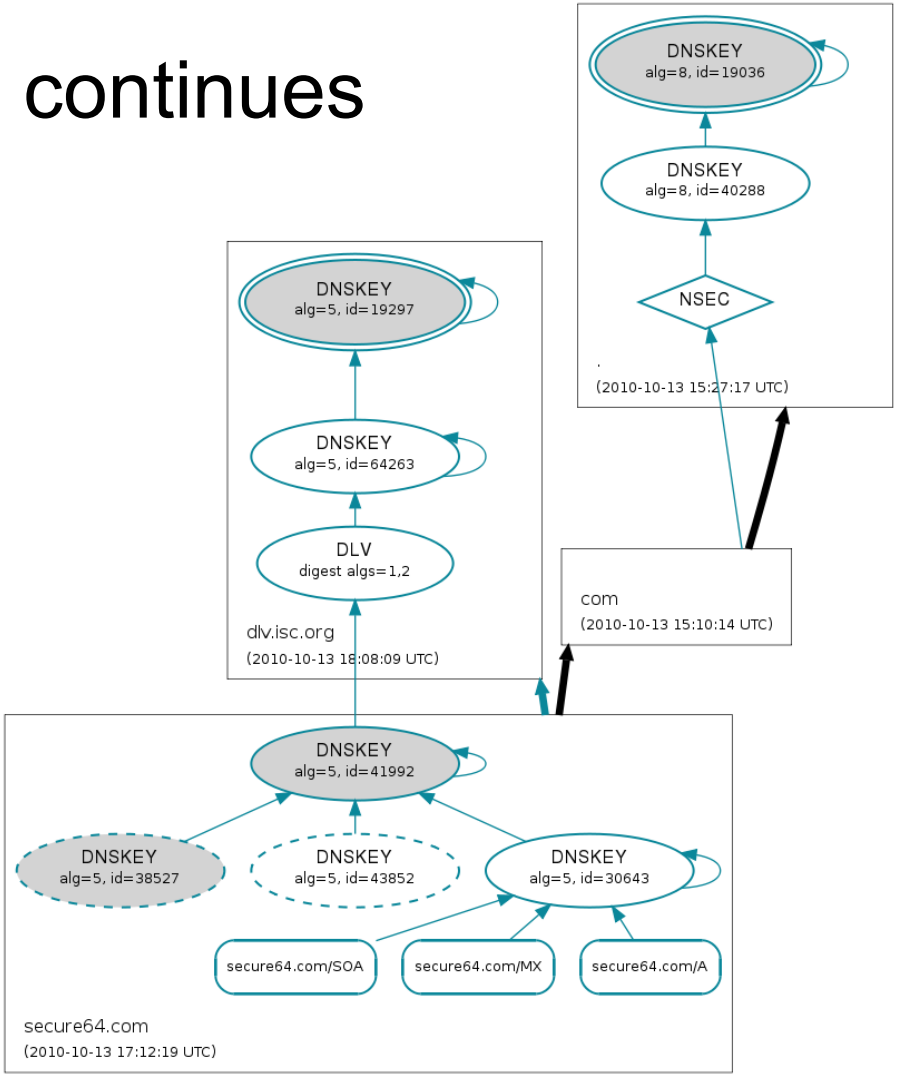


Broken delegation under island of security



DNSSEC – important points

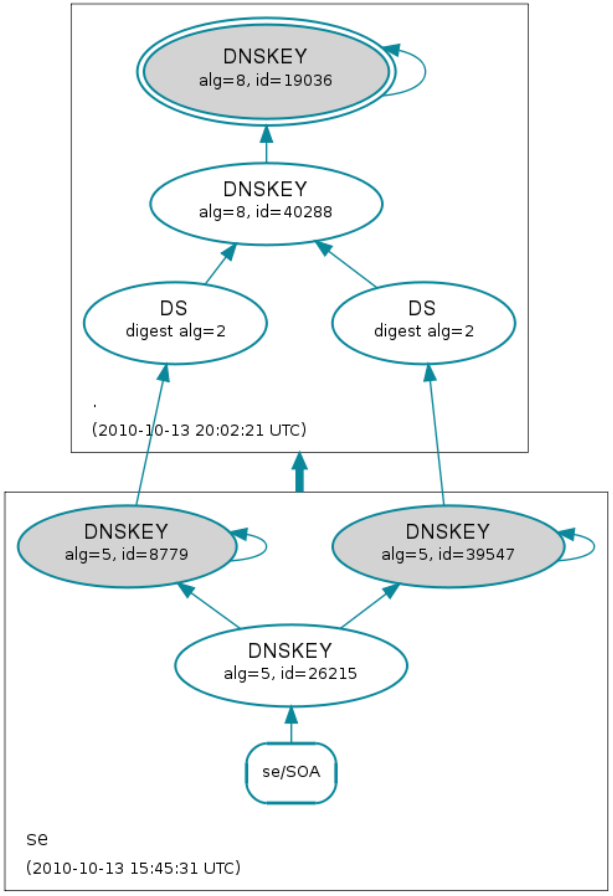
- DLV use continues



Sandia National Laboratories

Visualization challenges

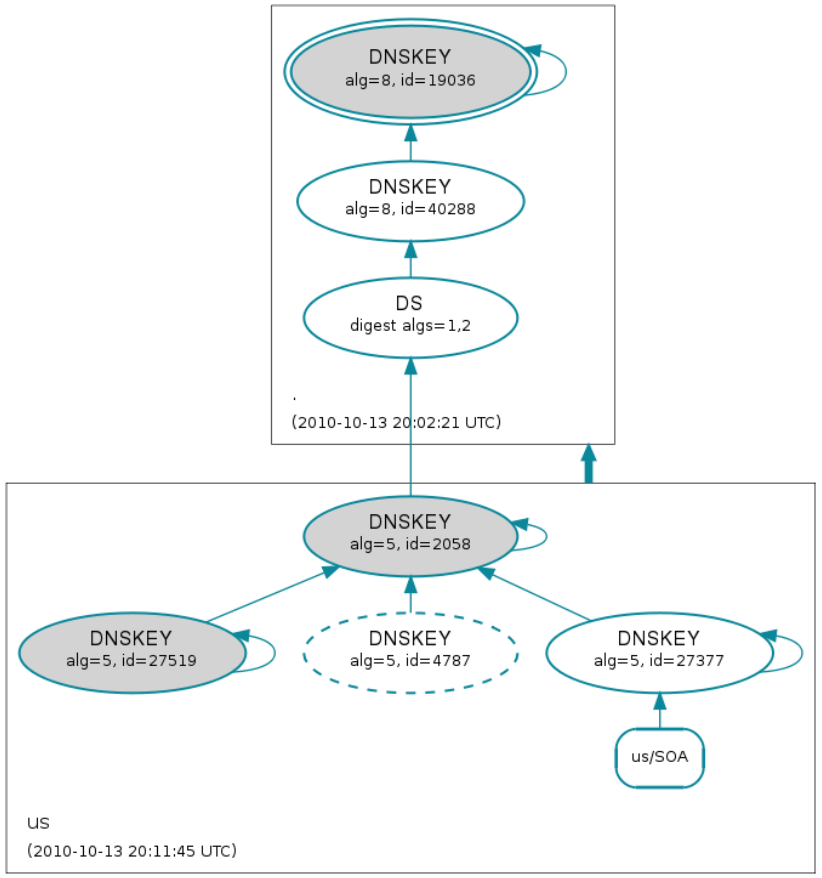
- DNSKEY and DS RRs are useful individually, but are validated as part of an RRset
  - DNSKEY RR is a single node, but considered as part of the entire DNSKEY RRset
  - Set of DS RRs having same name, alg, key tag is a single node



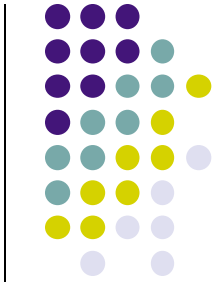
Sandia National Laboratories

Visualization challenges

- KSK/ZSK setup
  - ZSK signs DNSKEY RRset
  - Multiple active KSKs, but only one with DS
  - ZSK also corresponds to DS RR

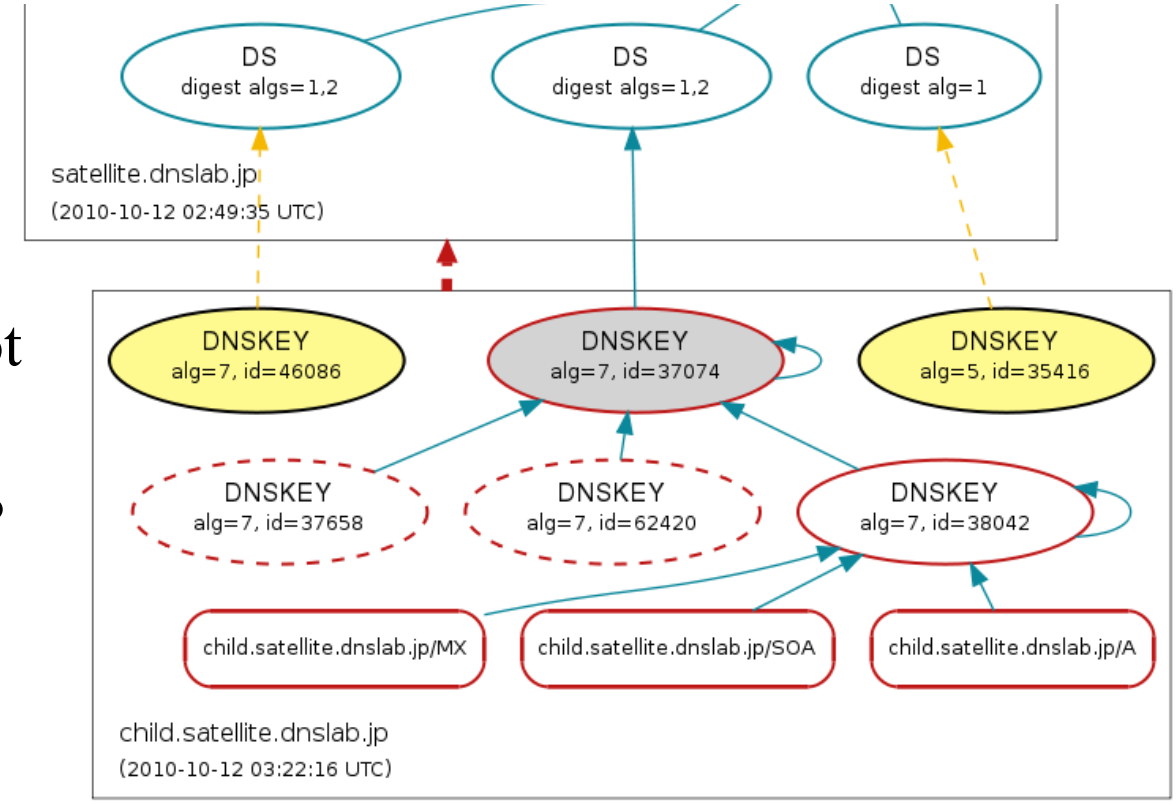


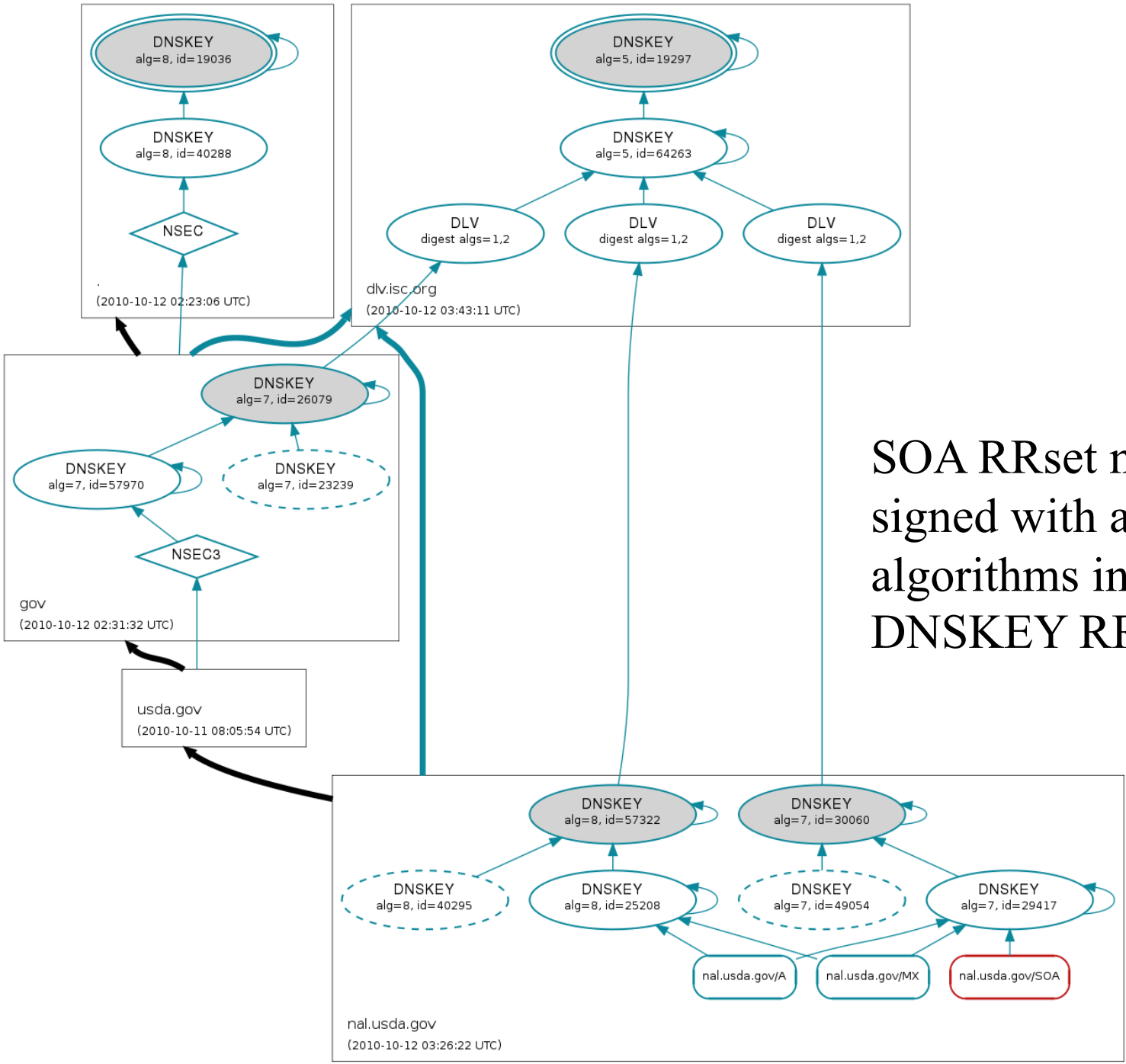
Visualization challenges



- Multiple algorithms in DNSKEY RRset or DS RRset
  - Is there a valid path to the DNSKEY RRset for each algorithm in the DS RRset?
  - Is there a valid path to each RRset for each algorithm in the DNSKEY RRset

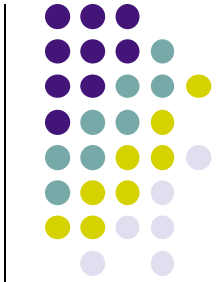
DNSKEY RRset not signed with all algorithms from DS RRset





SOA RRset not signed with all algorithms in DNSKEY RRset

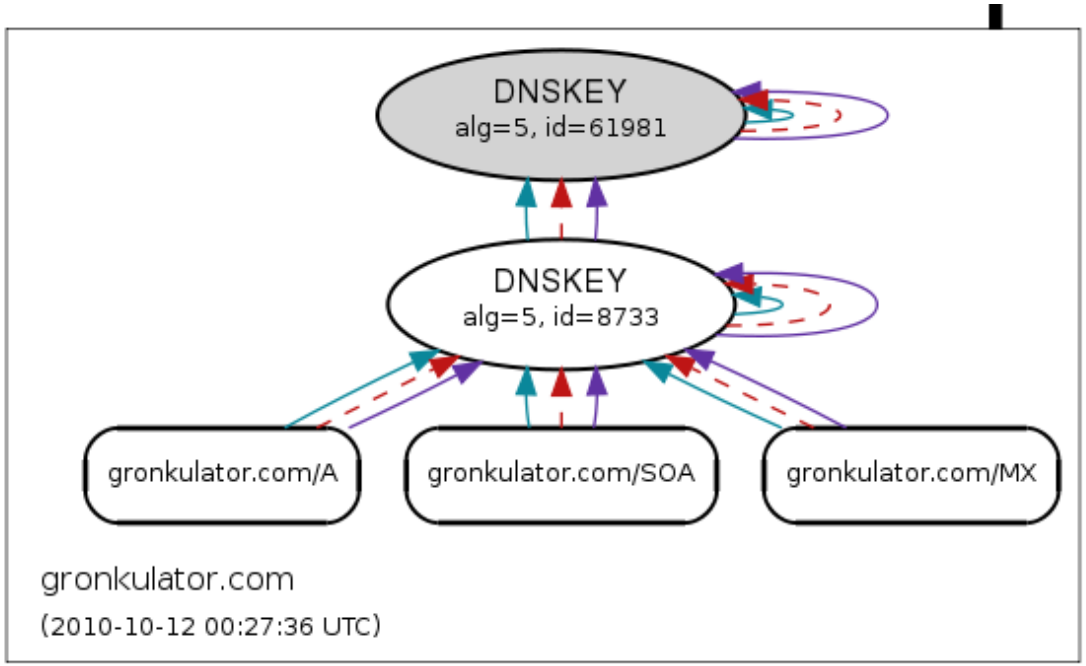
Visualization challenges



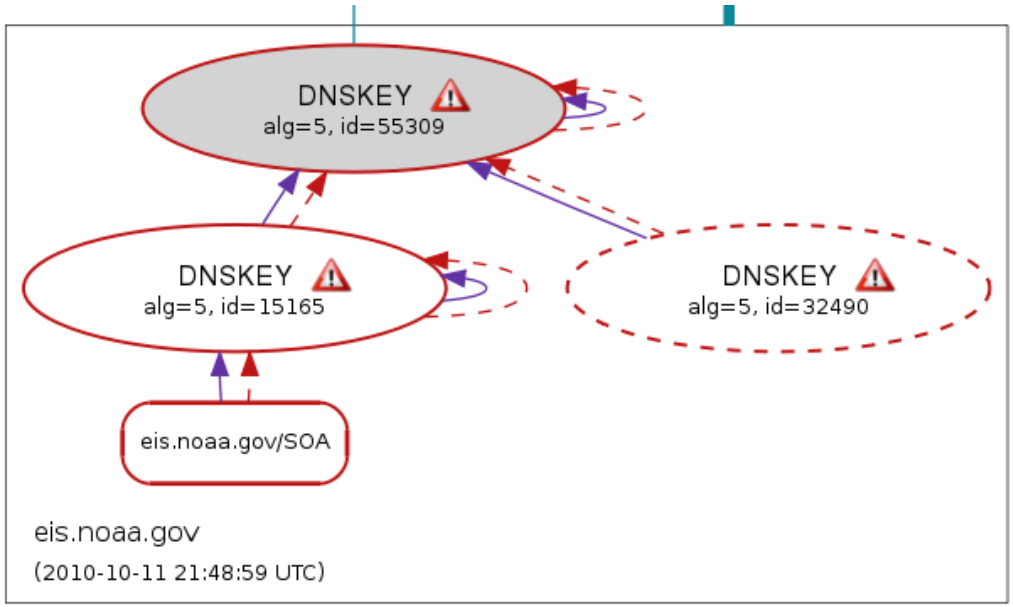
- Server consistency issues:
  - Missing or inconsistent DNSKEYs
  - Not returning RRSIGs
  - Not returning NSEC/NSEC3 RRs

Sandia National Laboratories

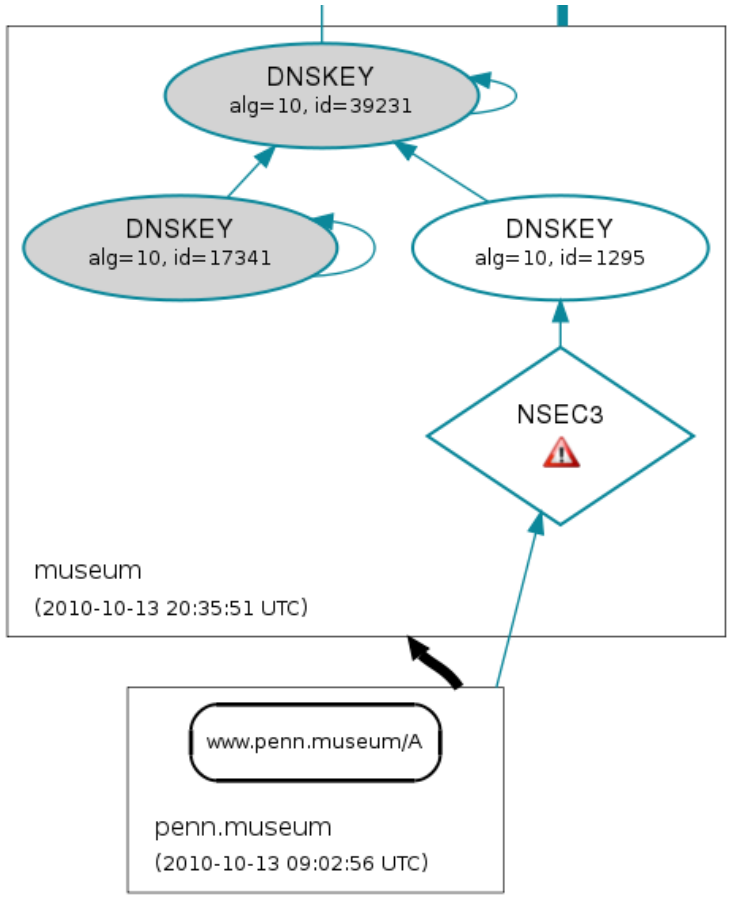
Valid, expired, and missing RRSIGs on different authoritative servers



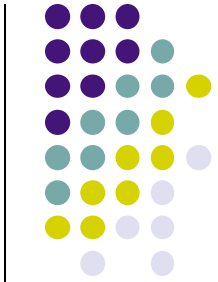
Some authoritative servers not serving DNSKEY RRs nor RRSIGs

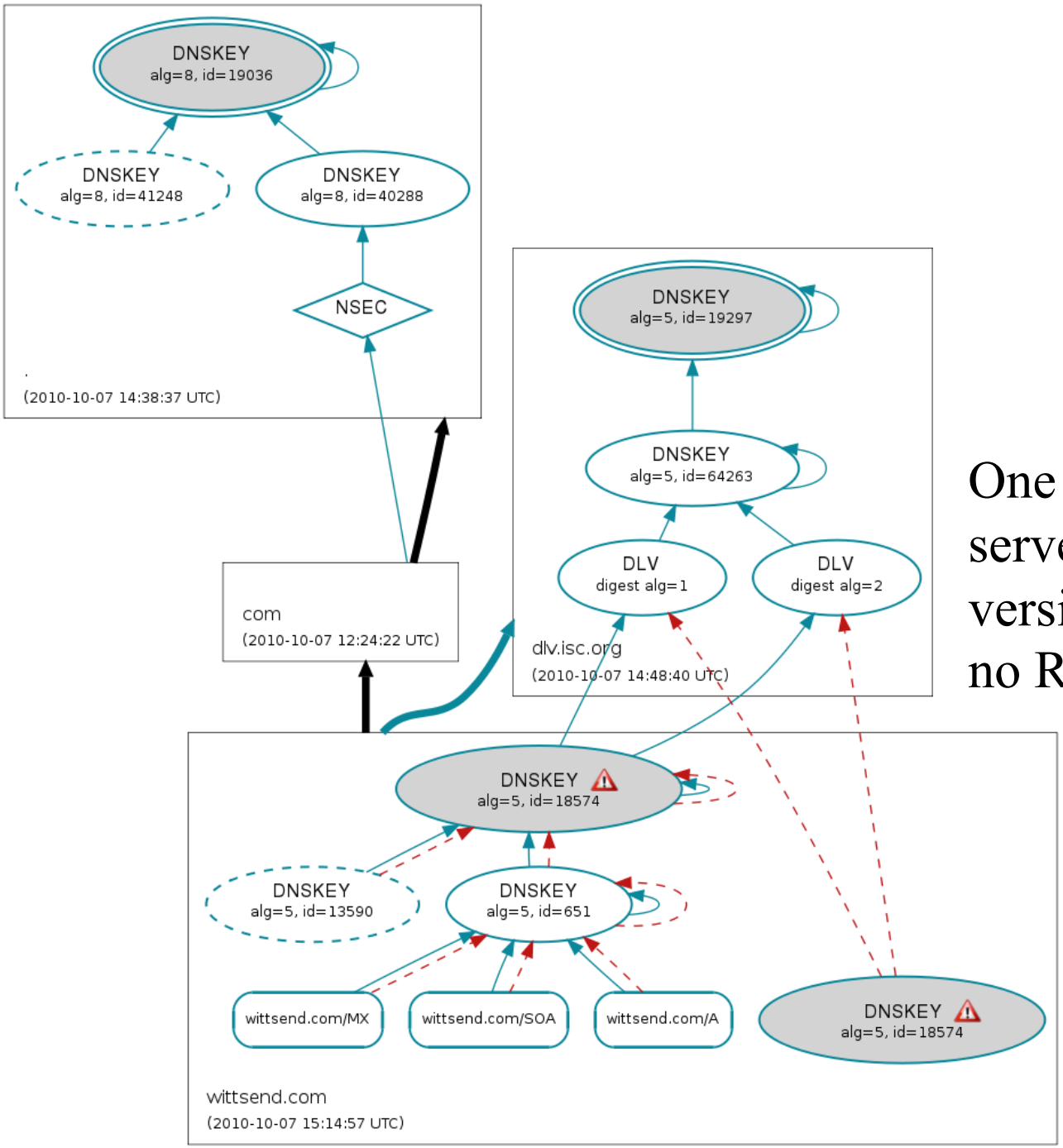


Some authoritative servers not serving NSEC3 RRs; resolver cannot prove insecure delegation



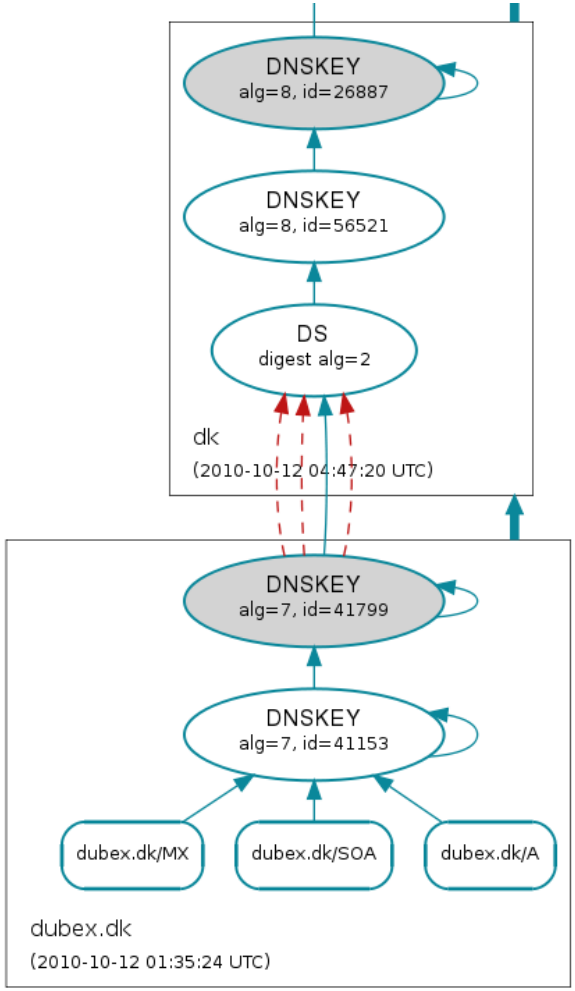
Other interesting behavior



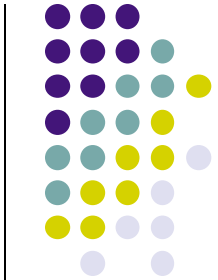


One authoritative server serves corrupt version of KSK (and no RRSIGs)

Four different DS RRs for a particular DNSKEY, only one of which is valid

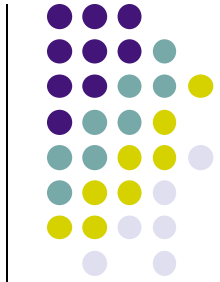


Future work



- DNSSEC history
- RESTful interface
- Tie-in to other sources, such as DNSDB

Sandia National Laboratories

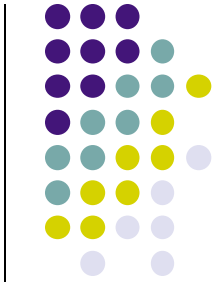


Questions?

ctdecci@sandia.gov
http://dnsviz.net/

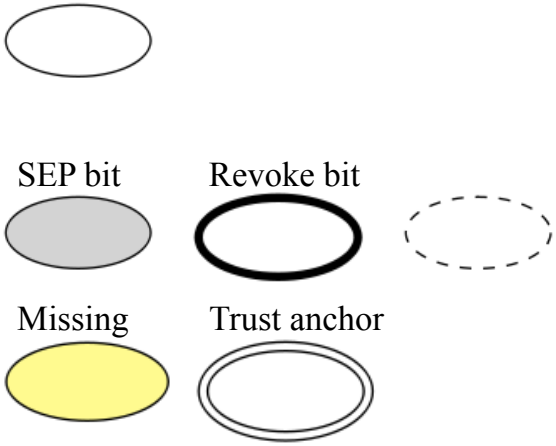
Sandia National Laboratories

DNS Visualization



RRset

DNSKEY/DS RR



NSEC/NSEC3
covering DS