NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Trustworthy Networking Program

DNSSEC Developments and Updates

Scott Rose
scott.rose@nist.gov

ISPAB

11/4/2010

DNSSEC

U.S. DEPARTMENT OF HOMELAND SECURITY

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

What is DNSSEC?

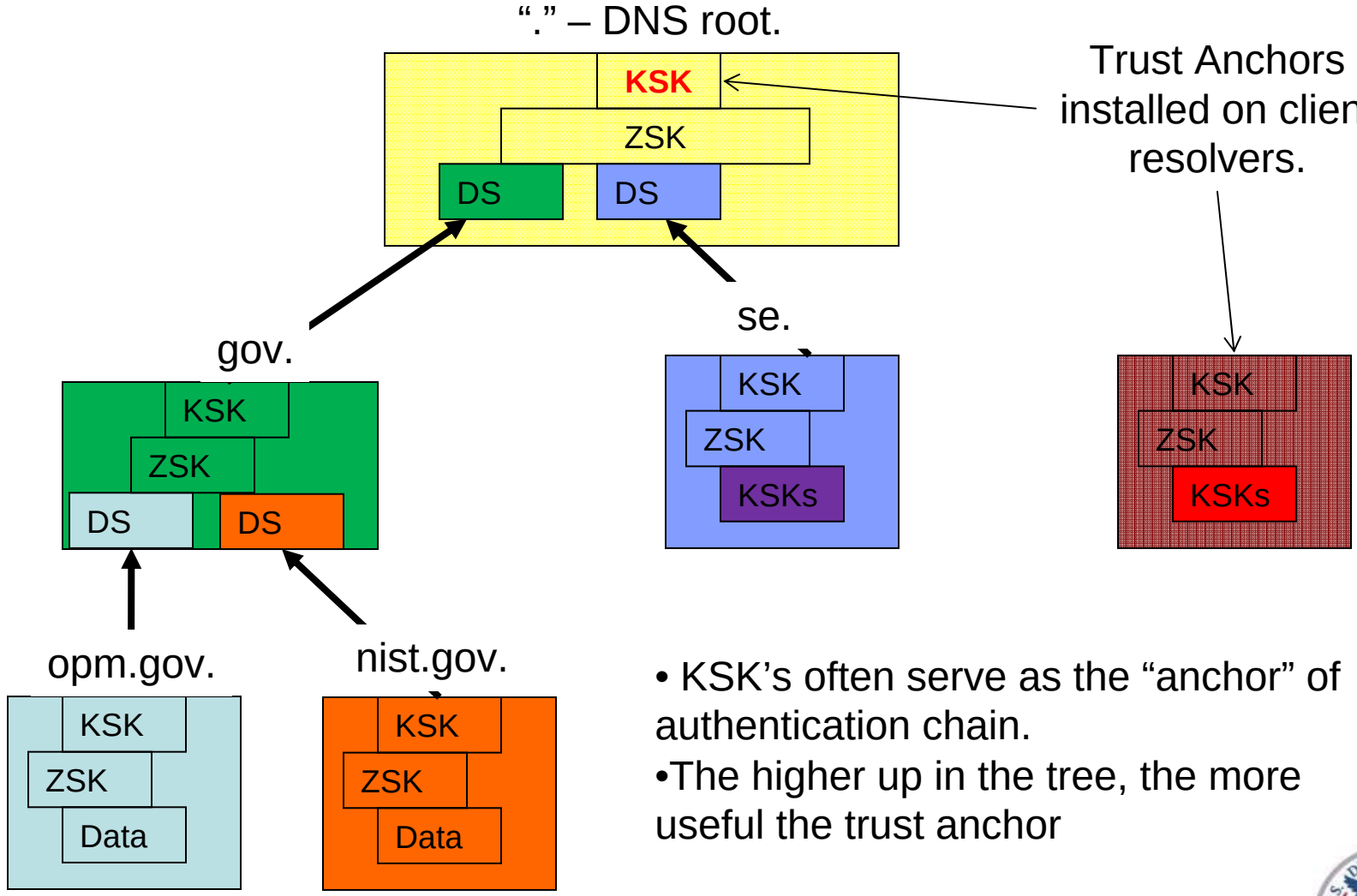
- DNS Security Extensions (DNSSEC)
  - Provides source authentication and integrity protection for DNS data in responses
    - Uses digital signatures over DNS Resource Records
    - Public keys also stored in DNS
  - Authentication chains link response data to installed trust anchor.
    - similar to X.509 certificate chains, but totally contained in the DNS
- NIST has been involved in DNSSEC development and deployment since 2000
  - Sticks: helped provide input on DNSSEC policy in the USG
  - Carrots: Produce guides, tools and testbeds to aid admins in deployment.

Trustworthy Networking Program

DNSSEC

U.S. Department of Homeland Security

DNSSEC Chain of Trust



- KSK's often serve as the "anchor" of authentication chain.
- The higher up in the tree, the more useful the trust anchor

History: Deployment Drivers (Sticks)

- Office of Management and Budget (OMB) issues Memo (M-08-23), August 2008
  - Issued order to sign the .gov TLD by Dec. 08 (actually signed Jan. 09)
  - All 2nd level, external facing zones signed by Dec. 09
- Federal Information Security Management Act (FISMA)
  - Security audit for all US Federal IT systems
  - Audit controls covering DNSSEC included in Dec. 2007 (expanded in latest revision in 2009-10)

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Deployment Phases

- USG DNSSEC Incremental Deployment Plan– Not a chicken and egg problem...
  - Phase1: 2005-2010 Technology Development/Guidance.
  - Phase2: 2010-2012 Deploy Signed DNS Infrastructure
  - Phase3: 2012-2014 Deploy Validating Resolver Infrastructure.
  - Phase4: 2014-> Exploit Trusted Naming Infrastructure.
- Phase 1 complete
  - Development of DNSSEC Specification in the IETF (2005)
  - Development of FISMA controls (2010) (Stick)
  - Development of NIST SP 800-81(r1) and the Secure Naming Infrastructure Pilot Testbed created (Carrots)

Trustworthy Networking Program

DNSSEC

U.S. DEPARTMENT OF HOMELAND SECURITY

Current State of Deployment

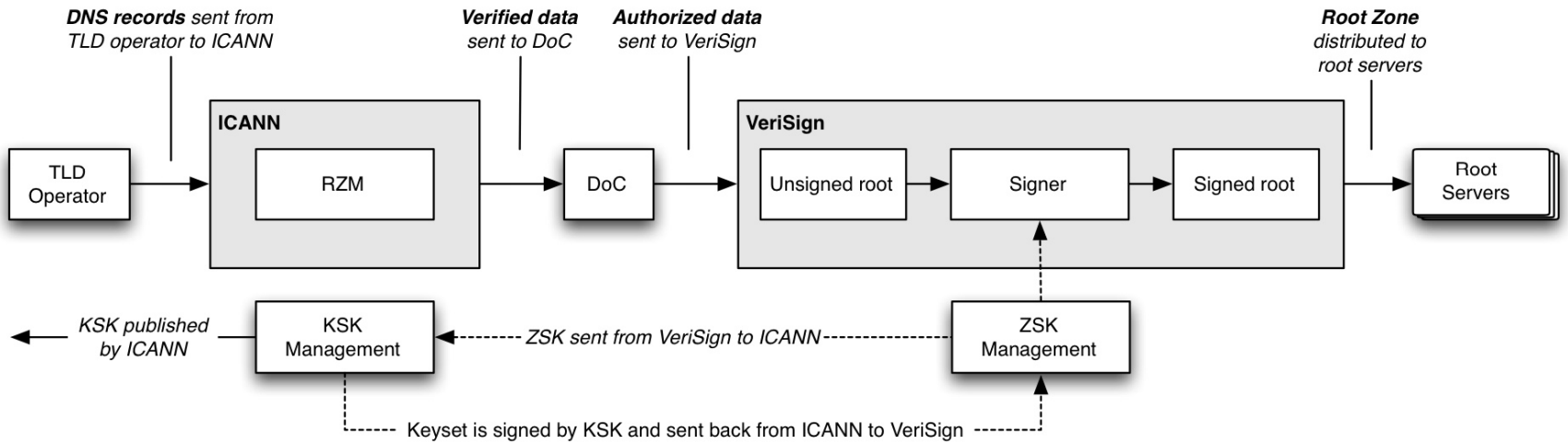
- We are now in Phase 2
  - .gov domain signed (2009-2010)
  - OMB Deadline passed, Latest DNSSEC FISMA controls now applicable
    - Roughly 705 out of 1400+ Federal delegations signed
    - Validation only required for HIGH impact systems in this FISMA revision
- Seen deployment in several TLD's
  - .edu, .org, .biz, multiple country codes (including .us).
  - .net/com announced deployment plans for 2011

More DNSSEC Aware Products

- Multiple server implementations
  - Both authoritative and validating recursive servers
  - Open source (e.g. BIND) and Proprietary (e.g. Windows Server 2008)
- Special Purpose appliances
  - DNSSEC Signers and signer/server appliances.
  - Load balancers that use DNS (e.g. F5 Networks)
- DNSSEC offered as a service
  - DNS hosting services
  - Content Distribution Networks

Deployment at the Root

- July 15th – DNS Root zone signed
  - Joint effort between NTIA/NIST, ICANN and VeriSign



NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Root Zone DNSSEC Deployment

- USG keeps a largely “hands-off” approach
  - only approves change requests to the root & does not play a role in key generation or signing.
- Technical details:
  - Signed using RSA/SHA-256 with 2048 bit keys
    - ZSK changes every 3-6 months, KSK every 5 years.
  - Trust anchor generated using HSM’s, access requires several people (Trusted Community Representatives): not ICANN/USG/VeriSign staff.
    - Regular key generation/signing ceremonies at ICANN secure data centers in LA and Virginia
    - Crypto modules FIPS 140-2 level 4 certified, data centers comparable to HIGH Impact FISMA system.

Trustworthy Networking Program

DNSSEC

U.S. Department of Homeland Security

DNSSEC Deployment on the Client Side

- ISP's and universities turning on validation now.
  - Comcast testbed moved to production servers.
- Windows 7 has DNSSEC as a managed policy setting
  - No validation on client side, but client requests DNSSEC and checks for validation done by upstream recursive servers
- DNSSEC appearing in applications
  - open source patches for Firefox, Thunderbird, IM clients, SSH clients.

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

USG DNSSEC Experiences

- Lessons Learned
  - Planning for DNSSEC provides opportunity to revisit DNS structure.
    - Many agency level DNS operators were forced to discover and revisit their DNS architectures.
  - Many “new” DNSSEC management processes improve existing DNS operations.
    - DNSSEC requires regular maintenance (e.g. resigning)
    - DNSSEC inspires careful consideration of authentication, notification, and monitoring process to maintain signed zones.

Trustworthy Networking Program

DNSSEC

U.S. Department of Homeland Security

Lessons Learned

- Administrator education should be a major priority during deployment.
  - Admin error the cause of most problems
  - Give administrators time to plan and clear policy guidance about what they need to do.
  - Know who to contact when mistakes occur
  - Establish a help desk/support network to resolve issues.
- For large domains: establish a procedure for your delegations to upload key material to the parent zone

Lessons Learned

- DNSSEC centric crypto policy is important (DNSSEC is not a PKI)
  - US Federal key policy aimed at PKI certificates (i.e. large, long lived keys), not DNSSEC.
    - causes large response sizes and problems in some routers/firewalls
- Look at your other network components for hidden dangers
  - Old routers/switches or firewalls may drop large DNSSEC responses
    - 1500 bytes a reasonable MTU setting
  - Firewall rules may need changed (UDP & TCP port 53)

Next Steps in .gov

- Finish Phase 2
  - Continue to use policy to drive signing by 2012.
  - Crypto-migration to ECC by 2015
- How to transition to Phase 3?
  - Requiring resolvers capable of validation is easy part.
  - The transition to actually requiring validation requires care
    - Need additional guidance on trust anchor use/management
    - Validation support in OS/browsers/applications need to mature.
- What to expect from Phase 4?
  - Using the DNS as a trusted infrastructure:
    - ID Management (store credentials or certificates) – e.g. DKI
    - SSL & IPSec support for web traffic (key distribution)
    - etc.

Deployment Links

- DNSSEC Blog (DHS program):
  - http://www.dnssec-deployment.org/
- NIST Secure Naming Infrastructure Pilot (SNIP)
  - http://www.dnsops.gov/
- Root Zone DNSSEC deployment
  - http://www.root-dnssec.org/

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

DNS Related Controls in FISMA

- SC-8 Transmission Integrity (DNS zone replication)
- SC-20 Secure Name/Address Resolution Service (Authoritative Source)
  - DNSSEC signing of *all* zone data (all Impact Levels)
- SC-21 Secure Name/Address Revolution Service (Recursive or Caching Resolver)
  - Recursive servers (Primary and Secondary) must be able to validate DNSSEC signed responses (HIGH Impact only).
- SC-22 Architecture and Provisioning for Name/Address Resolution Service

Trustworthy Networking Program

DNSSEC

U.S. DEPARTMENT OF HOMELAND SECURITY