DNSSEC and the Authoritative Root Zone

Fiona Alexander

Tim Polk

April 1, 2009

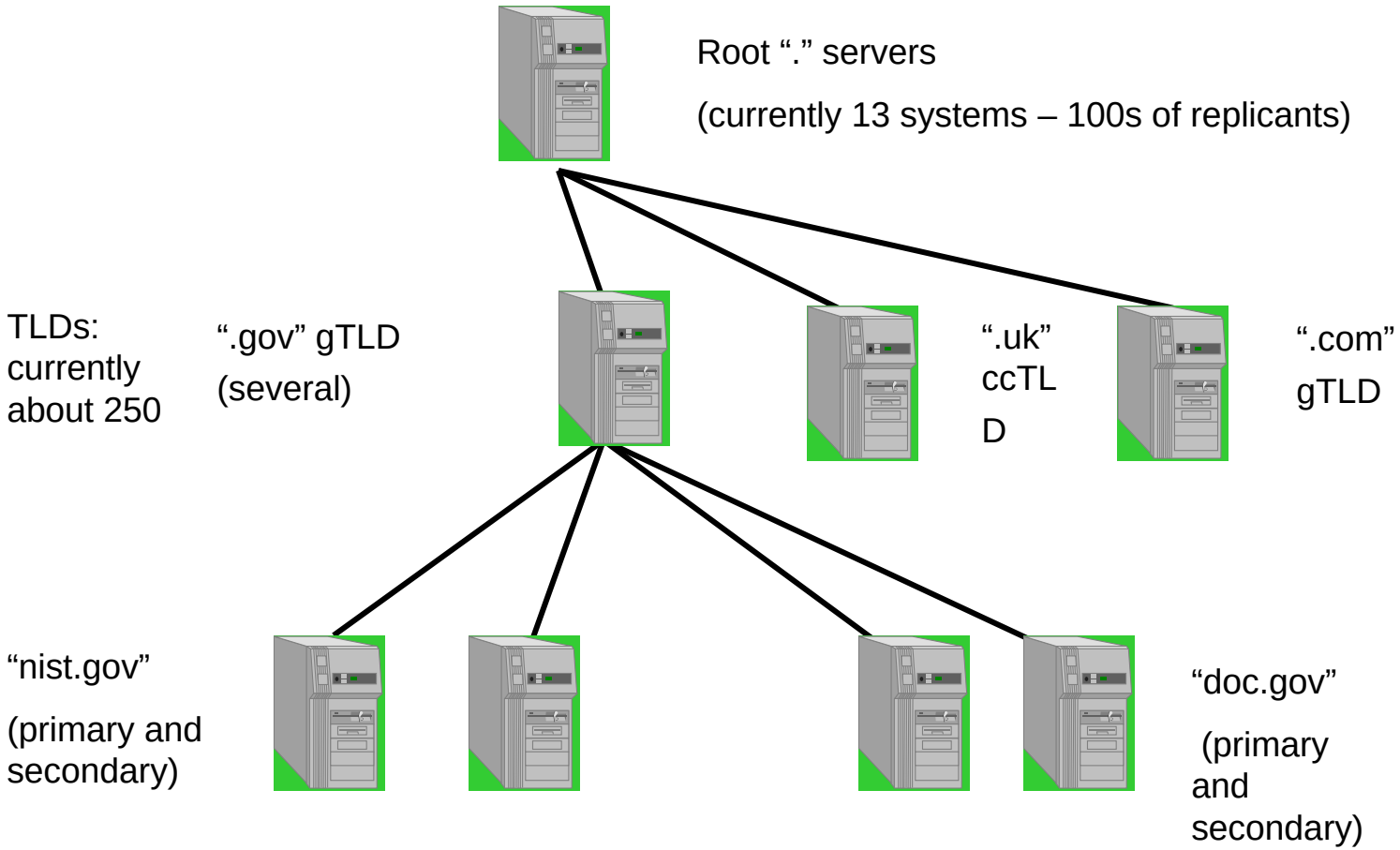
Overview

- The Internet Domain Name System
- The Authoritative Root Zone & DoC's Role
- The DNSSEC Standards: What & Why
- Importance of Deploying DNSSEC in the Authoritative Root Zone
- Progress Towards a Signed Authoritative Root Zone

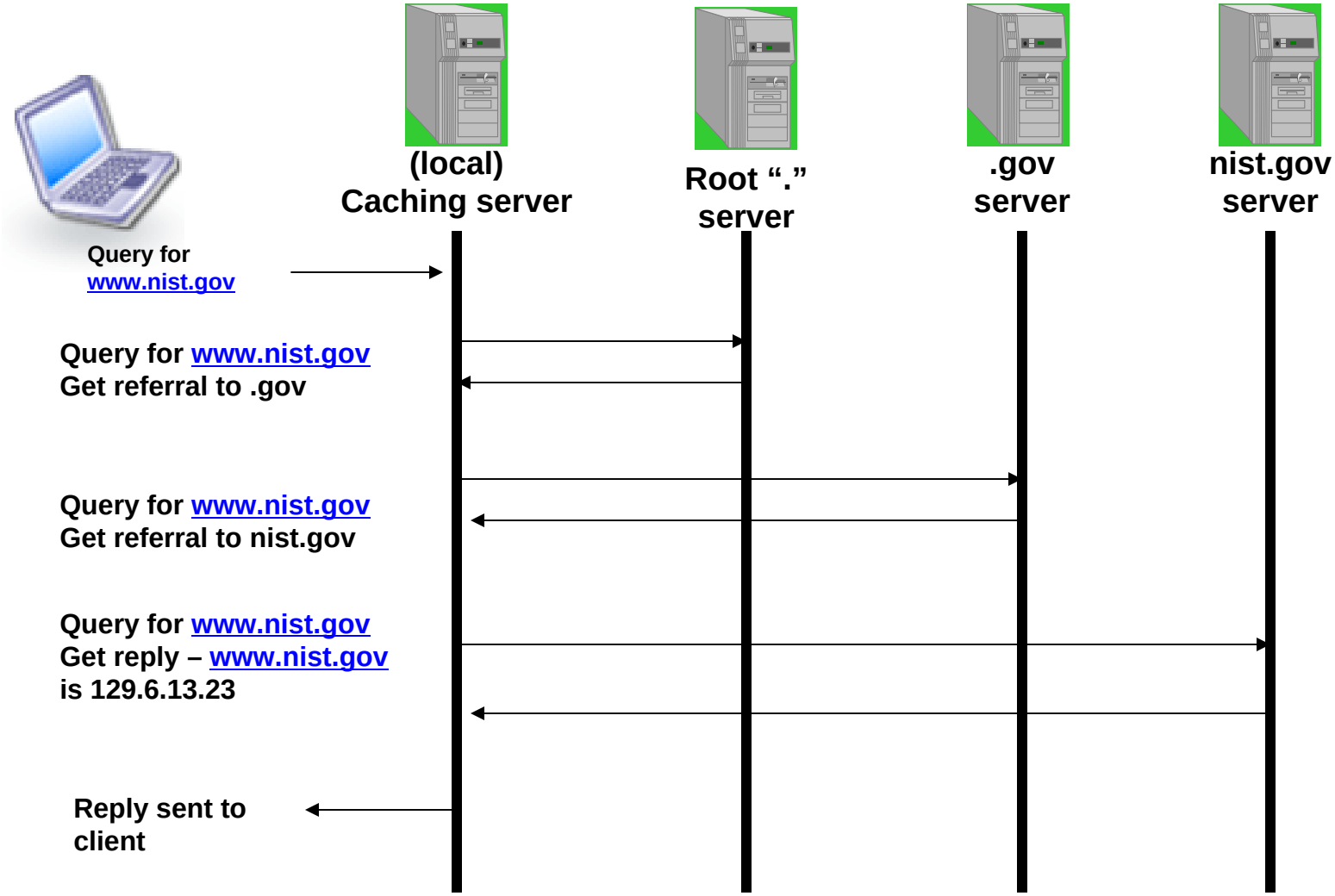
The Internet Domain Name System

- Foundational Technology
  - Maps user friendly domain names to Internet Protocol v4 or v6 addresses
- Distributed Hierarchical system
  - Each subordinate zone maintains the mappings for that domain
  - To obtain a mapping for a specific hostname, start at root zone and work your way down the tree

Topological View of DNS



Example of DNS Query



DOC Role -The Authoritative Root Zone

- The authoritative root zone file is the top of the DNS hierarchy, for which the U.S. Department of Commerce has policy oversight.
- The Department of Commerce's current legal agreements with ICANN (IANA functions contract) and VeriSign (Cooperative Agreement) set forth the root zone management process as:

(1) TLD operator submits change request to the IANA Functions Operator (ICANN);

(2) the IANA Functions Operator processes the request;

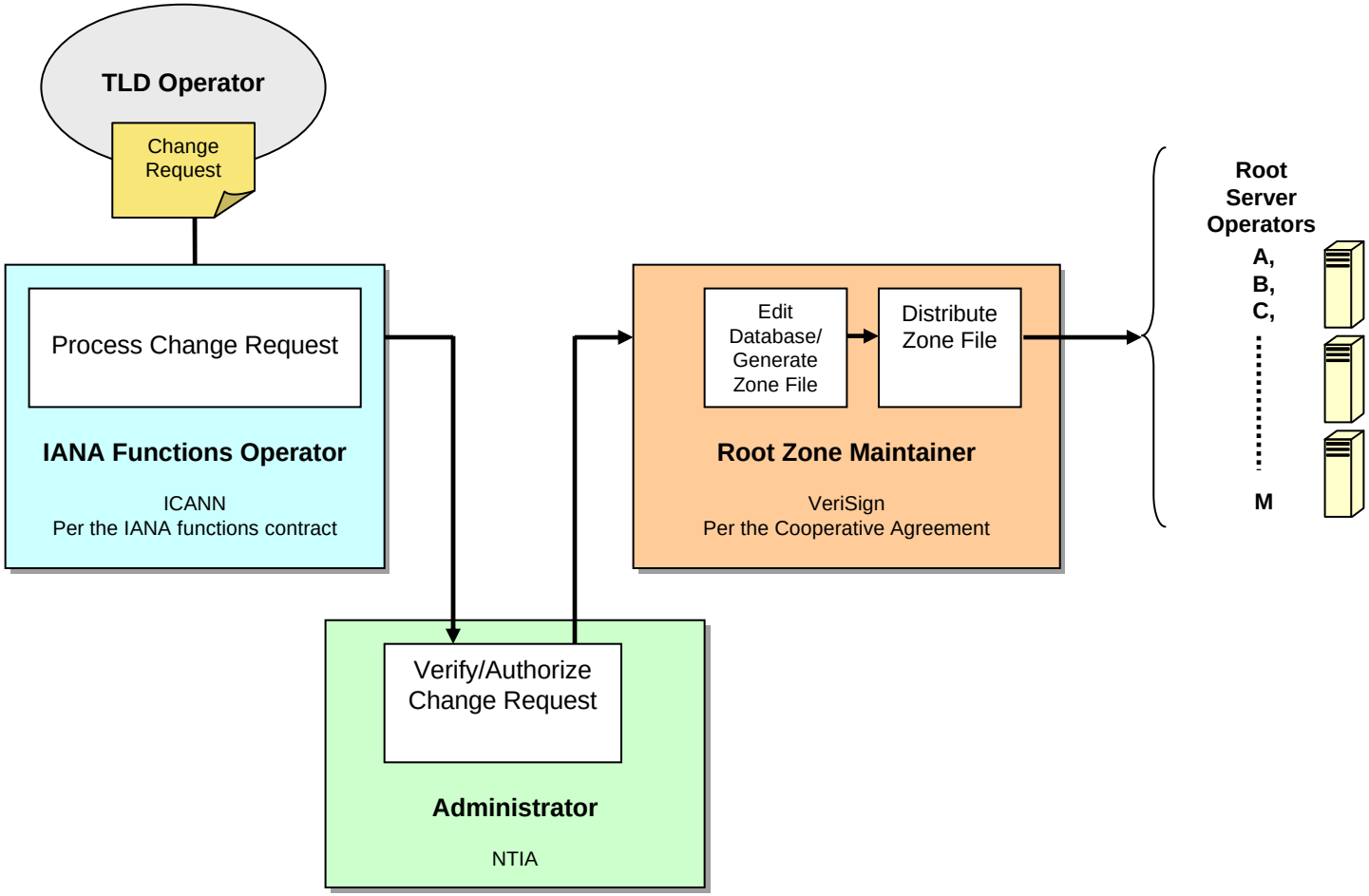
(3) the IANA Functions Operator sends a request to the Administrator (DOC) for verification/authorization;

(4) the Administrator sends verification/authorization to the Root Zone Maintainer (VeriSign) to make the change;

(5) the Root Zone Maintainer edits and generates the new root zone file; and

(6) the Root Zone Maintainer distributes the new root zone file to the 13 root server operators.

Current Root Zone Management Process



Security and the Internet Domain Name System

- Accuracy, integrity and availability of the DNS are essential to the systems and services that use the Internet
- However, the DNS was not originally designed with strong security mechanisms
  - Recent attacks (Kaminsky) have highlighted the need to provide these services
- Accuracy and integrity can be provided using DNSSEC, but deployment has been slow

Cache Poisoning Attack

- Inserting false data into a resolver's cache
  - Inserting fake data into a resolver's cache by sending fake replies
  - Since replies are not authenticated, the resolver relies primarily on a 16 bit random in the request to authenticate the response
  - If the attacker guesses the right number, the fake reply looks authentic
- Since a caching resolver serves many end systems, this can be an efficient attack

Kaminsky Cache Poisoning

- Cache poisoning attacks are not new, but Dan Kaminsky refined them into an art form
  - DNS vendors informed early 2008, patches developed
  - Publicly disclosed August 2008 at Black Hat
- Attacks on unpatched systems were easy
  - 50% chance of success in ten seconds, 5% in one second
- Patches were developed and have been widely implemented
  - Added port randomization and random capitalization (non-standard!)
  - Patched systems are less vulnerable, but can still be exploited (ex: 50% in 28 days, 5% in 2.8 days)

Summary: Kaminsky Attack

- Technically nothing new (known since 1995)
- What opened eyes:
  - …was the scope of vulnerability – millions of recursive resolvers.
  - … was the ease of executing the attack.
  - … was the novel ways in which cache poisoning could be used as a tool to undermine other critical network services and trust models.
- What people are learning:
  - “The patch” – while important – only moved the vulnerability from trivial to exploit to easy to exploit
  - The Kaminsky attacks will continue – software available, patched systems proven still vulnerable.
  - The Kaminsky attack is just the latest instance to exploit a systemic problem. There will be more..
- The real vulnerability is the inherent lack of security in the DNS.

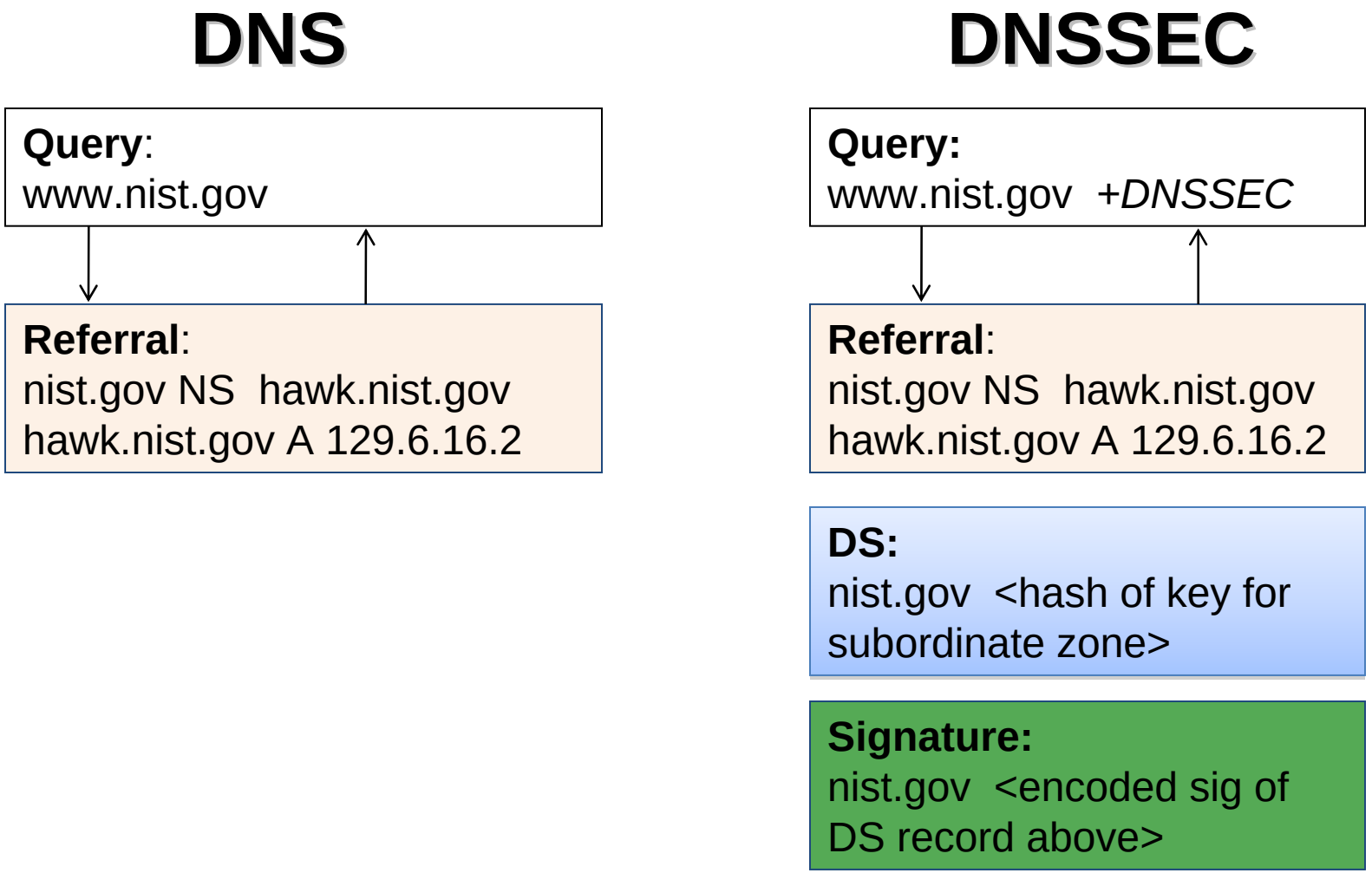
Implications of Security Attacks on the Domain Name System

- 1st order implications are clear:
  - 1st step in every instance of Internet communication.
  - Attacks can hijack/DoS services, machines, zones.
- There are 2nd order implications of the implicit trust model that is based upon this insecure basic service:
  - Exploiting the DNS is a tool in undermining what we think of as “trusted” services.
    - CA validations, SSL connections, on-line authentication factors.
  - Sophistication of attacks increasing as are their risks.

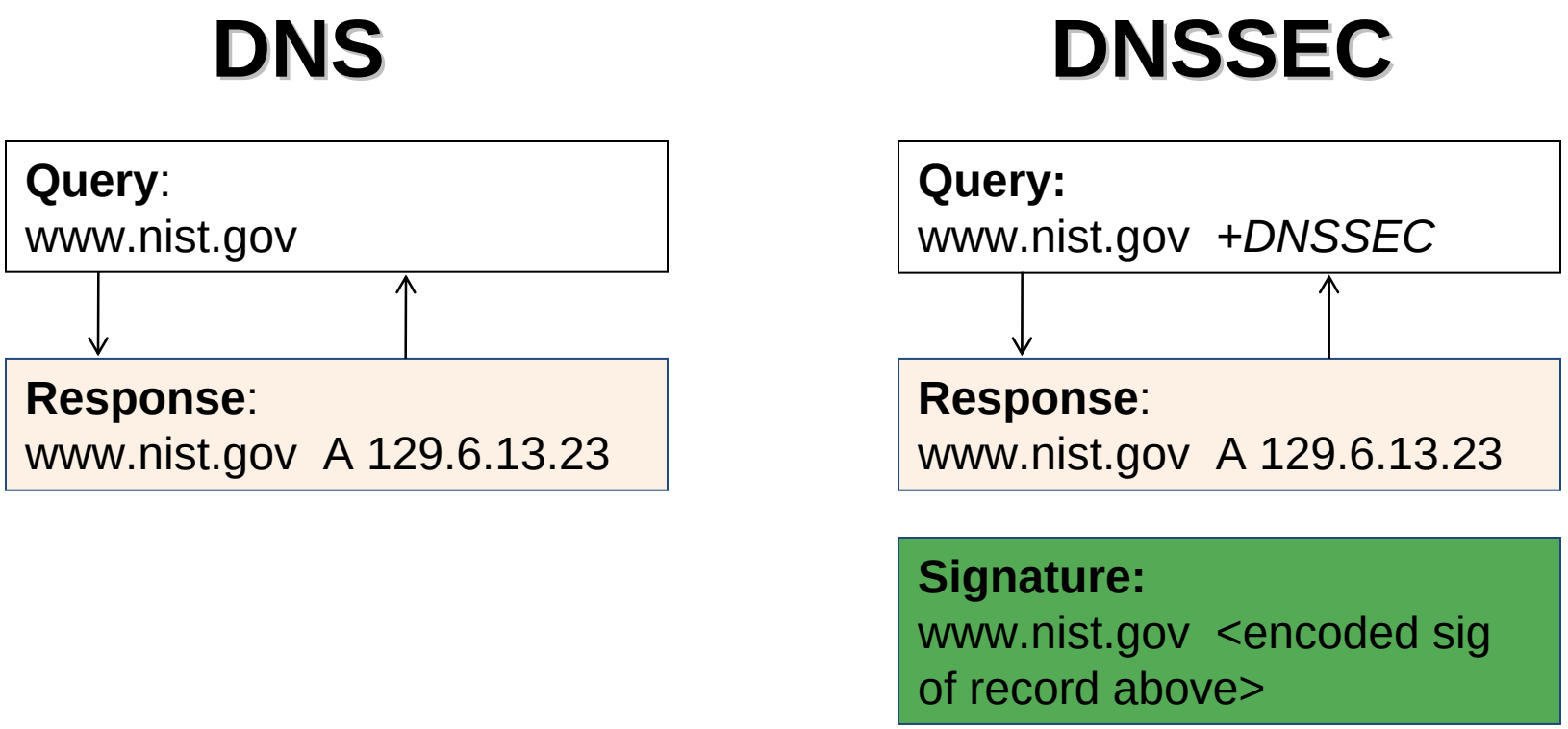
DNS Security Extensions

- DNSSEC Standards:
  - Open, consensus, international IETF standard extensions to **add** basic security mechanisms and trust models to the DNS.
  - Adds digital signatures to DNS data.
    - Source authentication and Data integrity
  - Incremental deployment model on current DNS infrastructure.
  - Enables establishment verifiable “chain of trust” between parent and child zones.
  - Requires establishment / management of “trust anchors” to boot strap the process.

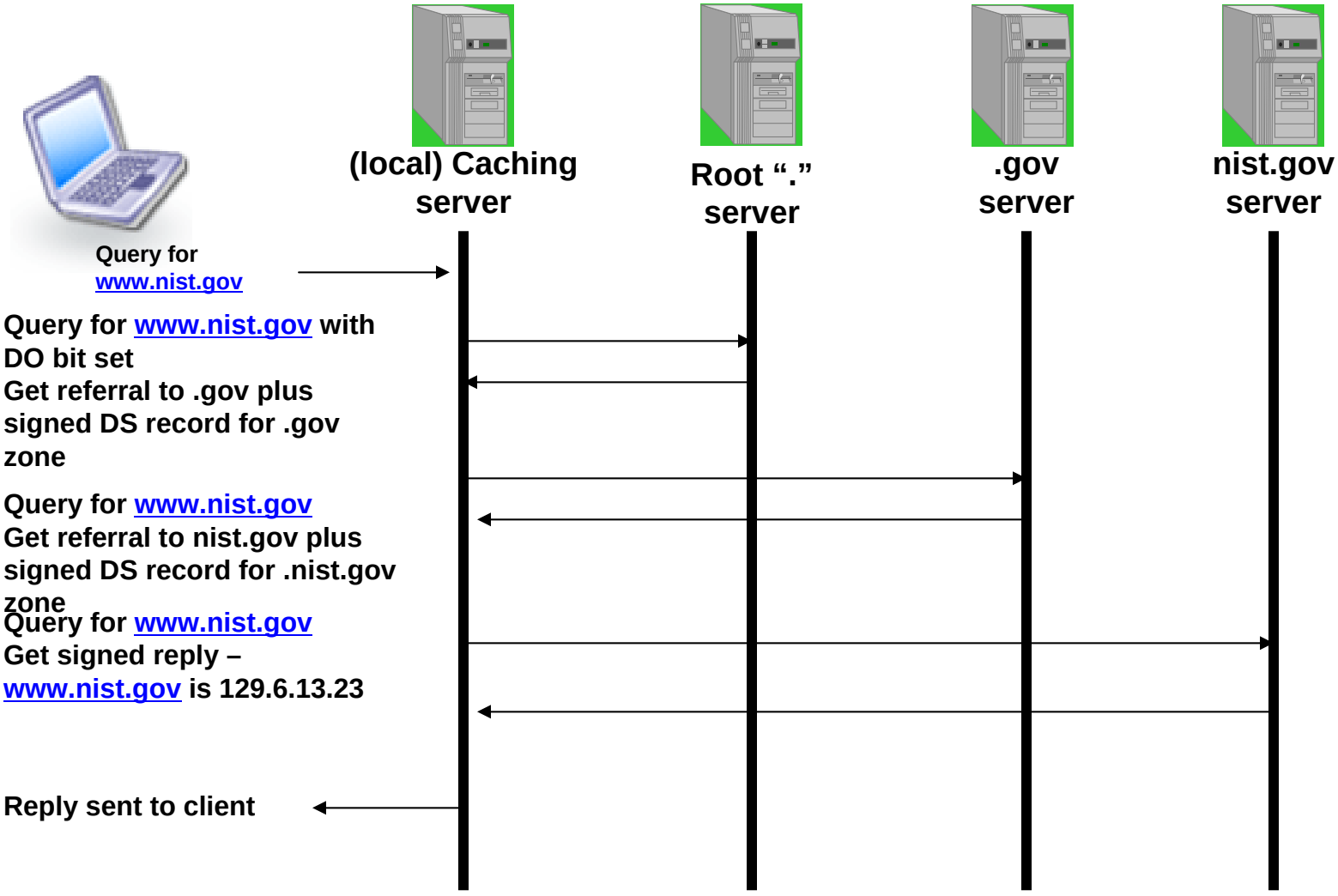
DNS Referral + DNSSEC



DNS + DNSSEC


DNS
Query:
www.nist.gov
Response:
www.nist.gov A 129.6.13.23
DNSSEC
Query:
www.nist.gov +DNSSEC
Response:
www.nist.gov A 129.6.13.23
Signature:
www.nist.gov <encoded sig of record above>

DNSSEC Query (Full Deployment)



Note: Caching server may need to make additional queries for any missing DS or DNSKey records

Services Provided by DNSSEC

- **Source Authentication**
  - Verify that DNS response data is from authoritative server / source.
- **Integrity Protection**
  - Verify that DNS response data was not altered since signing.
- **Authenticated Denial of Existence**
  - Verify that a Name does not exist in the DNS – and the owner of that zone can prove it.
- All aimed to protect the end user system

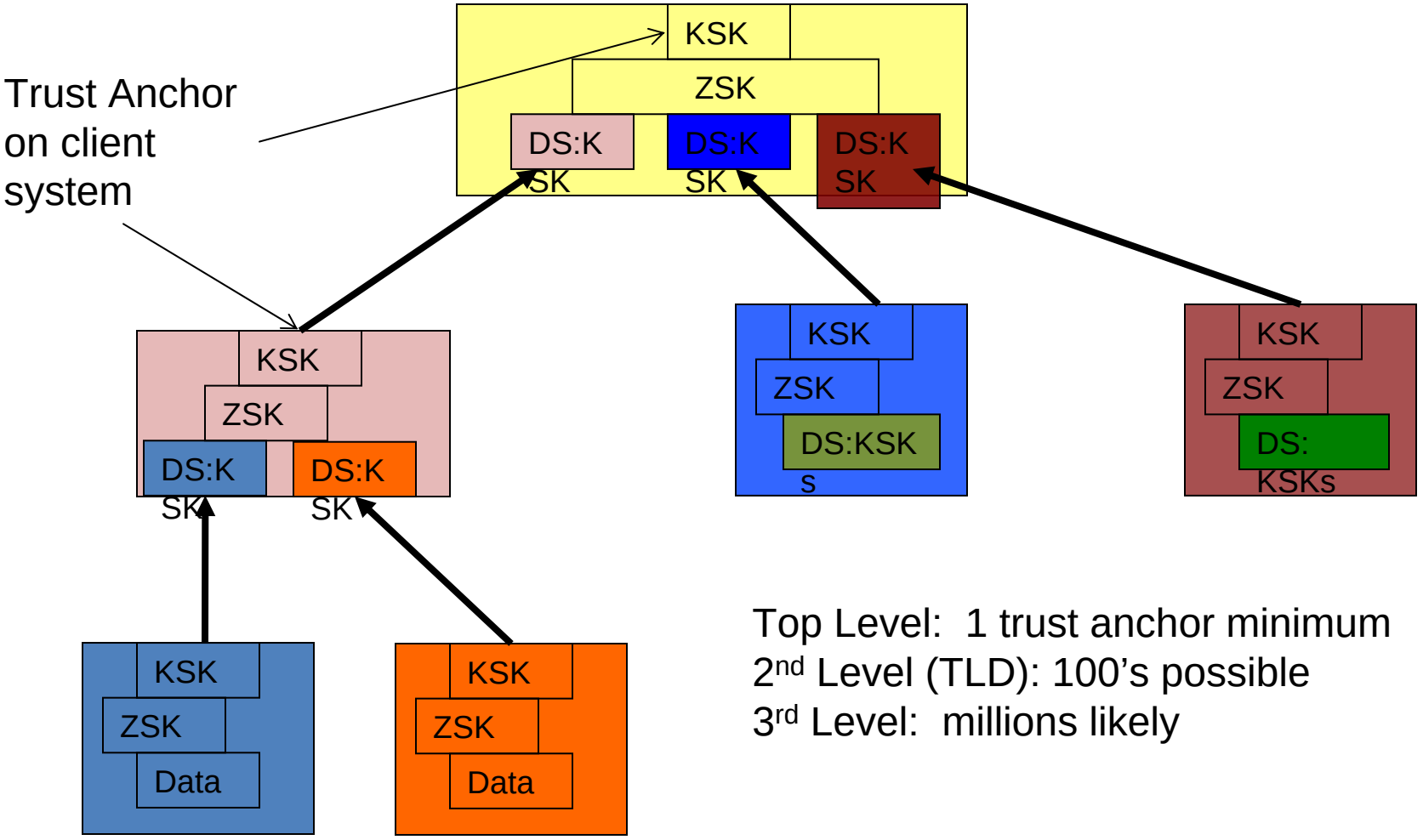
Services *Not* Provided by DNSSEC

- Confidentiality
  - DNS data is not encrypted
- DoS prevention at the server
- User/Service authentication
  - Just DNS data
- A poor man’s PKI

DNSSEC and Key Roles

- DNSSEC relies on Public Key Cryptography
  - Each zone has its own key pair(s)
- Types of DNSSEC of keys
  - (does not matter to the protocol – just administration and policy)
  - Zone Signing Key (ZSK) – key that signs DNS data
  - Key Signing Key (KSK) – key that signs the DNS keys and used to link trust from parent to child zones
- Key Management
  - Keys can be locally generated. Private key is guarded secret, public is shared with the world.
  - The owners of these two keys can be distinct
  - KSK can be thought of as the “Master Key” that authenticates the data signing key (ZSK)

Chaining of Keys in DNSSEC



Top Level: 1 trust anchor minimum
2nd Level (TLD): 100's possible
3rd Level: millions likely

DNSSEC is an Opt-in Technology

- DNSSEC can – and is – being deployed piecemeal in the DNS today
  - nist.gov has been signed for years
  - A number of TLDs (mostly country codes) have already turned on DNSSEC
- However, taking full advantage of these “islands” of DNSSEC would require hundreds of trust anchors
  - So few systems request signed records

Why we need DNSSEC at the Root

- Really a question of trust anchor management
  - If all TLDs were signed and root zone is unsigned, 250+ trust anchors to manage in each client
  - Worse if more TLD's are added, or if TLD is unsigned but subordinate zones deploy DNSSEC
- Root zone is top of the DNS (and therefore DNSSEC) hierarchy
  - Already a degree of trust in the root zone

Deploying DNSSEC in the Authoritative Root Zone

- Proponents of DNSSEC assert that widespread deployment of the protocol would mitigate many of the vulnerabilities currently associated with the DNS, increasing the security and integrity of the Internet DNS in a scalable fashion.
- Ubiquitous deployment of DNSSEC would also enable authentication of the hierarchical relationship between domains to provide the highest levels of assurance.
- Thus, to realize the greatest benefits from DNSSEC, there needs to be an uninterrupted chain of trust from the zones that choose to deploy DNSSEC back to the authoritative root zone.
- The Department of Commerce concluded a Notice of Inquiry (NOI) in November 2008 that indicated almost unanimous consensus for DNSSEC implementation at the root zone level as soon as possible in a manner that maintains the security and stability of the DNS

Deploying DNSSEC in the Authoritative Root Zone

- The U.S. Government remains committed to preserving the security and stability of the Internet DNS.
- Timely deployment of DNSSEC at the root zone level is consistent with this commitment.
- To that end, the U.S. Department of Commerce intends to work with the Internet technical community through a transparent and collaborative process to develop requirements and a testing plan that will permit DNSSEC to be implemented and a signed root operational by the end of 2009.

Questions?