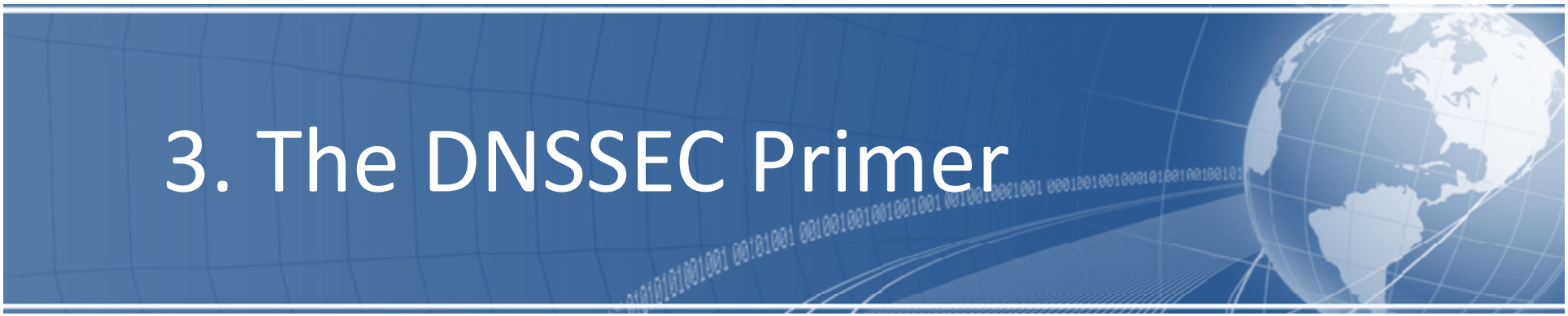
3. The DNSSEC Primer



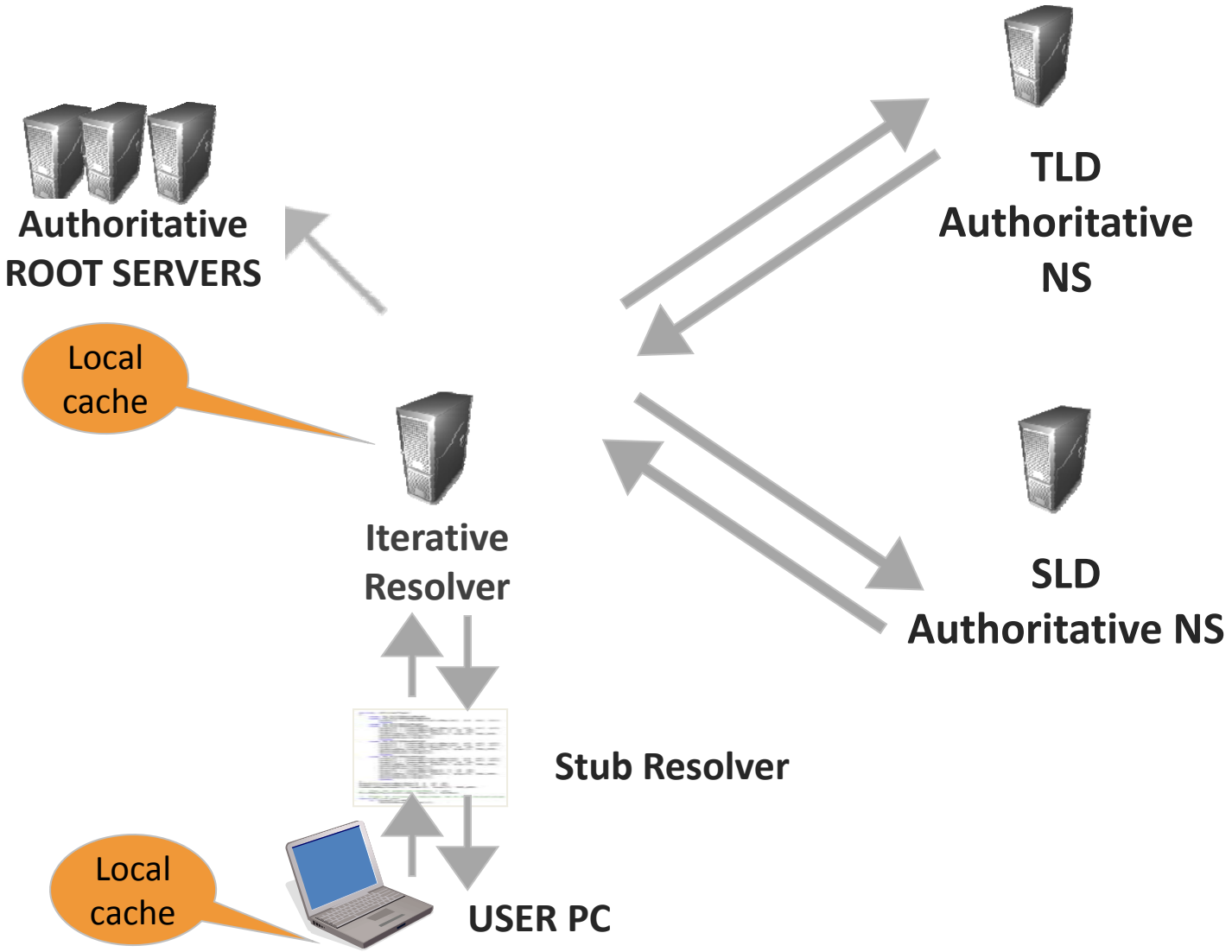
Authentication (keys, signatures)

Data Integrity (hashes)

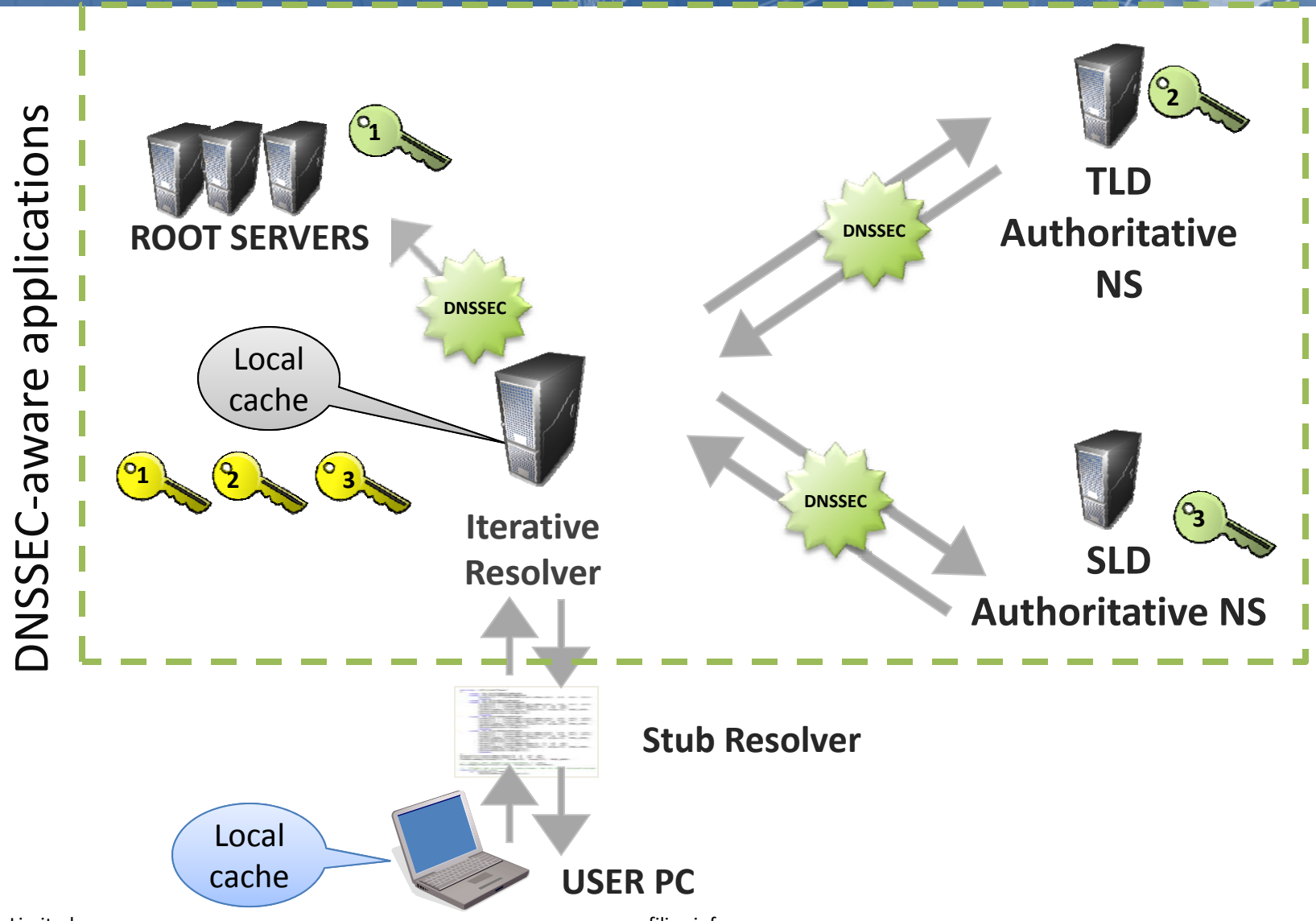
Chain of Trust (root zone, when signed)

Authenticated Denial of Existence (NSEC, NSEC3)

DNS



DNS with DNSSEC



Authentication

1

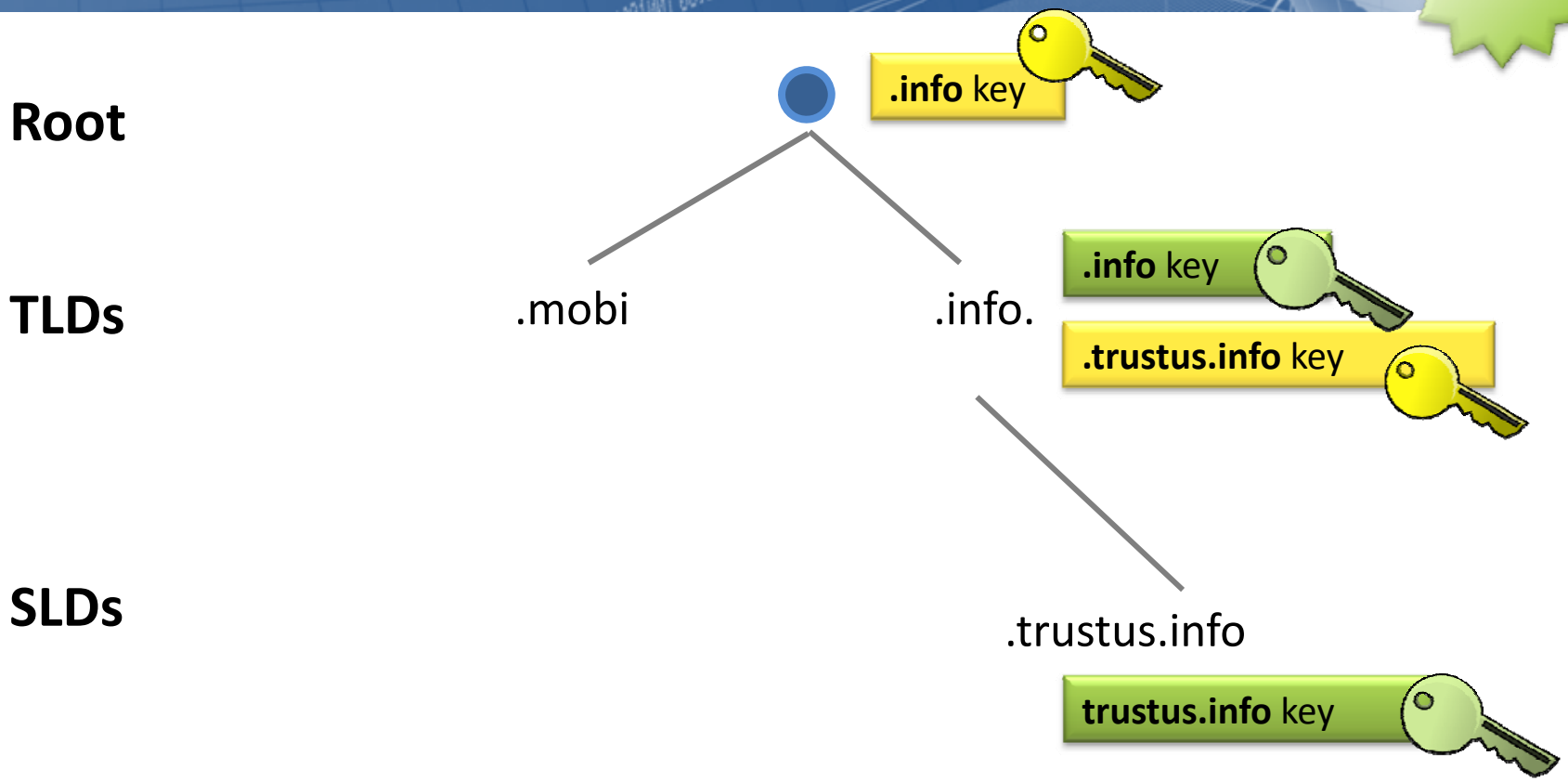
Authentication

*Originator signs using own **private** key*

DNS Response

*Recipient authenticates response with **public** key of originator*

Where are the keys?



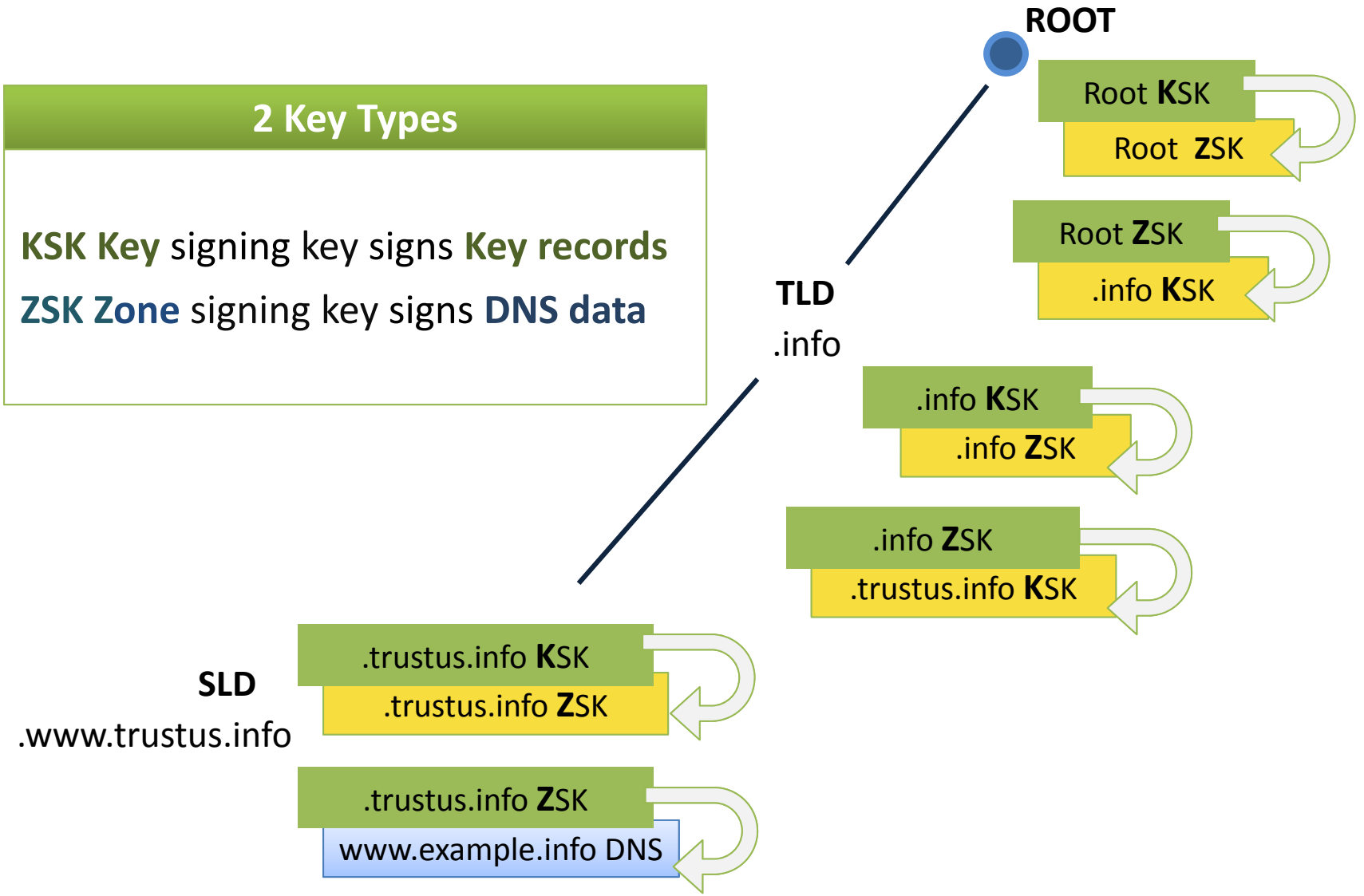
Key information (digest, not actual key)
held by parent level in hierarchy

DNSSEC key types

2 Key Types

KSK Key signing key signs **Key records**

ZSK Zone signing key signs **DNS data**



Chain of trust

The Chain of Trust

If I trust a **public key**,
I can use that key to:

1) **validate** the signature and

2) **verify** the data

- **Root zone** key
  - Must be trusted
  - Root zone pointers point to lower zones
  - Each pointer is validated with the previous validated zone key
- **Parent zone** key
  - Extends chain of trust
  - Root zone key binds TLD key to TLD name
  - TLD key binds SLD key to SLD name

Integrity

Authentication

*Originator signs using own **private** key*

DNS Response

*Recipient authenticates response with **public** key of originator*

2 Integrity

*Originator **hashes** DNS response*

*Originator **signs** hash using own **private** key*

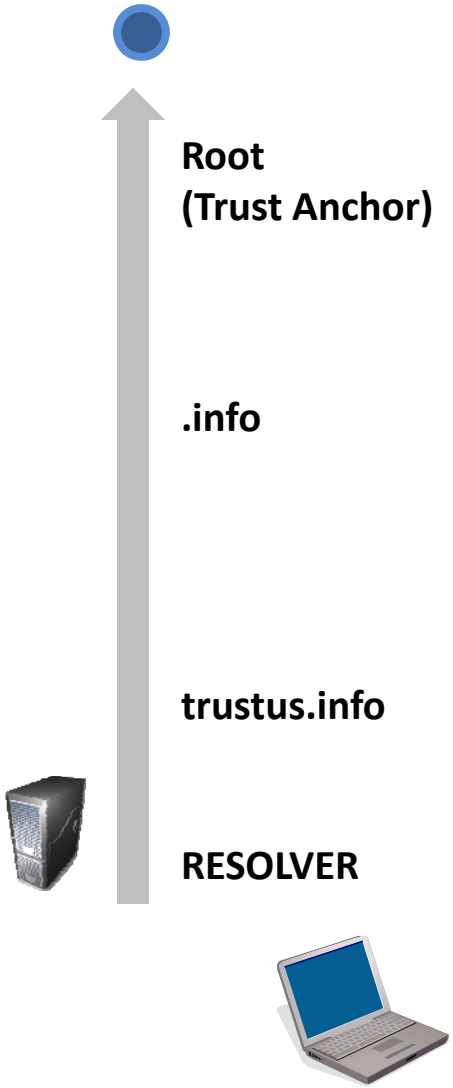
DNS Response

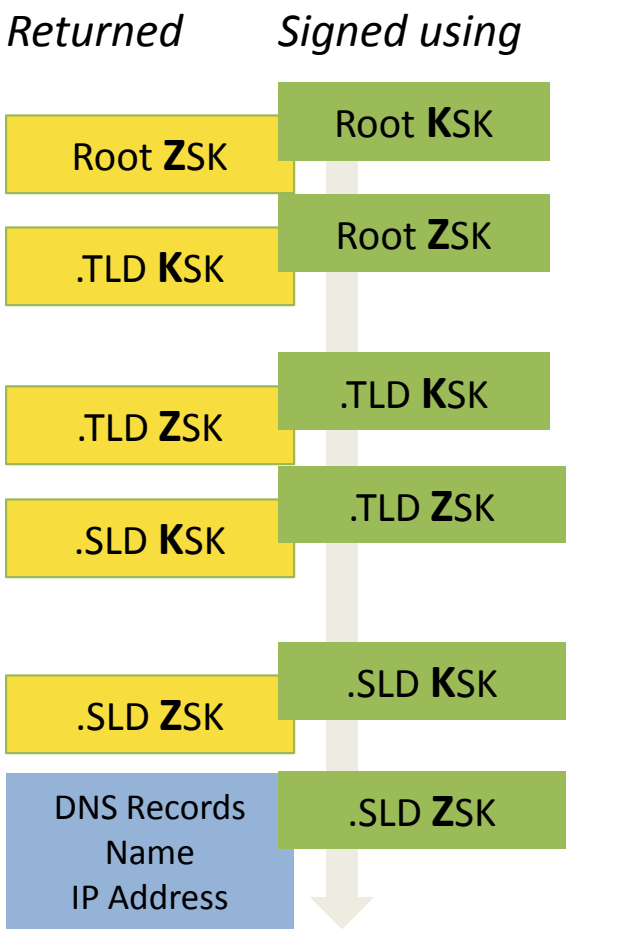
*Recipient **recomputes** hash of response*

*Recipient uses **public** key of originator to **retrieve** hash*

*Recipient compares computed hash to received hash to **validate** response*

Data integrity in practice





Name
IP Address

or

Does NOT Exist

DNSSEC security

Authentication

*Originator signs using own **private** key*

DNS Response

*Recipient authenticates response with **public** key of originator*

Integrity

*Originator **hashes** DNS response*

*Originator **signs** hash using own **private** key*

DNS Response

*Recipient **recomputes** hash of response*

*Recipient uses **public** key of originator to **retrieve** hash*

*Recipient compares computed hash to received hash to **validate** response*

3

Denial of Existence

*Originator signs NSEC or NSEC3 record using own **private** key*

DNS Response

*Recipient authenticates response with **public** key of originator*

Resolution with authenticated denial of existence

- Asserts that a name does not exist in the zone
- NSEC
  - For smaller zones
  - Better performance (speed, not footprint)
- NSEC3
  - Prevent zone walking
  - Domains Opt-In

4. Key Management Primer

Focus on key rollovers

Key management

- Creation
  - Typically handled by implementation choice
  - Important to have a good source of randomness
- Storage
  - Private key must be protected
  - Typically not archived
- Access Control
  - Usage of private key must be controlled
- Rollover

What is a key rollover?

- A key rollover will occur whenever the key owner needs to change its key pair
- When a key rollover occurs:
  - Data must be re-signed with new private key
  - Everyone will need to update their validating resolvers with the new public portion of the key

Why perform a key rollover?

1. As a best security practice
2. Revoke a compromised private key
3. To mitigate attacks on a private key

Key rollover types

1. **Planned**: publish schedules*
2. **Unplanned**: move unexpectedly to “on deck” key; announced as it happens; revoke old key
3. **Emergency**: a newly created key that has not yet been distributed

- Only approximately—consider jitter and other variables

Best practice
Always have two sets of a keys: one active and one “on deck”

DNSSEC recap

- Extends DNS (but backward compatible)
- Adds **digital signature** to each block of response
  - For proof of origin
- Adds a **hash**
  - Proof that the data has not been modified in transit
- Largest operational impact is on zone operations
  - For example, key rollovers

DNSSEC **does not** encrypt data

DNSSEC resources

- Afilias DNSSEC
  - http://afilias.info/dnssec
- The Domain Name System Security Extensions
    - RFC 4033: DNS Security Introduction & Requirements
    - RFC 4034: Resource Records for the DNS Security Extensions
    - RFC 4035: Protocol Modifications for the DNS Security Extensions
- DNSSEC Coalition
  - http://www.dnsseccoalition.org
- Root signing:
  - http://www.root-dnssec.org