# DNSSEC

**Understanding DNSSEC…**

Nicolas Antoniello

ISPCP
December 2024

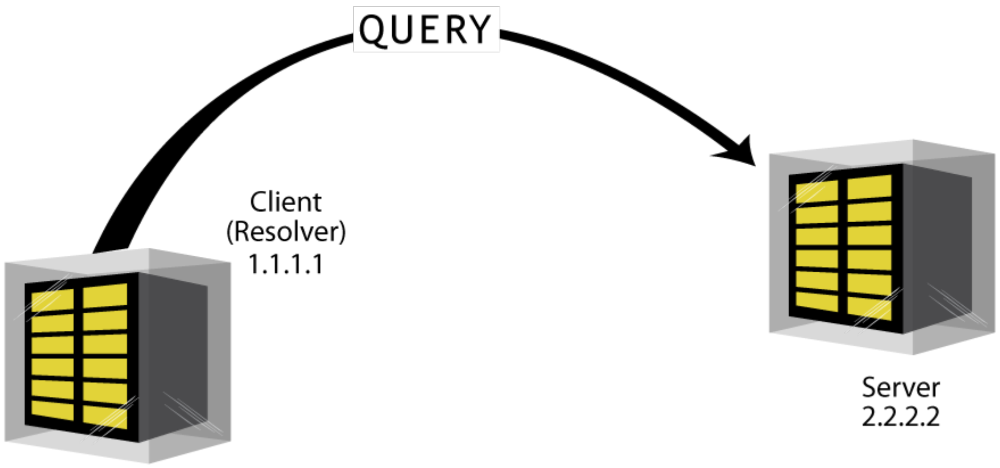
ICANN

# A world without DNSSEC…

ICANN

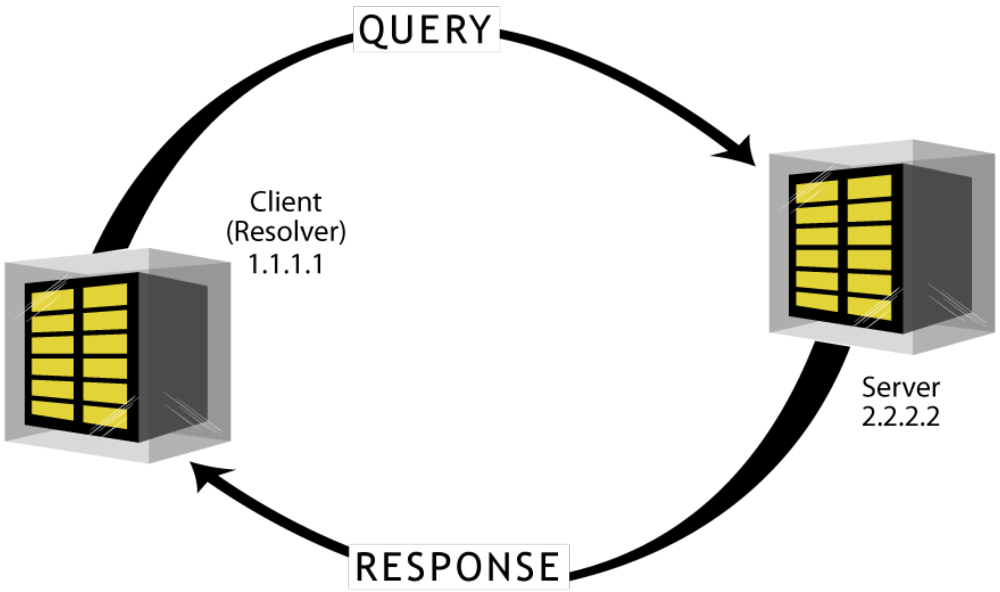
# DNS and Lack of Security

- One packet for a DNS query, one packet for a DNS response



# DNS and Lack of Security

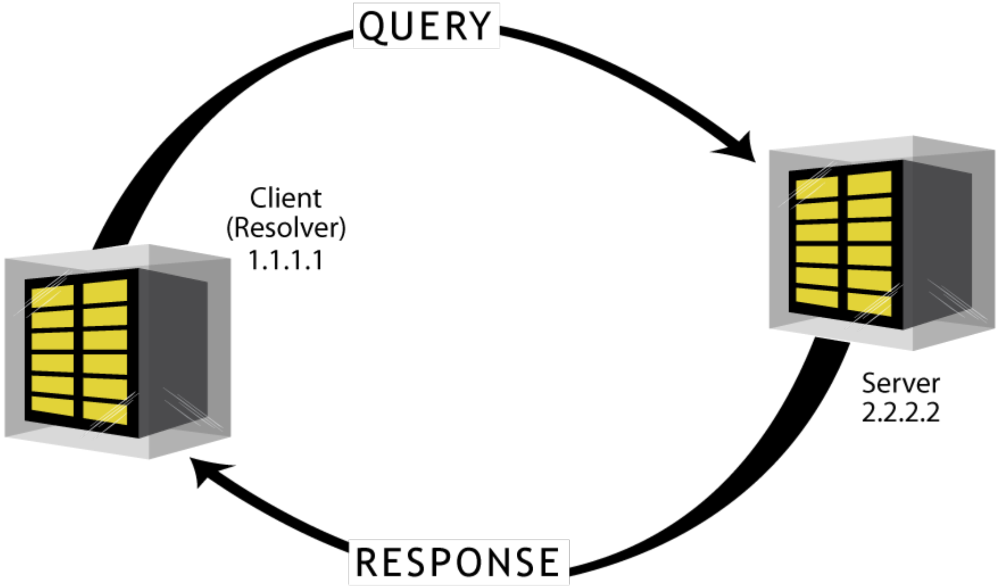
- One packet for a DNS query, one packet for a DNS response



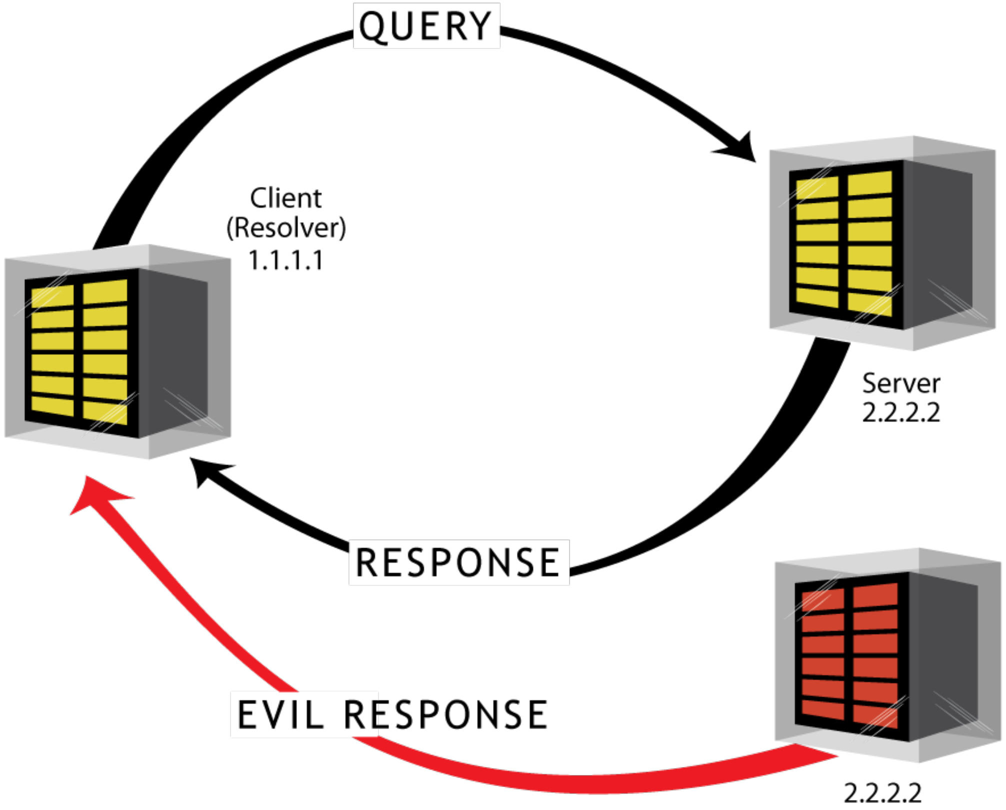
# Who are you *really?*

- Client has to trust the source address of the server
- But source addresses can be faked or “spoofed”

# Who are you *really?*



# Who are you *really?*



# A few cryptography basics …

ICANN

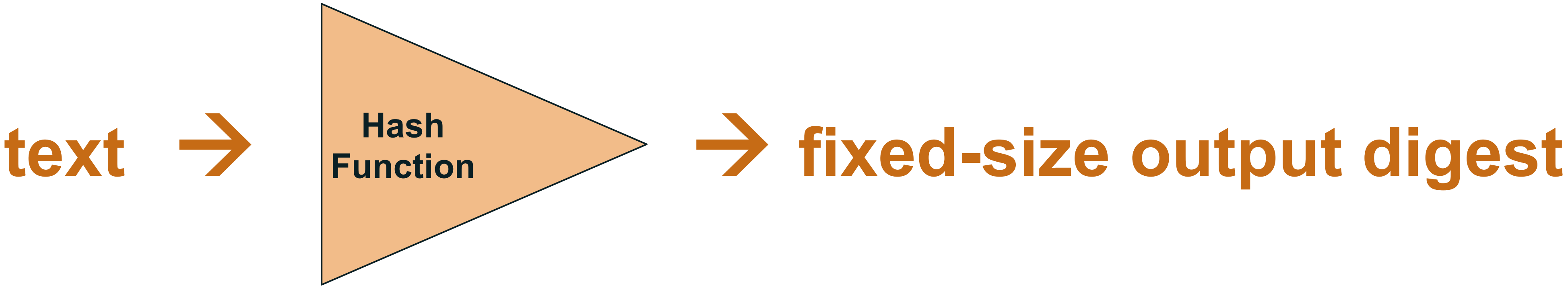
# Some Cryptography Basics

- With public key cryptographic algorithms, keys come in pairs: a **public key** and a **private key**
  - Data *encrypted* with the public key can be *decrypted* with the private key
  - Data *signed* with the private key and be *verified* with the public key
  - Example public key algorithms:
    - Oldest and most widely used is RSA
    - Newer algorithms based on elliptic curve cryptography (ECC), such as ECDSA, EdDSA and several others

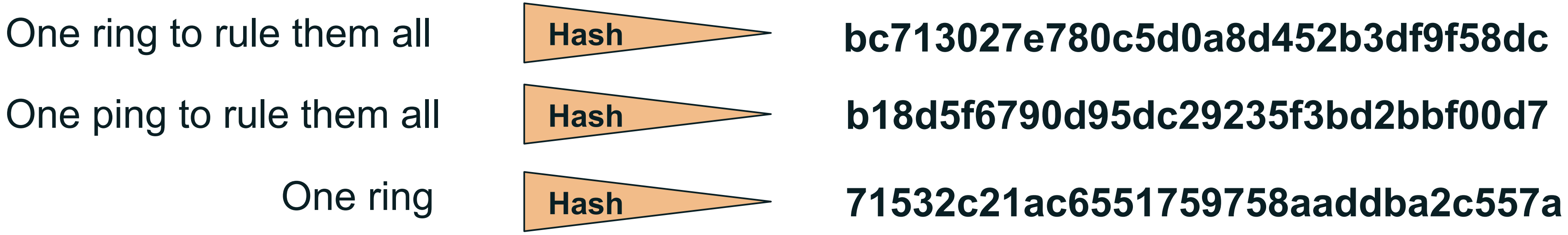
- A **cryptographic hash algorithm** produces a fixed-size output called a **hash** or **digest** for any size input
  - No two inputs produce the same output
  - The hash is therefore similar to a “fingerprint” of the document
  - Example cryptographic hash algorithms: SHA-256, SHA-1 (older), MD5 (even older)

# Hash Function

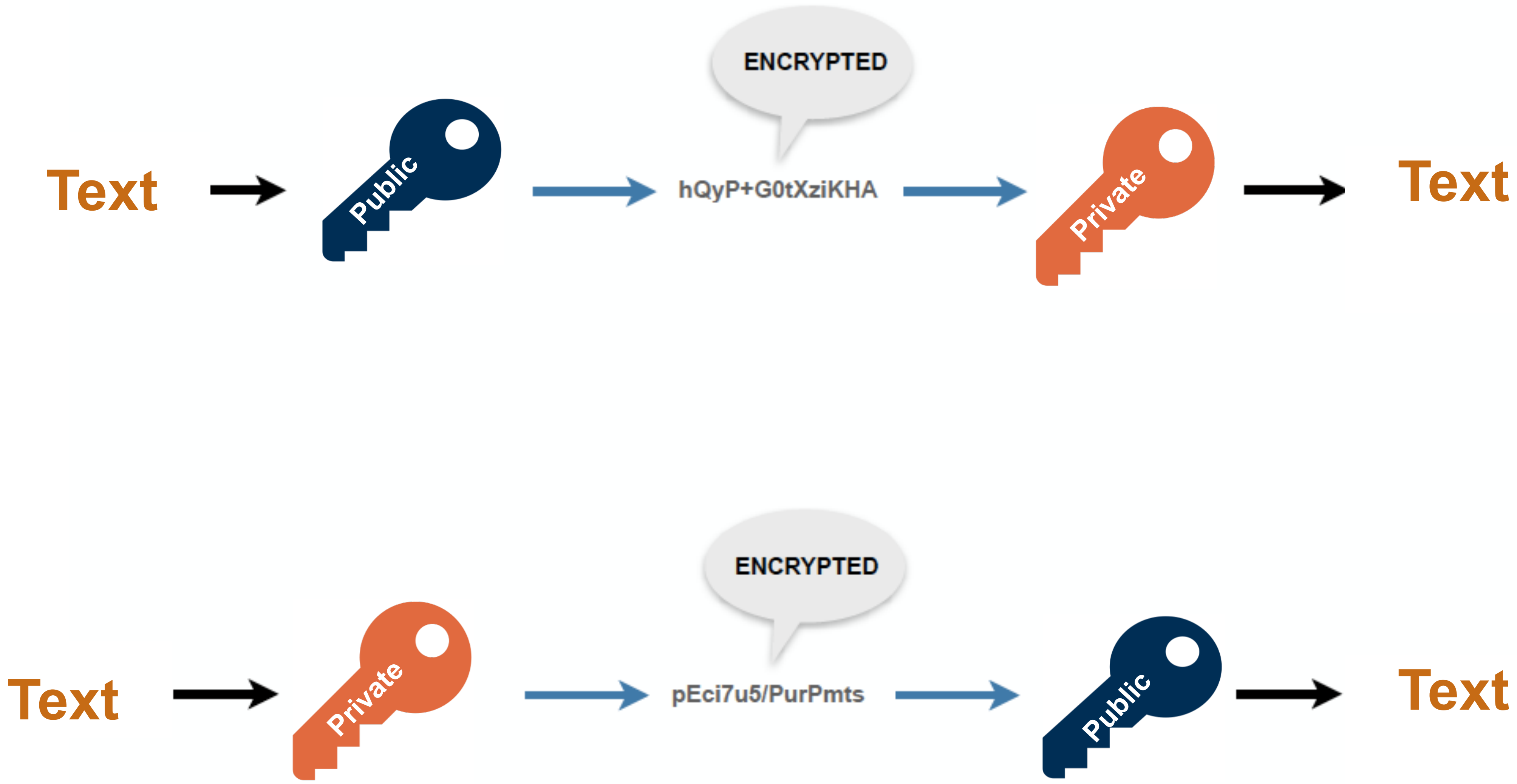
- A cryptographic hash algorithm produces a fixed-size output (fingerprint) called a hash or digest for any size input.




Example of MD5 digests (an MD5 hash is created by taking a string of an any length and encoding it into a 128-bit fingerprint):



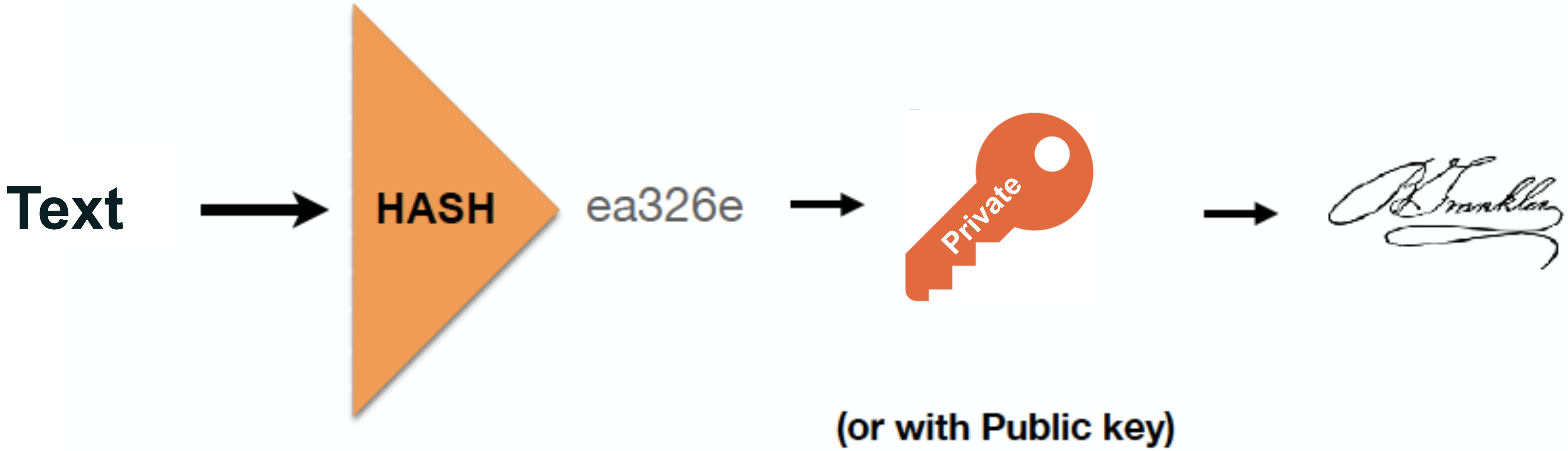
# Private and Public Keys



# Digital Signature

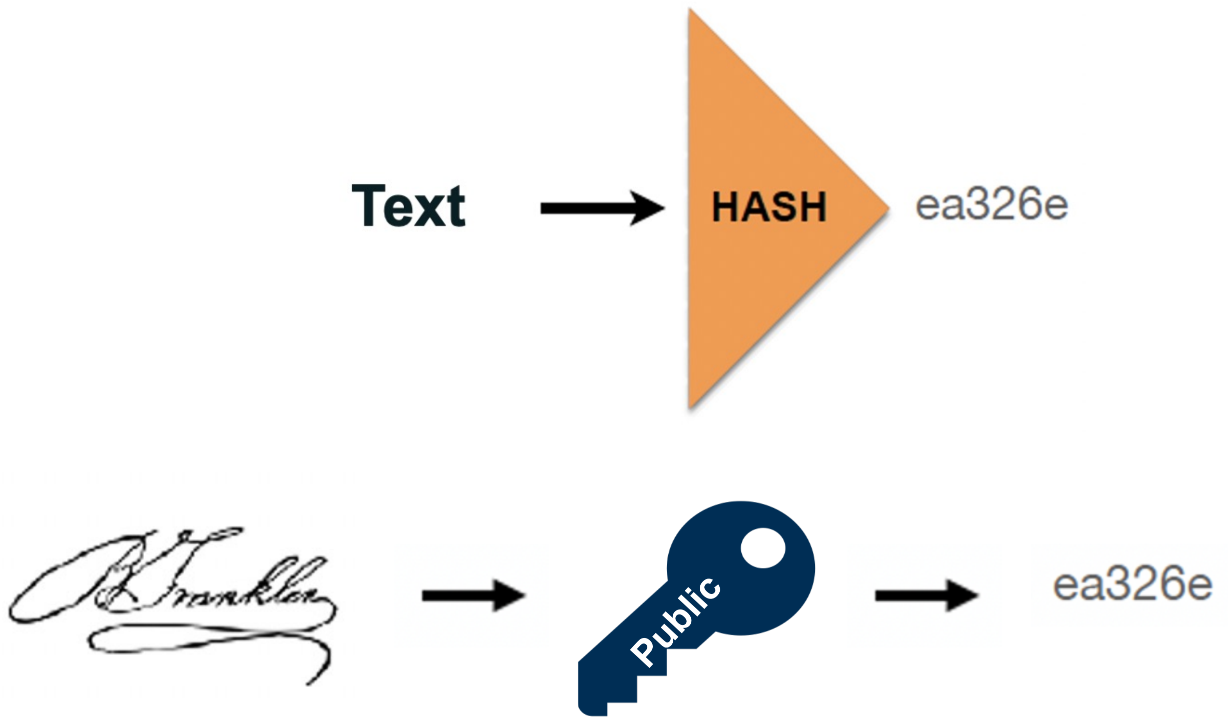
- We may combine *hash* with *private and public key*, to obtain a digital signature of any text

**Hashing + Encrypt = Digital Signature**



# Digital Signature

- To verify the digital signature I need the ***text*** and the ***public key*** (or *private key* if signed with *public key*)

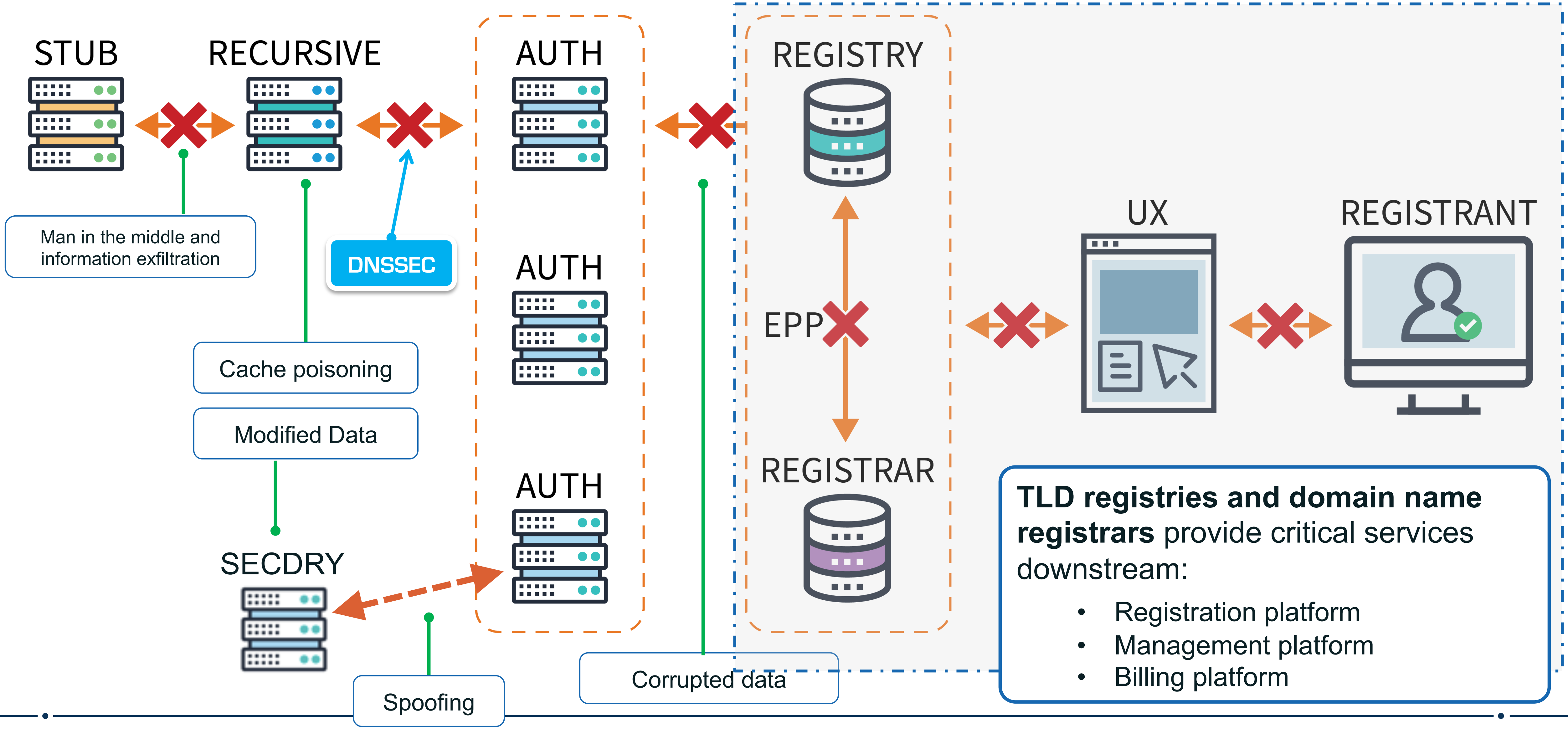



**(or with private key)**

# So, DNSSEC ?

## Fasten your seatbelts …

# DNS Threats @DNS ecosystem




**TLD registries and domain name registrars** provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

ICANN

# What DNSSEC Does

- DNSSEC uses public-key cryptography and digital signatures to provide:
  - Data origin authentication
    - "Did this response really come from the *example.com* zone authority?"
  - Data integrity
    - "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"
- DNSSEC offers protection against spoofing of DNS data (and so, for attacks like cache-poisoning, etc.).

# What DNSSEC Doesn't Do

- **DNSSEC does not**:
  - Provide any confidentiality for DNS data
    - No encryption.
    - Transferred data will be readable for person-in-the-middle.
  - Address attacks against DNS software
    - DDoS
    - “packets of death”
    - Etc.

# DNSSEC Signing

## DNSSEC enabled authoritative explained …

# Signing DNS Data

- In DNSSEC, each zone has a public/private key pair
- Data in the zone is signed with the private key
  - Signing the data is usually de-coupled from serving the data
  - The design allows data to be signed ahead of time rather than “on the fly” for each response
- Important: In DNSSEC, DNS *data* is signed, not DNS *messages*
  - Signing messages is called transaction security
  - A separate protocol called TSIG handles that

# Zone Key Pairs

- The zone's public key is published in the zone in a specific record.
- The zone's private key is kept safe:
  - The amount of protection required depends on how the zone owner evaluate the risks involved in case the private key is disclosed or compromised.
- Options for protecting a zone's private key:
  - Stored on-line in some encrypted form, only decrypted when needed for signing data
    - The minimum.
  - Stored offline also in some encrypted form
    - Offers more protection.
  - Stored in a hardware security module (HSM)
    - Offers the most protection but overkill (may also be costly) for many applications.

# Recalling Resource Records (RR)

- Data associated with domain names is contained in Resource Records.

  - **A** IPv4 address
  - **AAAA** IPv6 address
  - **NS** Name of an authoritative name server
  - **SOA** “Start of authority”, appears at zone apex
  - **CNAME** Name of an alias to another domain name
  - **MX** Name of a “mail exchange server”
  - **PTR** IP address encoded as a domain name (for reverse mapping)

DNSSEC adds some others:

- DNSKEY
- RRSIG
- NSEC
- DS

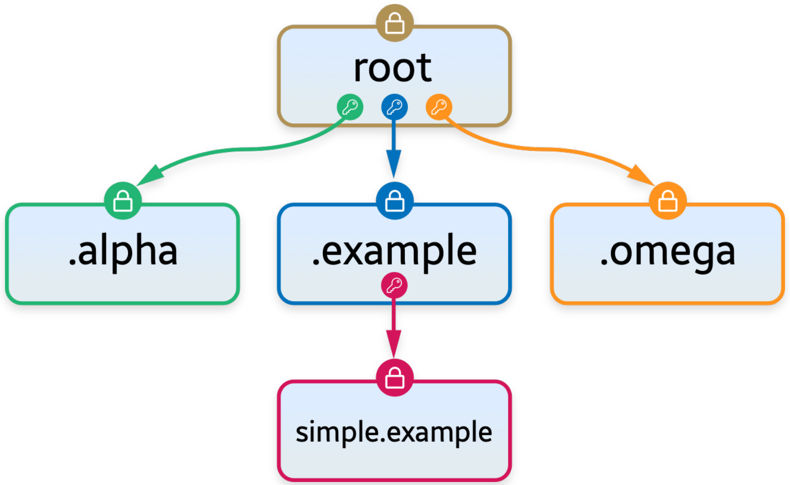
# New Resource Records

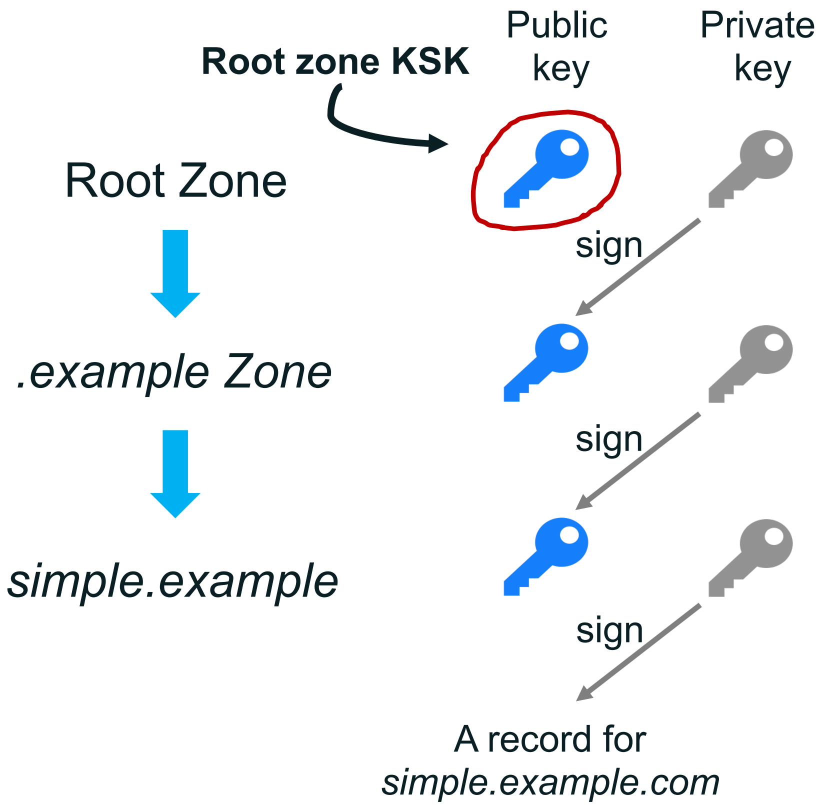
| | |
|---|---|
| **RRSIG** | Signed Resource Records |
| **DNSKEY** | Public Key |

# New Resource Records

**DS**

## Delegation Signer (Chain of Trust pointer)



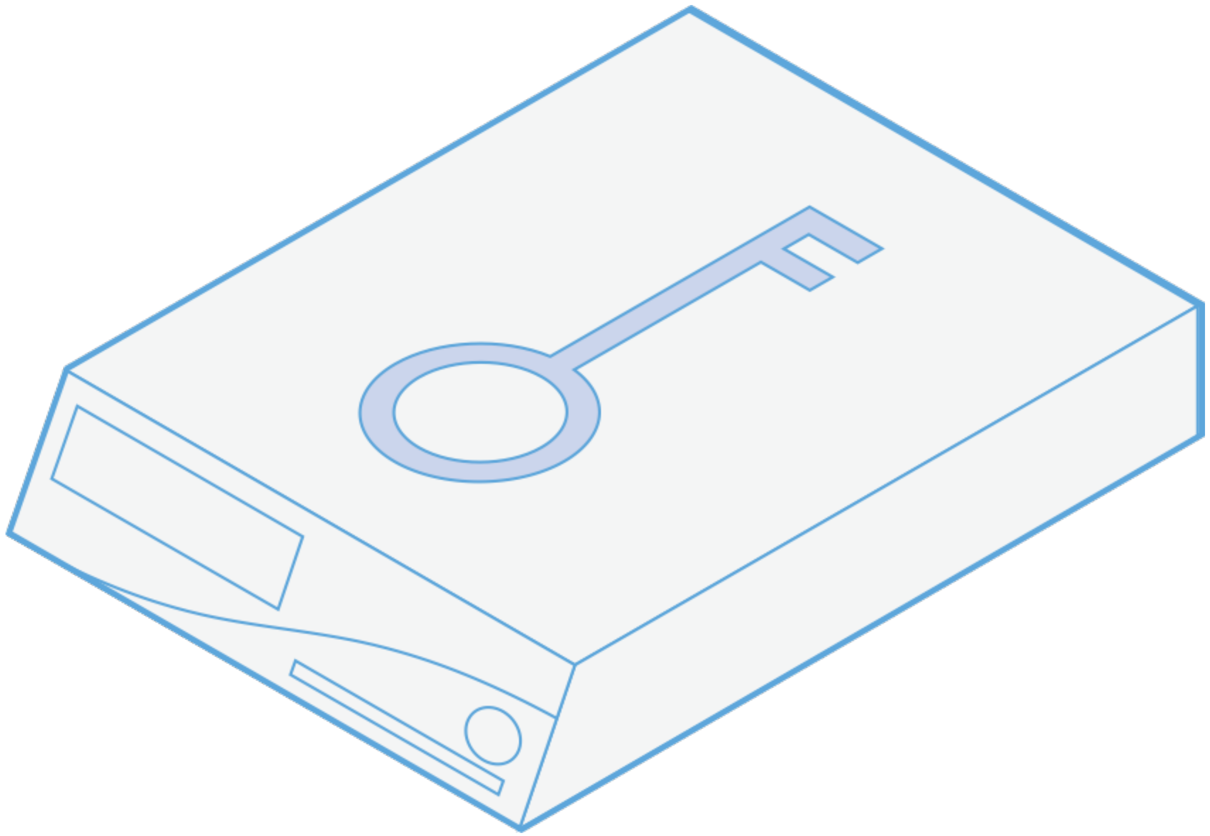




The mechanism for "trusting" the information needed to verify the digital signature of DNS information is based on each "parent" zone certifying the authenticity of said information about its "children". But… the Root zone has no parent. So we need a "trustworthy" mechanism to guarantee the authenticity of the Root's signature.

# Securing the “private” key for DNS Root signing…

# Security of the key to sign the Root

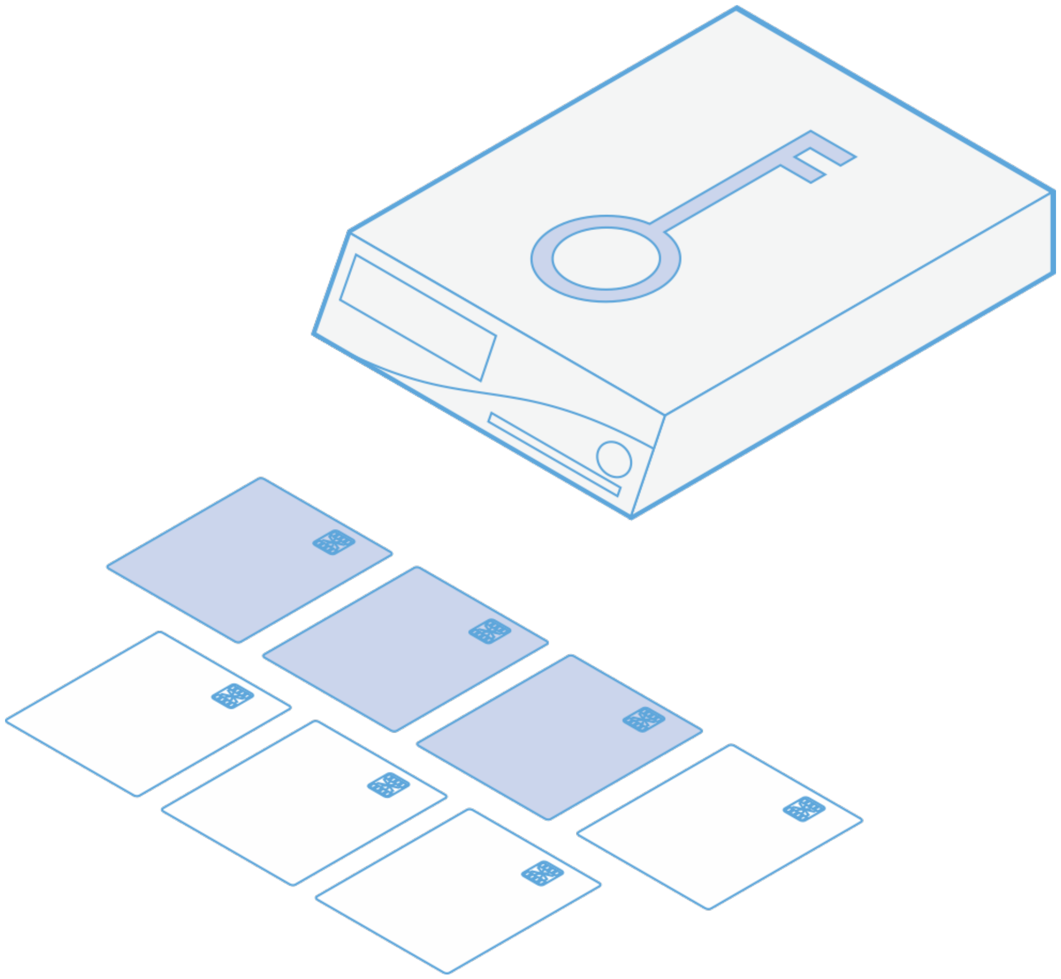
The key for signing the Root is stored in a device called a “hardware security module” (HSM) whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper-proof. If anyone tries to open it, the contents will self-destruct.



# Security of the key to sign the Root

There are seven smart cards that can activate each device. The device is configured so that 3 of the 7 smart cards must be present for it to be usable.

This means that if I do not have at least 3 of the 7 cards, I will not be able to access the contents of the device.

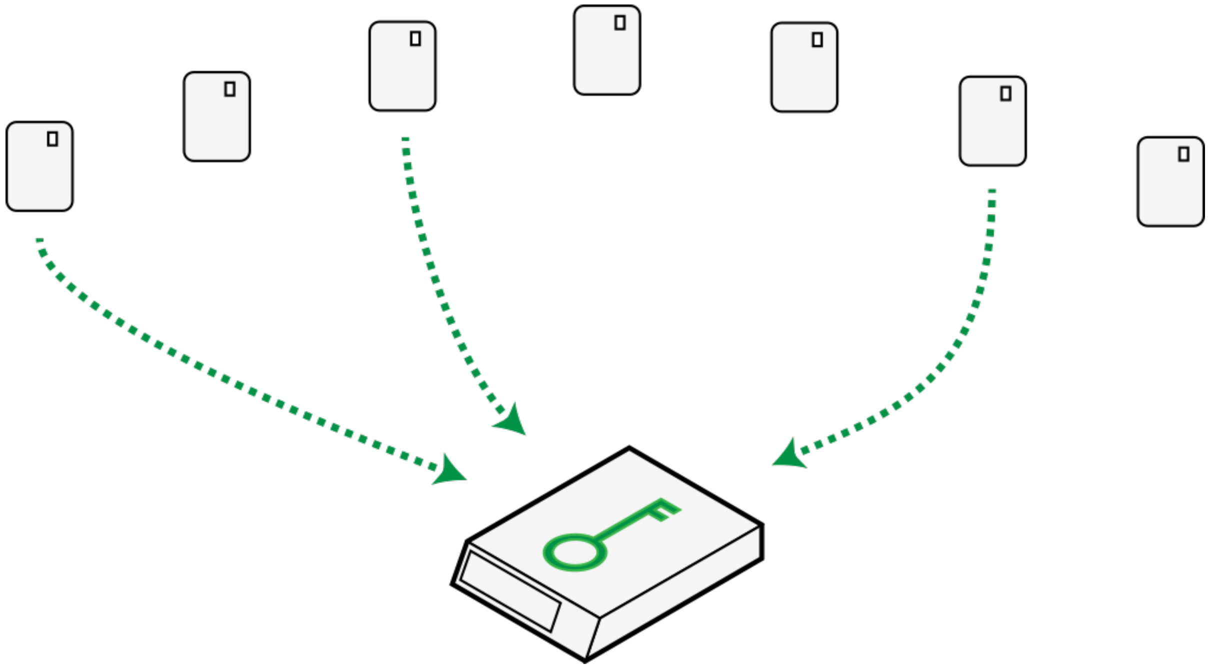


# Security of the key to sign the Root

Each smart card is assigned to a different member of the ICANN community, known as a “Trusted Community Representative” (TCR)

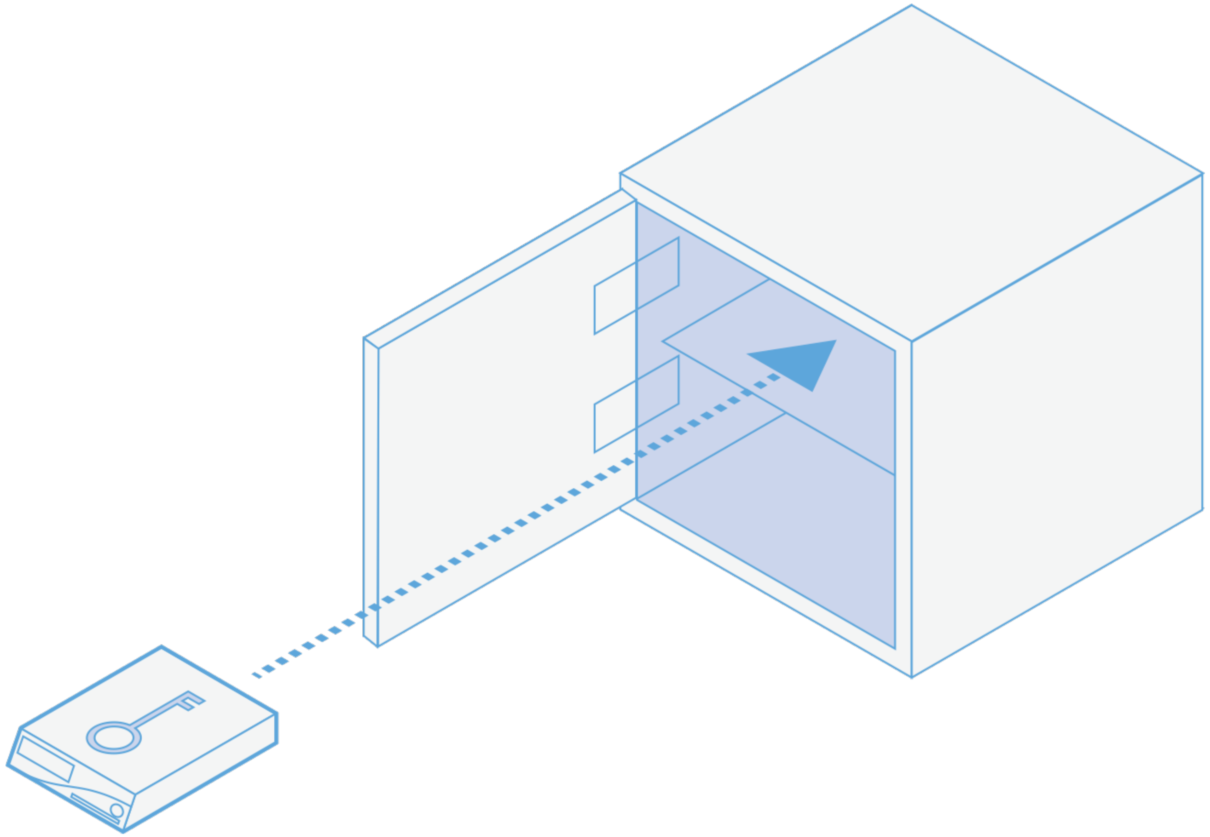
Therefore, to access the signing key, at least three of these TCRs must meet in person.

These planned events are called key signing ceremonies.



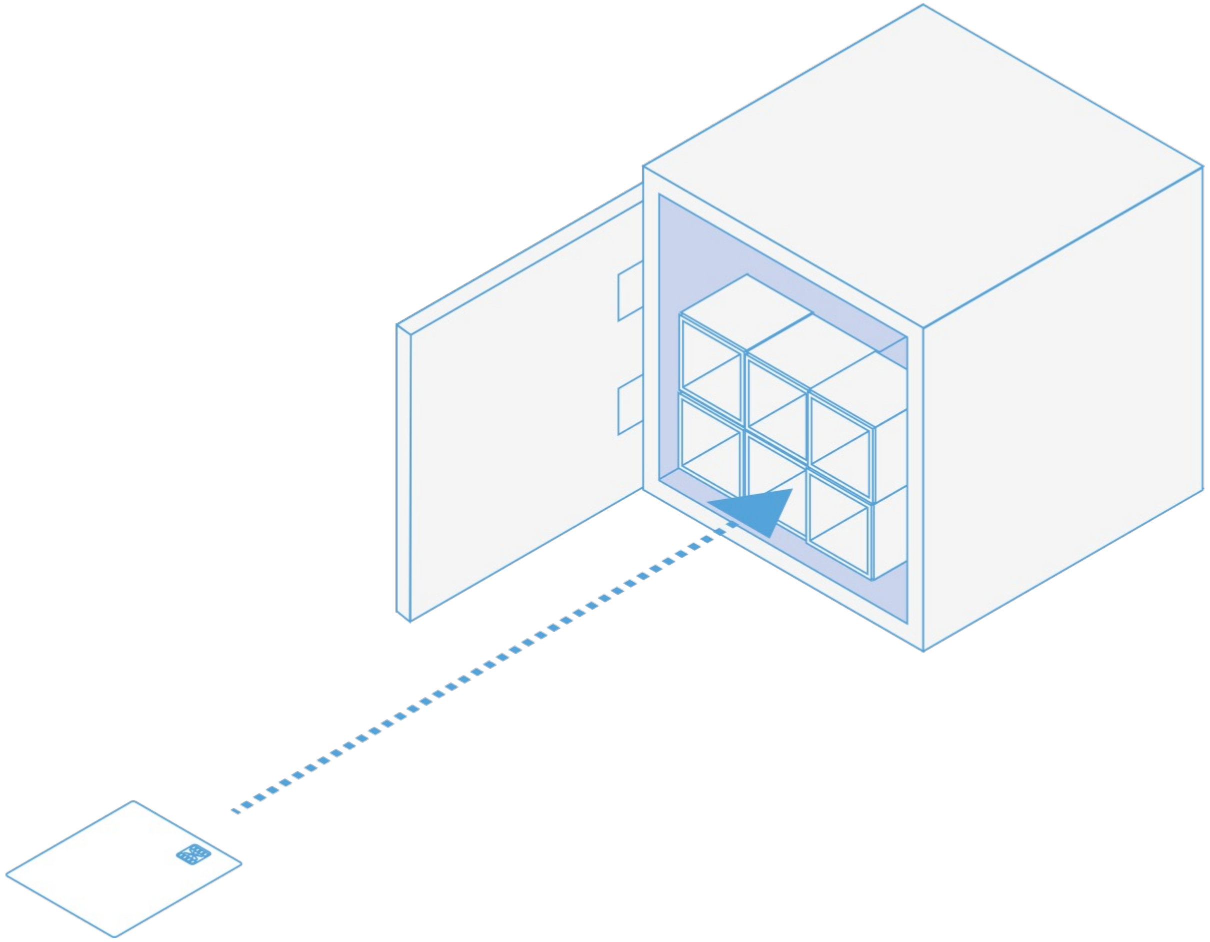
# Security of the key to sign the Root

The HSM is stored inside a high-security safe, which can only be opened by a designated person, the “safety controller”. The integrity of the safe is monitored with seismic and temperature sensors, among others.



# Security of the key to sign the Root

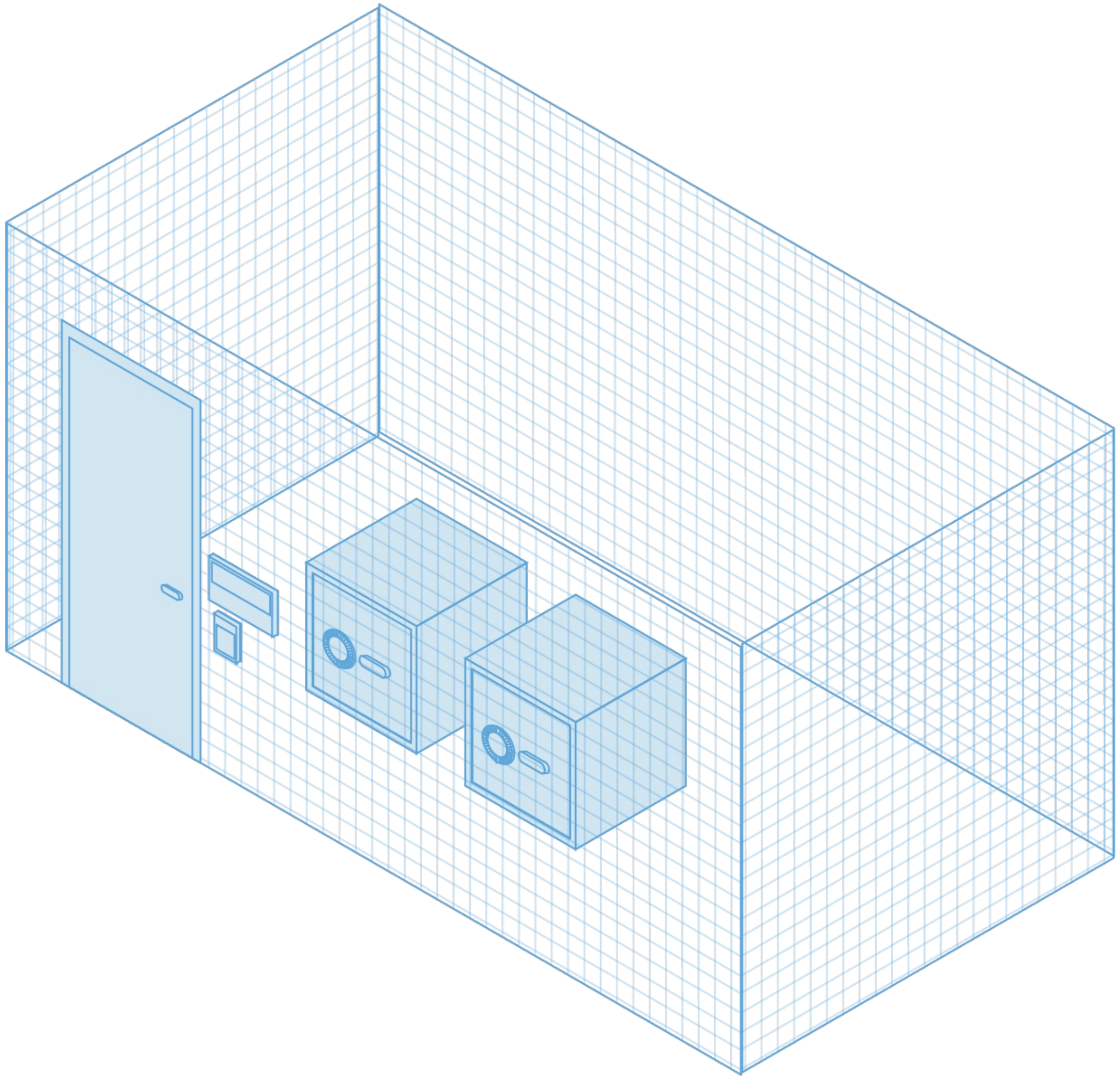
Each TCR's smart card is stored in a second credential safe containing a series of security boxes. Each security box is accessed by a mechanical key that the TCR carries with him or her and keeps secure between ceremonies.



# Security of the key to sign the Root

The two safes are kept in a secure, radio-frequency-isolated metal cage, which can only be opened jointly by two designated persons: the “administrator of the ceremony” and the “internal witness.”

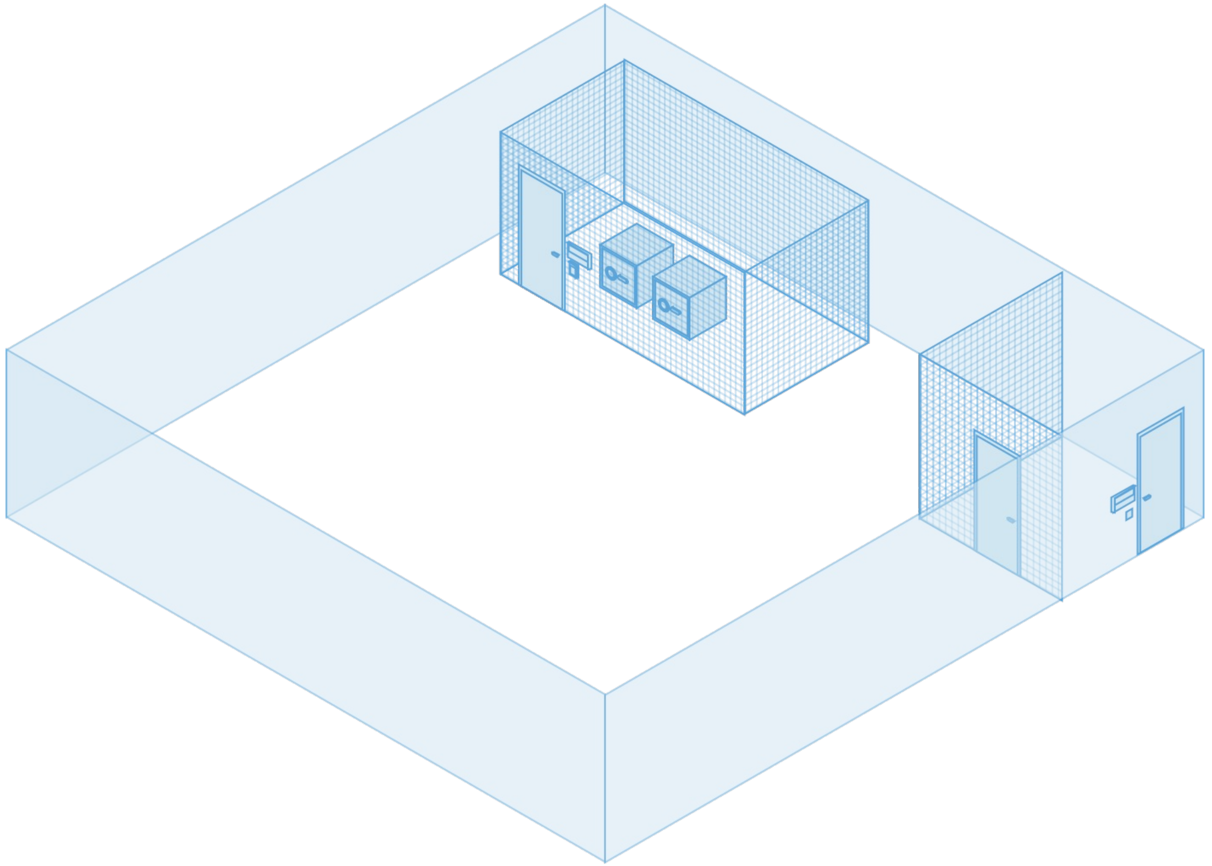
The room is monitored with intrusion and motion sensors and its access is controlled with biometric mechanisms.



# Security of the key to sign the Root

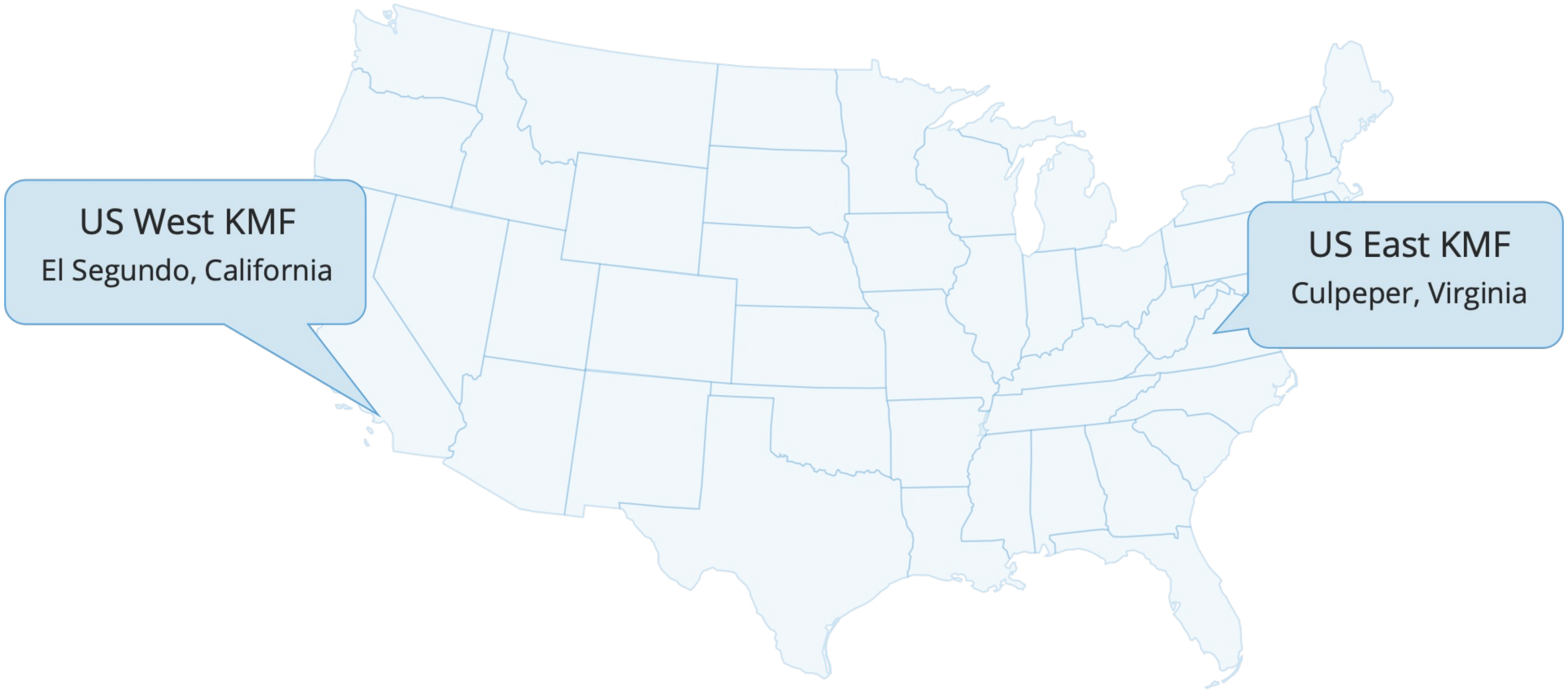
The secure room is located within a larger room where ceremonies involving TCRs and others are held. Ceremonies are video streamed, witnessed by participants and others, and audited by a third-party auditing firm.

Access to this room must be granted by another designated person, the “Physical Access Control Administrator,” who is not on-site, and through biometric access controls.



# Security of the key to sign the Root

The ceremony rooms, known as “Key Management Facilities” (KMFs), are located within two third-party-monitored facilities (Data Centers), one on the East Coast and one on the West Coast of the United States.



# Security of the key to sign the Root

Each ceremony is organized using a complete script that identifies each individual step that must be performed.

Act 1: Initiate Ceremony and Retrieve Materials

### Open Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 15 | CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.) | | |
| 16 | SSC1 opens Safe #1 while shielding the combination from the camera.<br>**Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.** | | |
| 17 | Perform the following steps to complete the safe log:<br>a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera.<br>b) IW provides the pre-printed safe log to SSC1.<br>c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated.<br>d) IW verifies the entry then initials it. | | |

### Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 18 | CA performs the following steps to extract each piece of equipment from the safe:<br>a) CAREFULLY remove each equipment TEB from the safe.<br>b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera.<br>c) Place each equipment TEB on the cart as specified on the list below.<br>d) Write the date, time, and signature on the safe log where "Remove" is indicated.<br>e) IW verifies the safe log entry, then initials it.<br><br>**HSM3: TEB # BB51184512 (Place on Cart)**<br>**HSM4: TEB # BB51184513 (Place on Cart)**<br>**HSM5W: TEB # BB51184514 (Check and Return)**<br><br>**Laptop3: TEB # BB81420125 (Check and Return)**<br>**Laptop4: TEB # BB81420103 (Place on Cart)**<br><br>**OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386 (Place on Cart)**<br><br>**KSK-2017: TEB # BB46584387 (Check and Return)**<br><br>**HSM3 Physical Keyboard Key: TEB # BB21907221 (Place on Cart)** | | |

### Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (Safe Room)

| Step | Activity | Initials | Time |
|---|---|---|---|
| 19 | SSC1 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it. | | |
| 20 | SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off. | | |
| 21 | CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room). | | |

Root DNSSEC KSK Ceremony 40 Page 8 of 38

Act 3: Activate HSM (Tier 7) and Generate Signatures

### Verify the KSR Hash for KSR 2020 Q2

| Step | Activity | Initials | Time |
|---|---|---|---|
| 8 | When the hash of the KSR is displayed on the terminal window, perform the following:<br>a) CA asks the Root Zone Maintainer (RZM) representative to identify themself in front of the room and provide documents for IW to review off camera for the purpose of authentication.<br>b) IW retains the hash and PGP word list for KSR 2020 Q2, and employment verification letter provided by the RZM representative and writes their name on the following line:<br><br>______________________________<br><br>c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used. | | |
| 9 | Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks **"are there any objections?"** | | |
| 10 | CA enters **"y"** in response to `"Is this correct (y/N)?"` to complete the KSR signing operation. The SKR is located in:<br>`/media/KSR/KSK40/skr-root-2020-q2-0.xml` | | |

### Print Copies of the KSR Signer log

| Step | Activity | Initials | Time |
|---|---|---|---|
| 11 | CA executes the commands below using the terminal window to print the KSR Signer log:<br>a) `lpadmin -p HP -o copies-default=X`<br>**Note: Replace "X" with the amount of copies needed for the participants.**<br>b) `printlog`[8] `ksrsigner-202002*.log` | | |
| 12 | IW attaches a copy of the required ksrsigner log to their script. | | |

### Back up the Newly Created SKR

| Step | Activity | Initials | Time |
|---|---|---|---|
| 13 | CA executes the following commands using the terminal window:<br>a) List the contents of the KSR FD by executing:<br>`ls -ltrR /media/KSR`<br>b) Copy the contents of the KSR FD to the HSMFD by executing:<br>`cp -pR /media/KSR/* .`<br>**Note: Confirm overwrite by entering "y" if prompted.**<br>c) List the contents of the HSMFD to verify it has been copied successfully by executing:<br>`ls -ltrR`<br>d) Unmount the KSR FD by executing:<br>`umount /media/KSR` | | |
| 14 | CA removes the **KSR FD** containing the SKR files, then gives it to the RZM representative. | | |

Root DNSSEC KSK Ceremony 40 Page 15 of 38

Act 4: Zeroize and Dismantle Hardware Security Module

### Remove Cryptographic Module and Card Reader from HSM3

| Step | Activity | Initials | Time |
|---|---|---|---|
| 15 | CA performs the following steps to remove the cryptographic module:<br>a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the cryptographic module to the case.<br>b) Lift the cryptographic module up to separate it from the case.<br>c) Using **Tool C**, remove both connectors from the cryptographic module as flush with the case as possible.<br>d) Place the cryptographic module in the **Critical Parts** bin, and the connectors in the **HSM Parts** bin on the ceremony table. | | |
| 16 | CA performs the following steps to remove the front panel and card reader:<br>a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the front panel to the bottom of the case.<br>b) Place the front panel in the **HSM Parts** bin on the ceremony table.<br>c) Using **Tool A+Bit 4**, remove the nut which secures the card reader.<br>d) Using **Tool A+Bit 3**, remove the 3 screws which secure the card reader.<br>e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the **Critical Parts** bin on the ceremony table.<br>f) Place the HSM case in the **HSM Parts** bin on the ceremony table. | | |

### Place the Critical HSM3 parts into a TEB

| Step | Activity | Initials | Time |
|---|---|---|---|
| 17 | CA places the container with the following critical parts into a prepared TEB, then seals it.<br>a) Cryptographic Module<br>b) Logic Board<br>c) Card Reader<br><br>**Note: The HSM case will not be destroyed.** | | |
| 18 | CA performs the following steps:<br>a) Read aloud the TEB number, then show it to the audit camera above for participants to see.<br>b) Confirm with IW that the TEB number matches below.<br>c) Initial the TEB along with IW using a ballpoint pen.<br>d) Give IW the sealing strips for post-ceremony inventory.<br>e) Give RKOS the TEB for destruction.<br><br>**HSM3: TEB # BB81420112** | | |

### Retire HSM Physical Keyboard Key

| Step | Activity | Initials | Time |
|---|---|---|---|
| 19 | CA performs the following steps to retire the listed HSM Physical Keyboard Key:<br>a) Remove the TEB from the cart.<br>b) Inspect TEB for tamper evidence.<br>c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used.<br>d) Remove and discard the TEB.<br>e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area.<br><br>**HSM3 Physical Keyboard Key: TEB # BB21907221**<br>**Last Verified: AT22 2015-07-20** | | |

Root DNSSEC KSK Ceremony 40 Page 23 of 38

# Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann