

DNSViz: A DNS Visualization Tool

Casey Deccio

Sandia National Laboratories

2010 DNS-OARC Workshop (2)

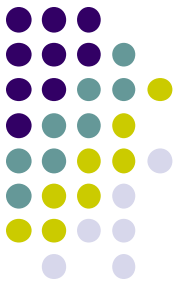
Denver, CO

Oct 14, 2010

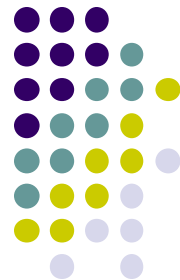


Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Objectives



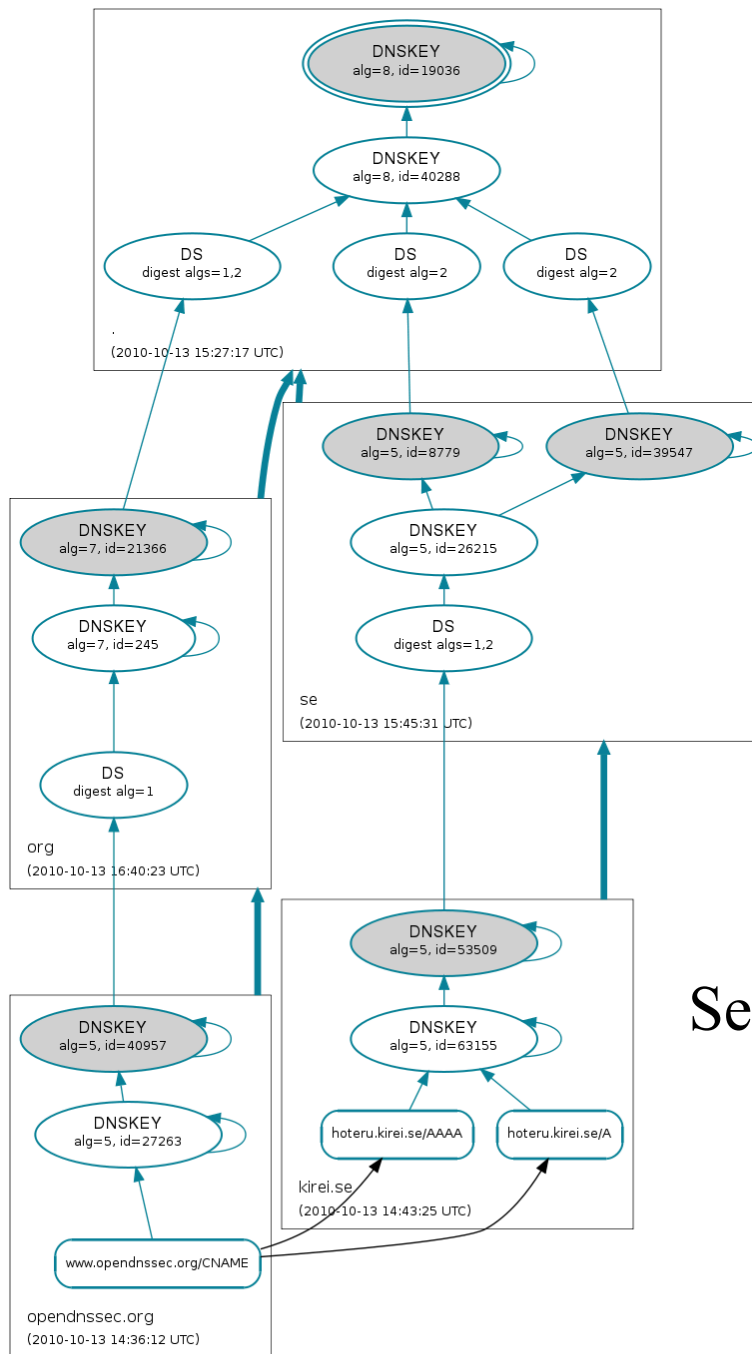
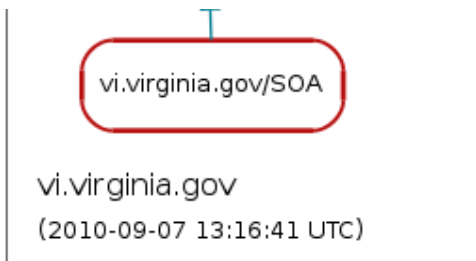
- Help administrators understand DNSSEC
 - Chain of trust
 - Secure/insecure/bogus status
 - Dependencies
- Facilitate DNSSEC troubleshooting
 - Easily identify problems or potential problems related to misconfiguration



Insecure



Bogus



Secure



Trust anchor

Secure delegation

Valid RRSIG

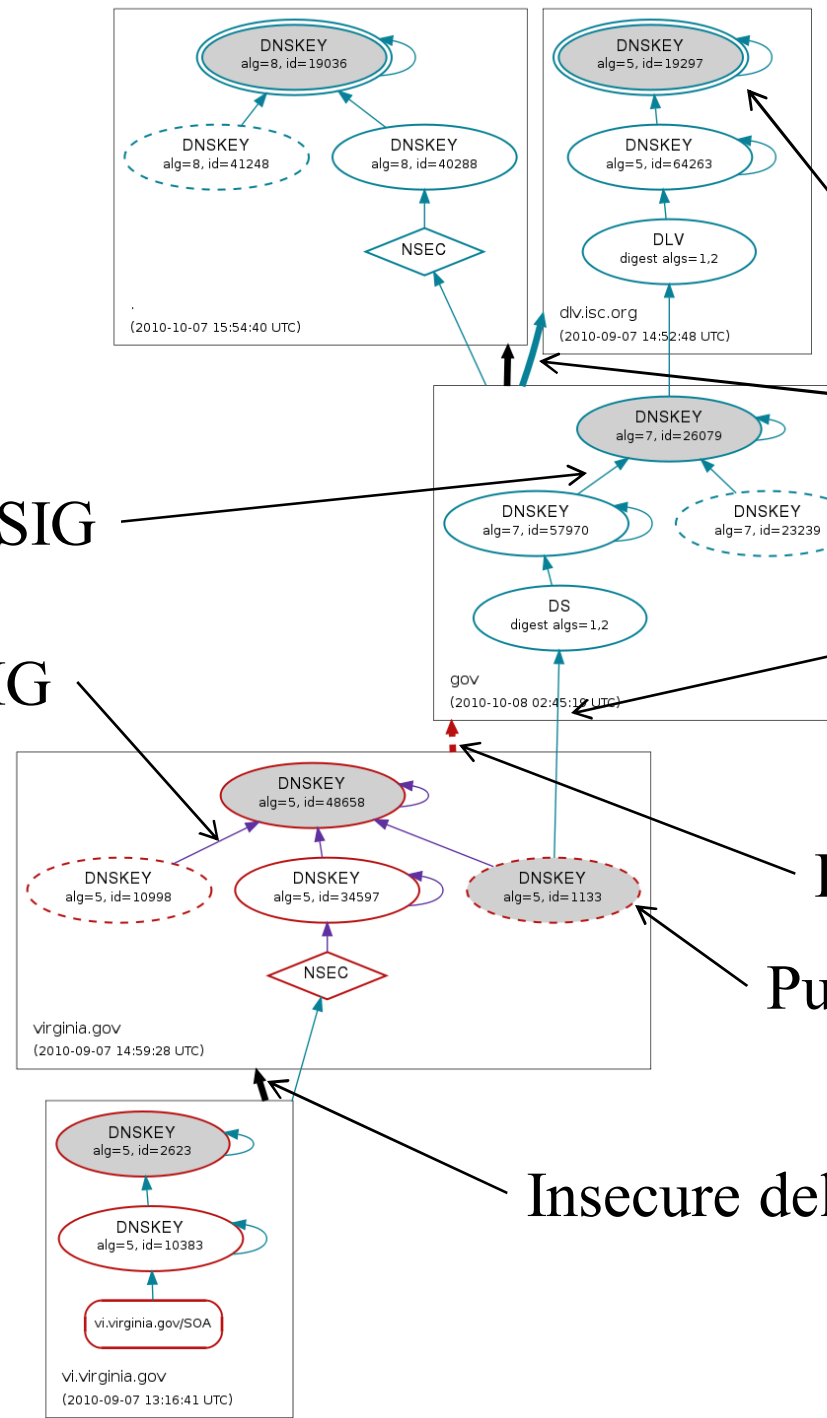
Correct DNSKEY digest

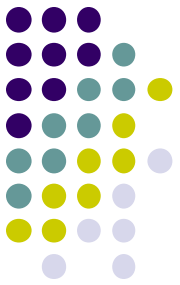
Expired RRSIG

Bogus delegation

Published DNSKEY

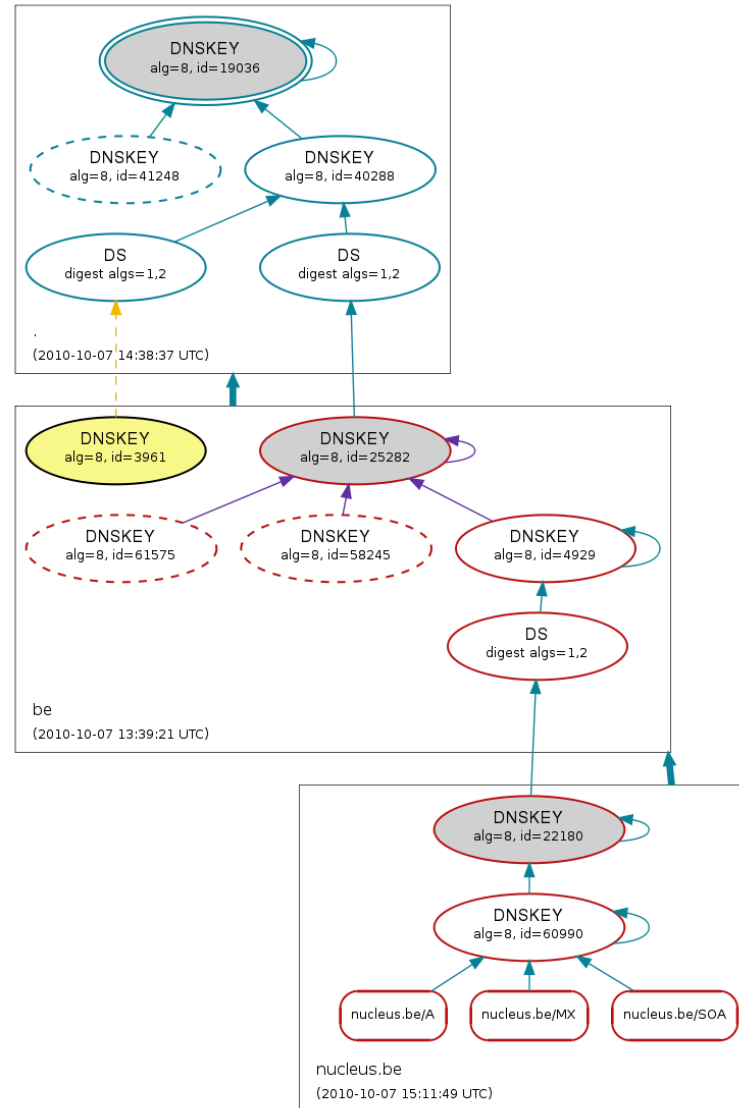
Insecure delegation

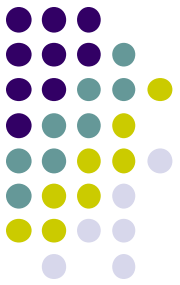




DNSSEC – important points

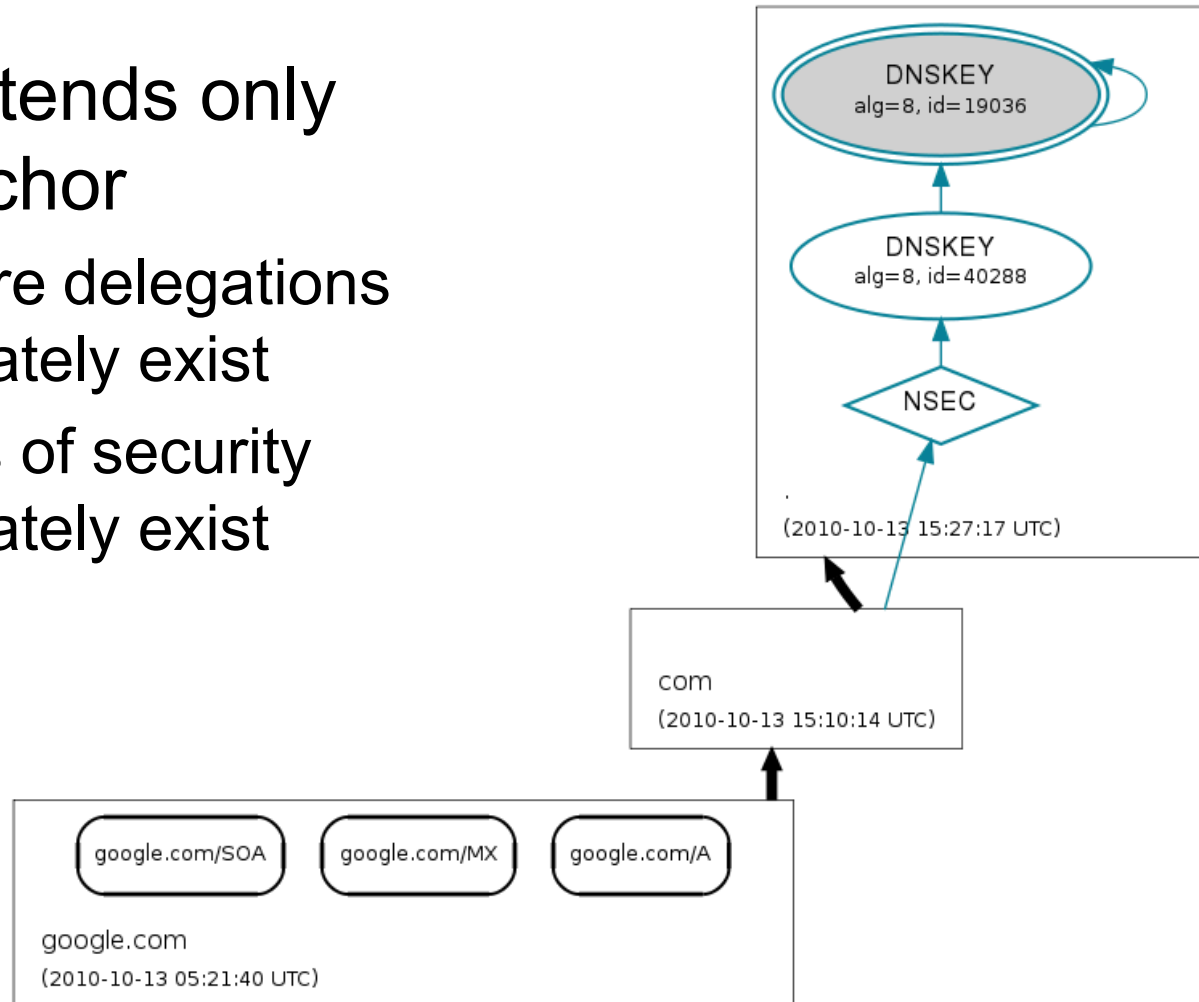
- A contextual view of a zone configuration is essential
 - Ancestry
 - Dependencies (CNAME, MX, etc.)





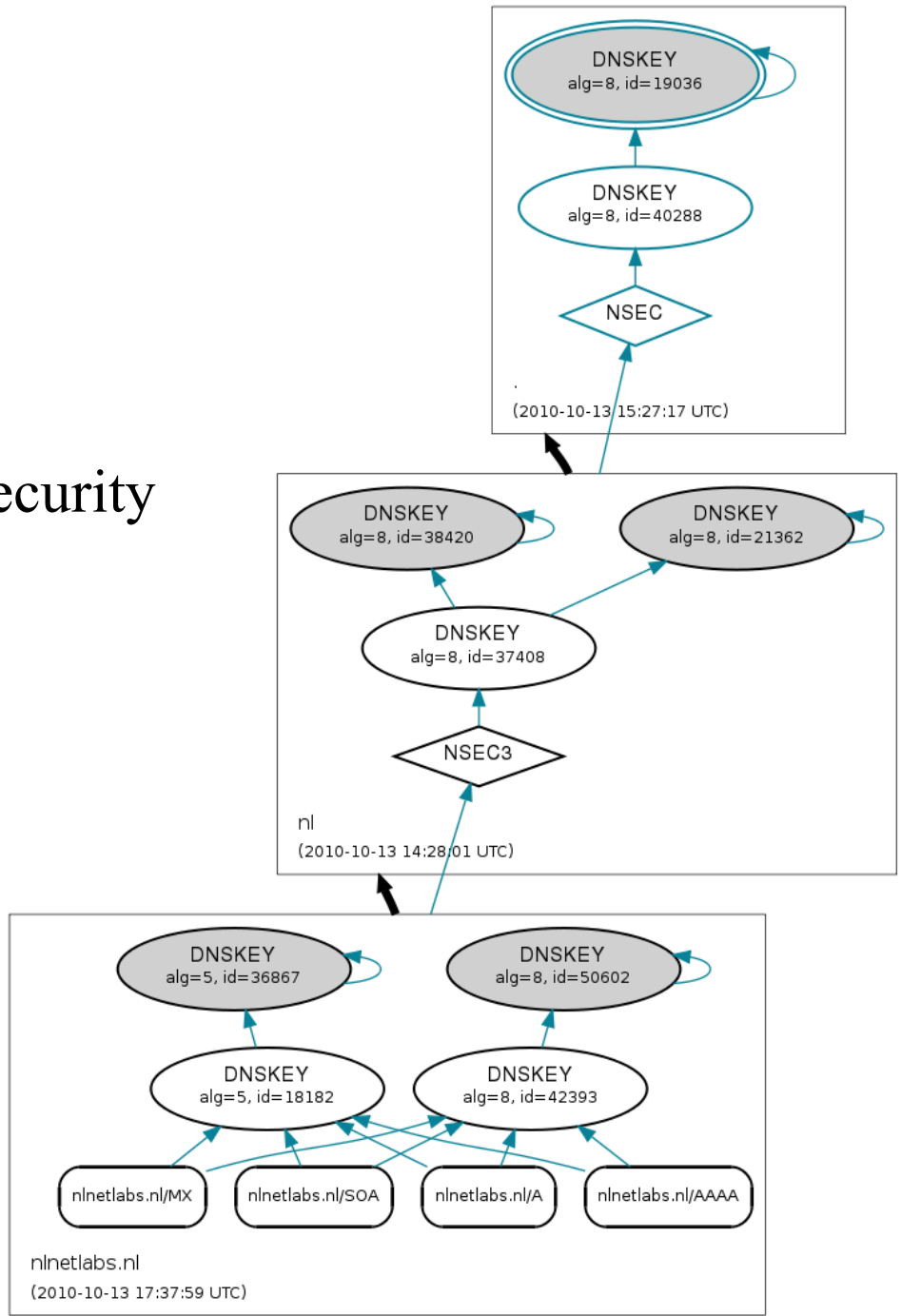
DNSSEC – important points

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

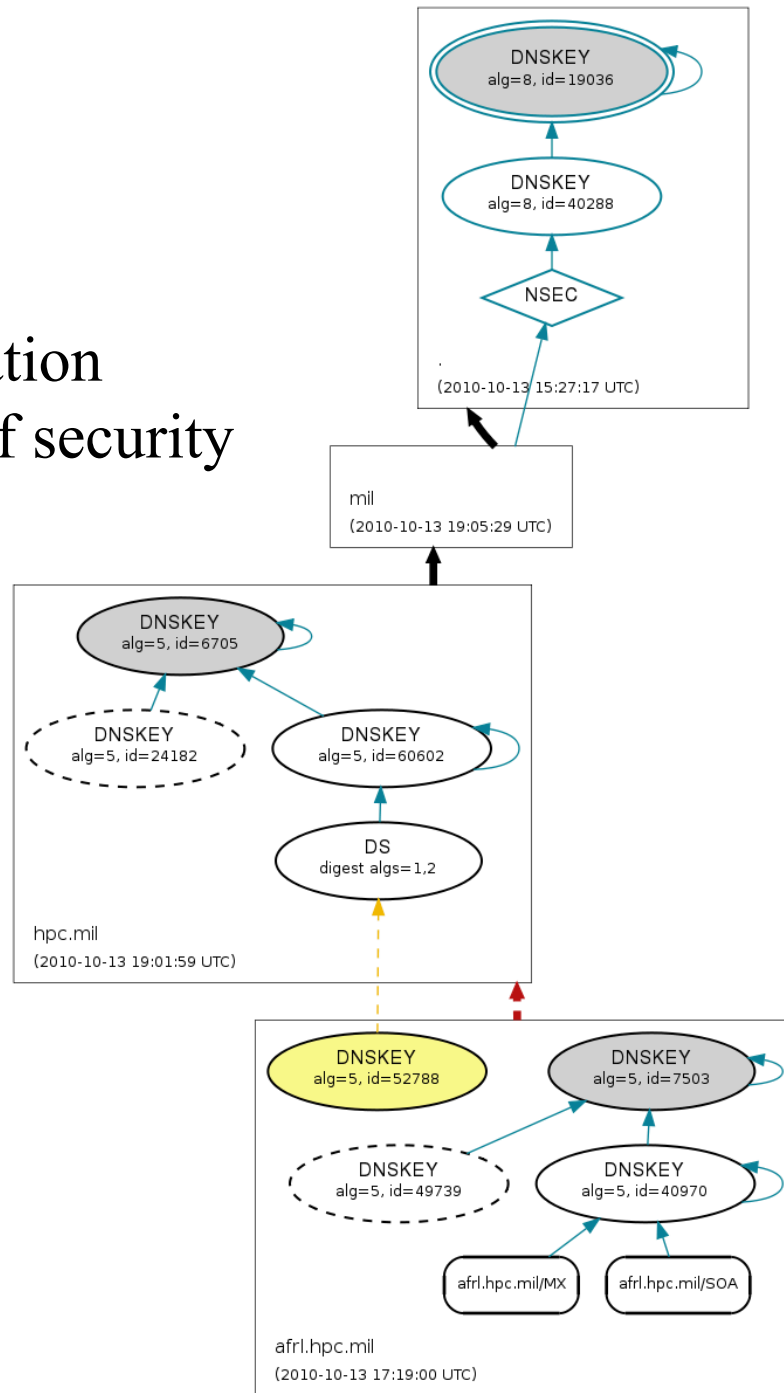




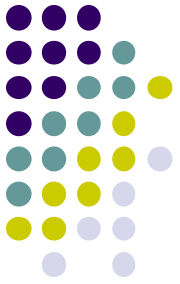
Islands of security



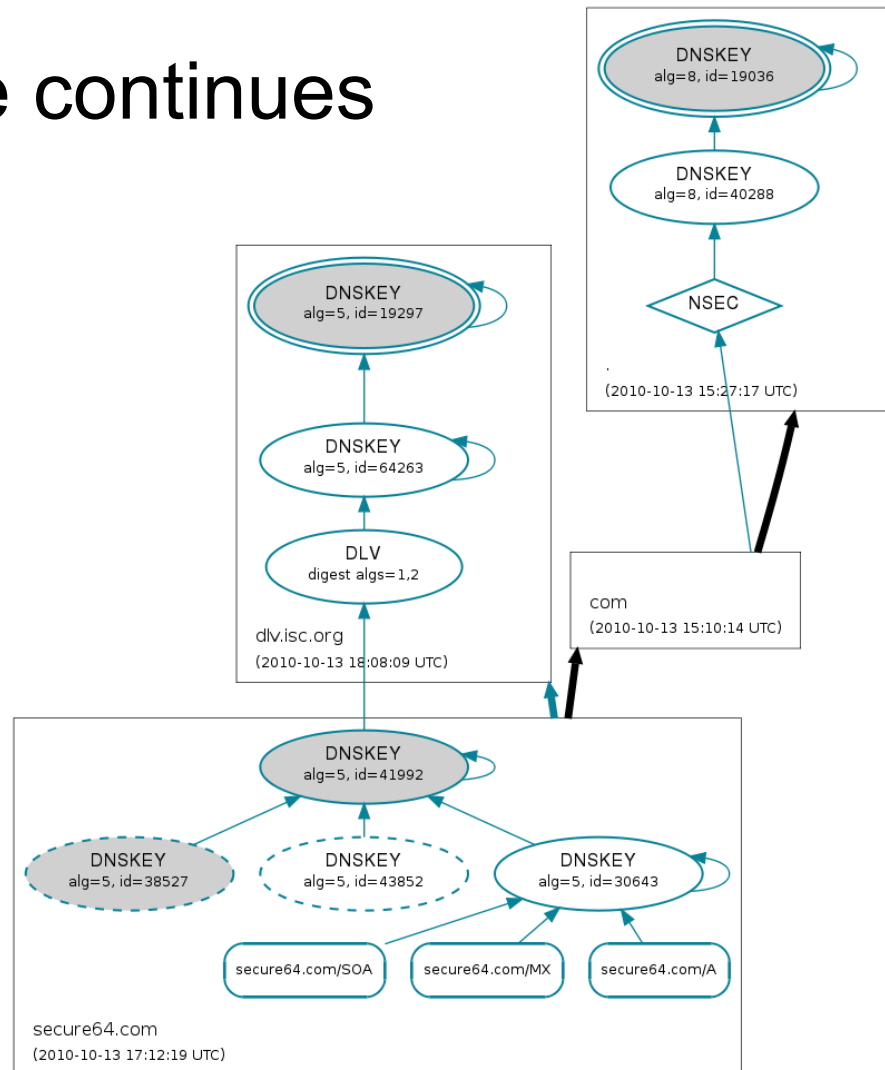
Broken delegation under island of security

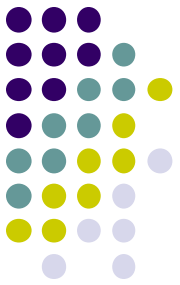


DNSSEC – important points



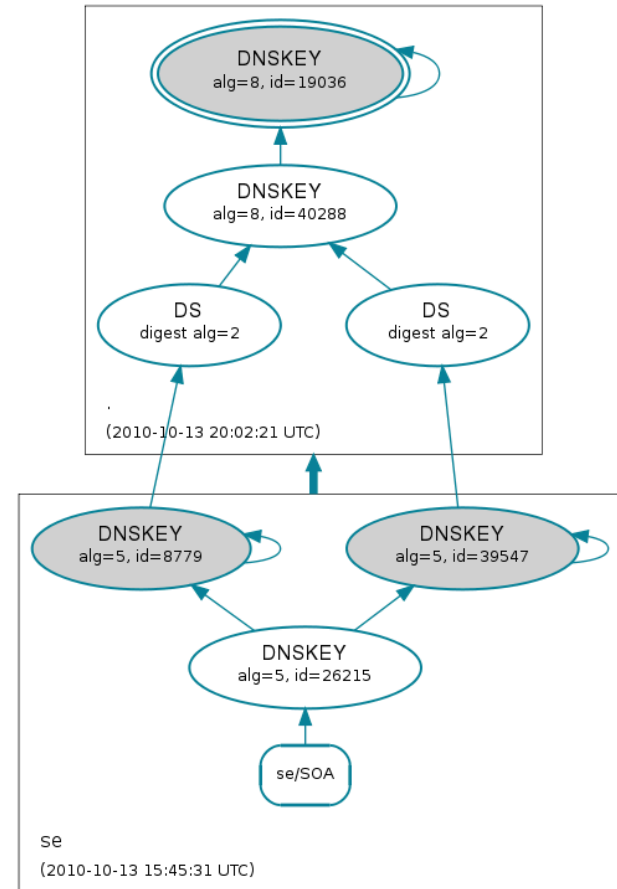
- DLV use continues

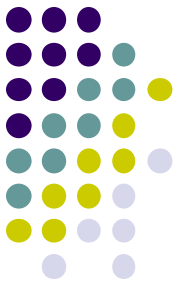




Visualization challenges

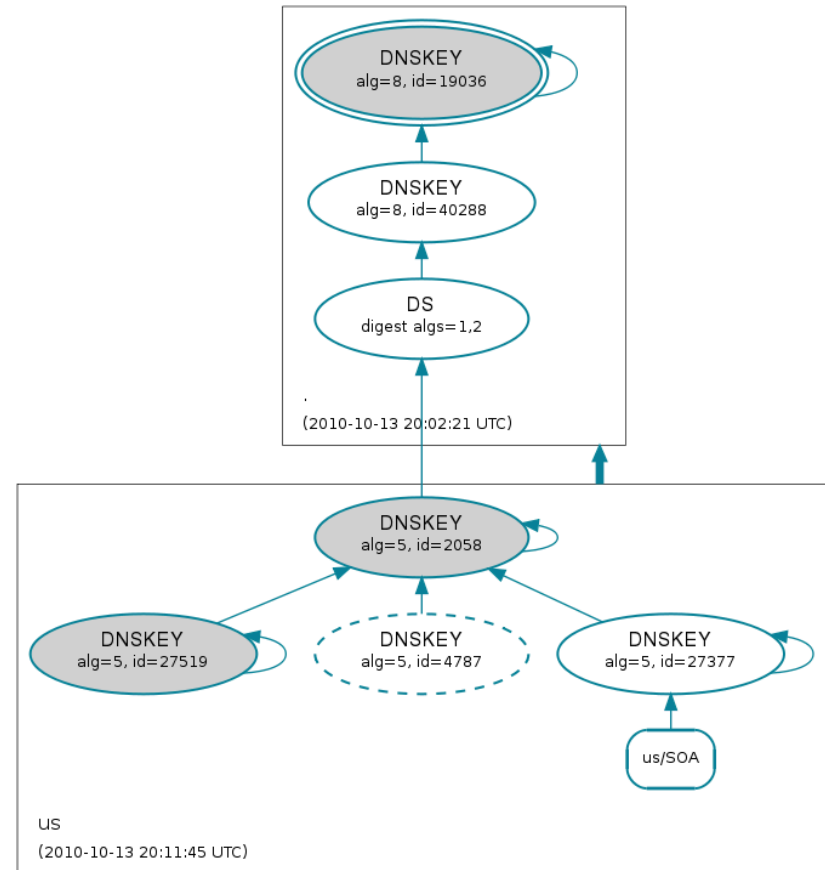
- DNSKEY and DS RRs are useful individually, but are validated as part of an RRset
 - DNSKEY RR is a single node, but considered as part of the entire DNSKEY RRset
 - Set of DS RRs having same name, alg, key tag is a single node



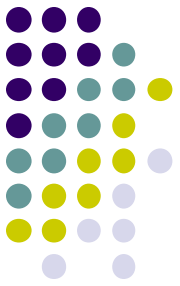


Visualization challenges

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

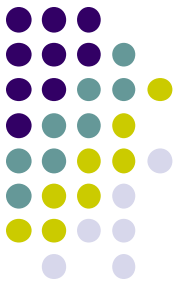


Visualization challenges

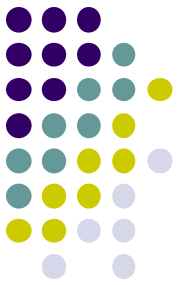


- Multiple algorithms in DNSKEY RRset or DS RRset
 - Is there a valid path to the DNSKEY RRset for each algorithm in the DS RRset?
 - Is there a valid path to each RRset for each algorithm in the DNSKEY RRset

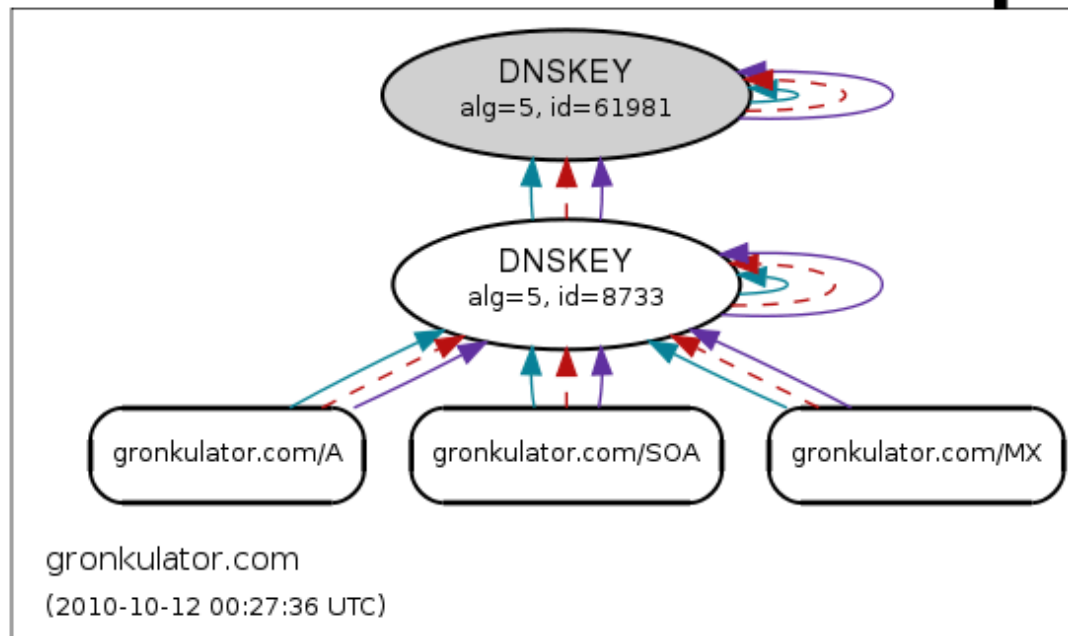
Visualization challenges

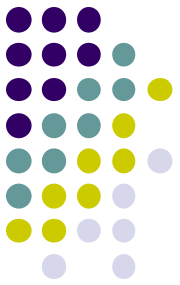


- Server consistency issues:
 - Missing or inconsistent DNSKEYs
 - Not returning RRSIGs
 - Not returning NSEC/NSEC3 RRs

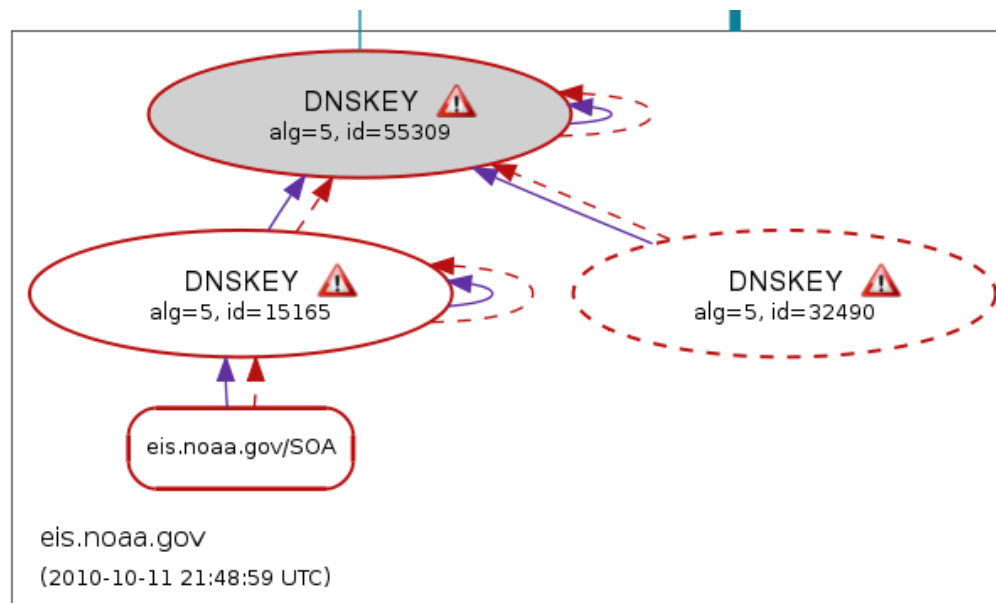


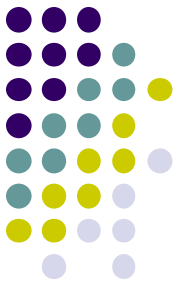
Valid, expired, and missing RRSIGs on different authoritative servers



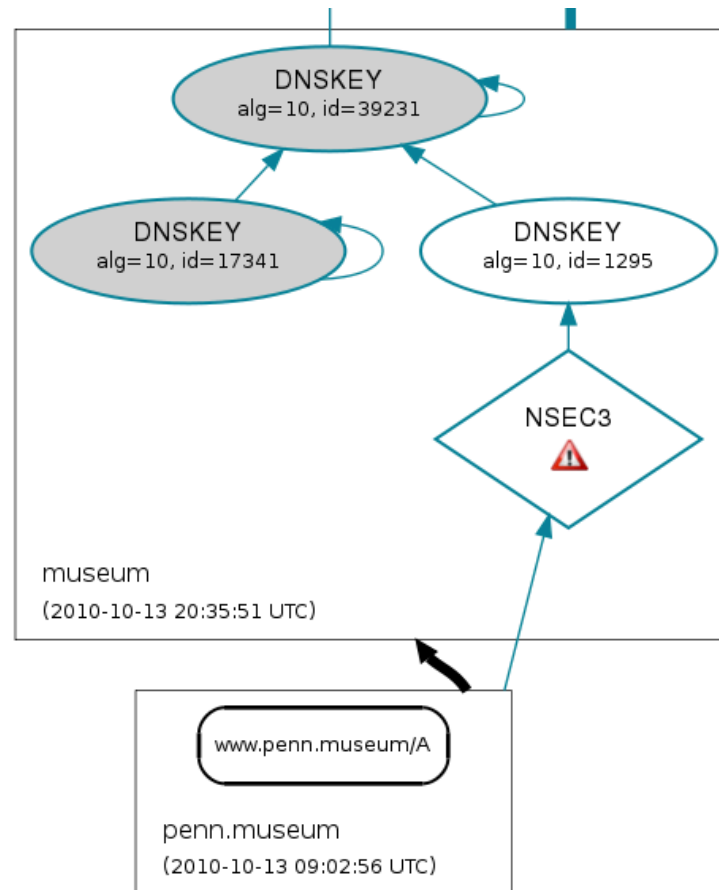


Some authoritative servers not serving DNSKEY RRs nor RRSIGs

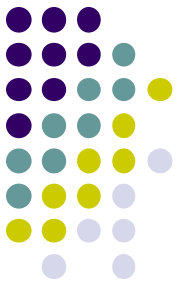


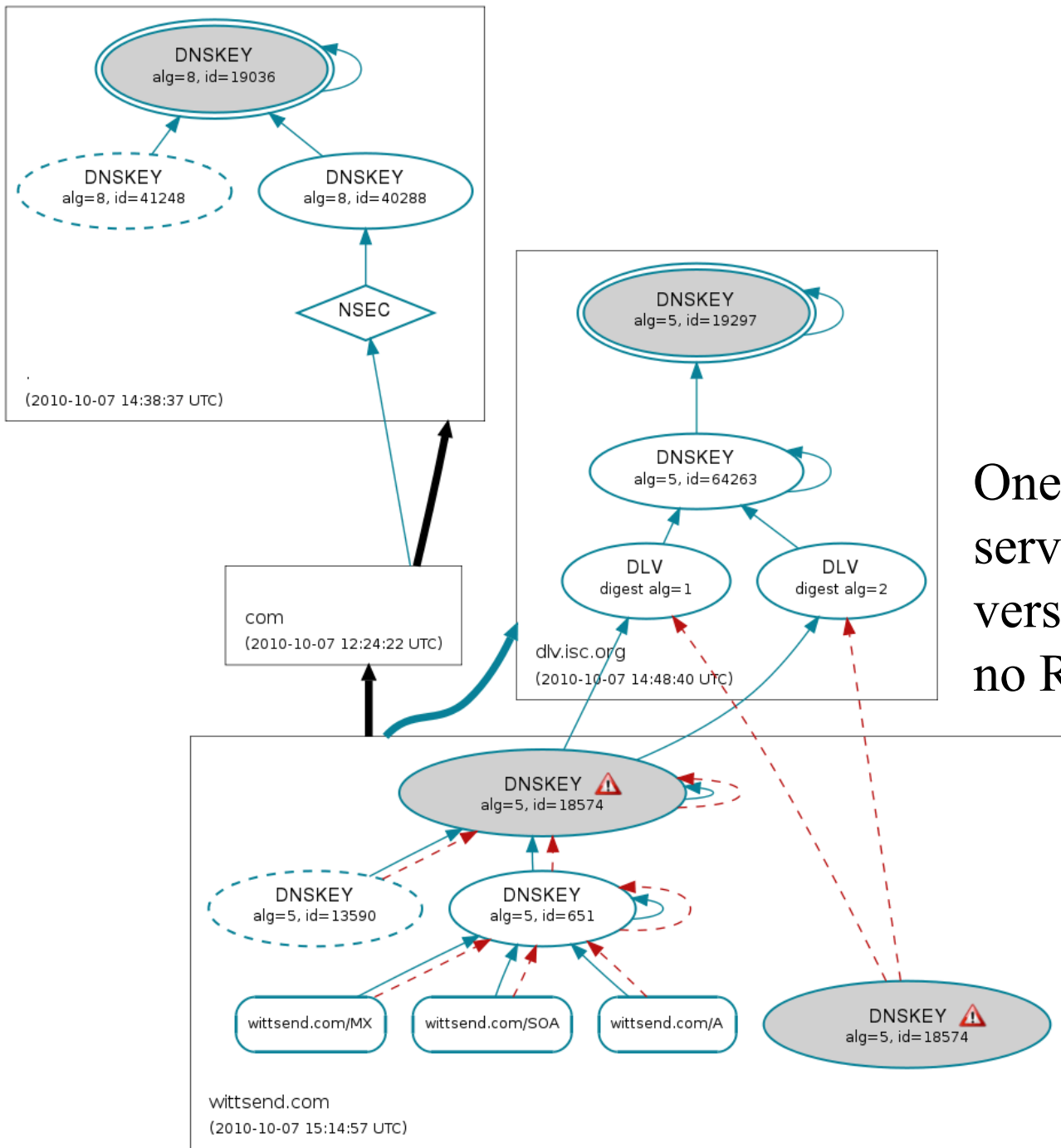


Some authoritative servers not serving NSEC3 RRs; resolver cannot prove insecure delegation

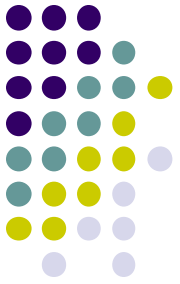


Other interesting behavior

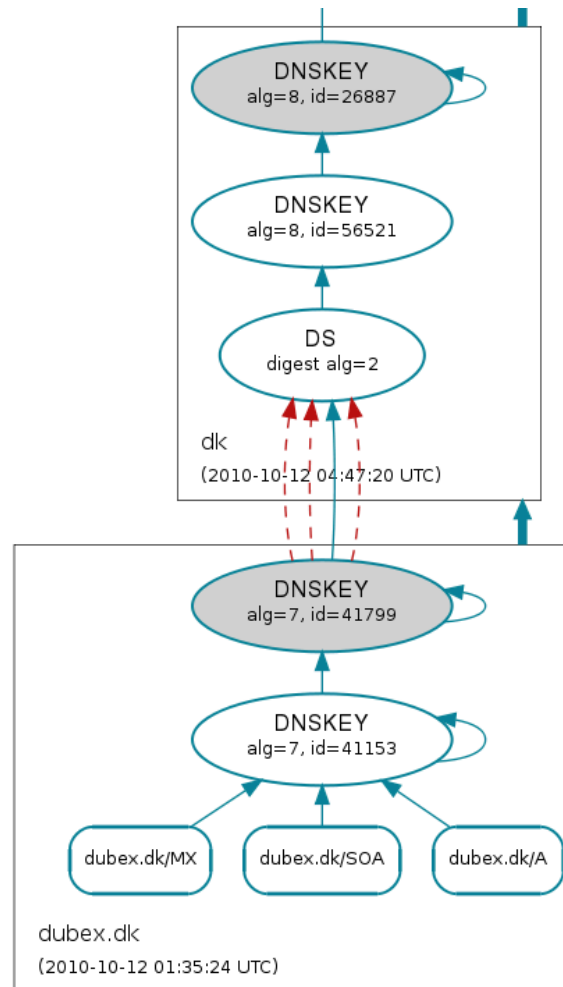


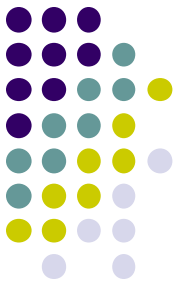


One authoritative server serves corrupt version of KSK (and no RRSIGs)



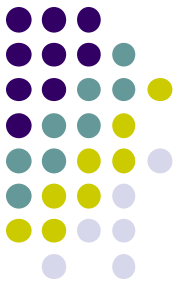
Four different DS RRs for a particular DNSKEY, only one of which is valid





Future work

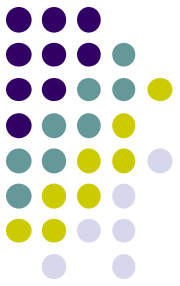
- DNSSEC history
- RESTful interface
- Tie-in to other sources, such as DNSDB



Questions?

ctdecci@sandia.gov

<http://dnsviz.net/>



DNS Visualization

RRset



DNSKEY/DS RR



SEP bit



Revoke bit



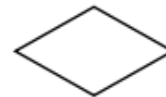
Missing



Trust anchor



NSEC/NSEC3
covering DS



Missing

