

# Overview of the IANA Functions

Marilia Hirano - Director, IANA Strategic Programs

Selina Harrington - IANA Operations Manager

Aaron Foley - Senior Cryptographic Key Manager

2nd IANA Function Review Team

January 10 2024

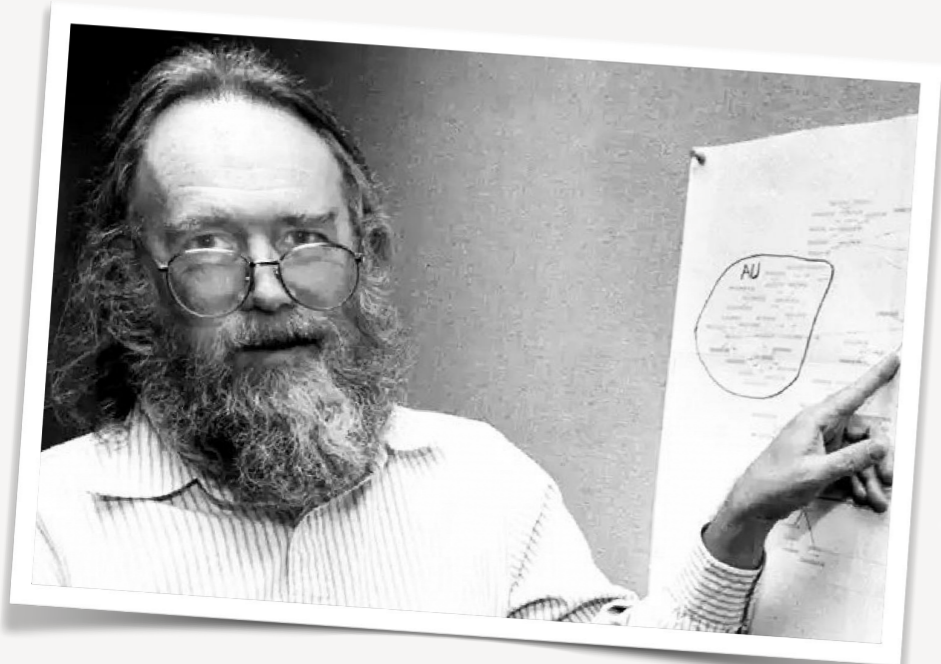
# Agenda

---

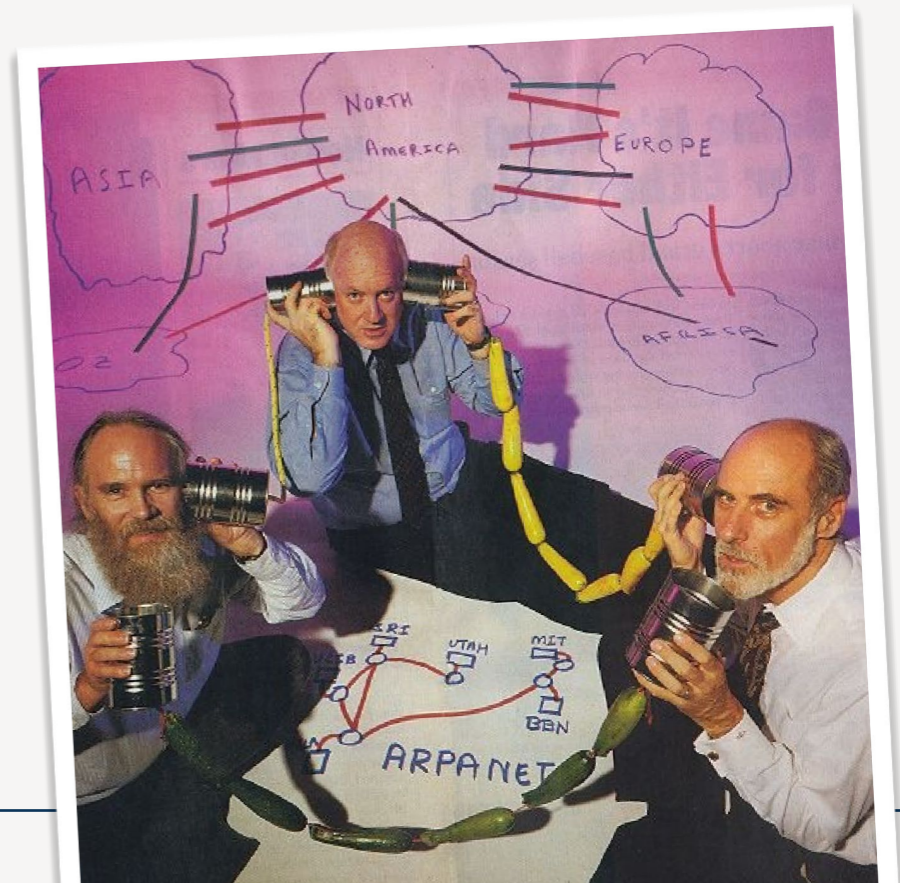
- What is IANA?
- Oversight & Accountability
- Core IANA functions
- Q&A

# What are the IANA functions?

- The record keeper for the unique names and numbers used by Internet technologies to interoperate
- The IANA functions pre-date ICANN. In 1998, ICANN was established to be the home of the IANA functions
- The unique identifiers include protocol parameters, Internet numbers and domain names
- The IANA team maintains these records according to policies adopted by Internet names, numbers and protocol standards communities



Jon Postel (L) started the IANA; with Steve Crocker and Vint Cerf (R)



# Why do the IANA functions exist?

- Coordinating the Internet unique identifier systems is needed to ensure the Internet interoperates globally
- If Internet-connected devices do not use the same system of identifiers and numbers to talk to one another, the system will not interoperate (i.e. speak a common language)
- The authoritative registries are used by vendors, service providers, businesses, application developers and others to innovate and expand the use of the Internet

**BGP Identifier Structure (32 bits):**

- Version (1 byte)
- My Autonomous System (2 bytes)
- Hold Time (2 bytes)
- BGP Identifier (4 bytes)
- Opt Param Len (1 byte)
- Option

**Parts of an SRV record:**

service	proto	name	TTL	class	priority	weight	port	target
_sip	_tls	example.yourdomain.com	600	IN	SRV	0	5 5060	sipserver.yourdomain.com.

**DNS Answers for www.google.com:**

- www.google.com: type A, class IN, addr 74.125.131.147
- Name: www.google.com
- Type: A (host address)
- Class: IN (0x0001)
- Time to live: 5 minutes
- Data length: 4
- Addr: 74.125.131.147
- www.google.com: type A, class IN, addr 74.125.131.103
- www.google.com: type A, class IN, addr 74.125.131.104
- www.google.com: type A, class IN, addr 74.125.131.106
- www.google.com: type A, class IN, addr 74.125.131.99
- www.google.com: type A, class IN, addr 74.125.131.105

**OID Tree Example:**

```
graph TD
  Root[Root] --> iso[iso (1)]
  Root --> org[org (3)]
  Root --> dod[dod (6)]
  Root --> Internet[Internet (1)]
  Internet --> directory[directory (1)]
  Internet --> mgmt[mgmt (2)]
  Internet --> experimental[experimental (3)]
  Internet --> private[private (4)]
  directory --> mib-2[mib-2 (1)]
  directory --> system[system (1)]
  mgmt --> interfaces[interfaces (2)]
  mgmt --> ip[ip (4)]
  experimental --> cisco[cisco (9)]
  private --> enterprise[enterprise (1)]
  enterprise --> microsoft[microsoft (311)]
  enterprise --> juniperMIB[juniperMIB (2636)]
```

**HTTP Status Codes:**

Code	Description
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Payload Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
418	I'm a teapot
421	Misdirected Request
422	Unprocessable Entity
423	Locked
424	Failed Dependency
426	Upgrade Required
428	Precondition Required
429	Too Many Requests
431	Request Header Fields Too Large
444	Connection Closed Without Response
451	Unavailable For Legal Reasons
499	Client Closed Request
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported
506	Variant Also Negotiates
507	Insufficient Storage
508	Loop Detected
510	Not Extended
511	Network Authentication Required
599	Network Connection Aborted

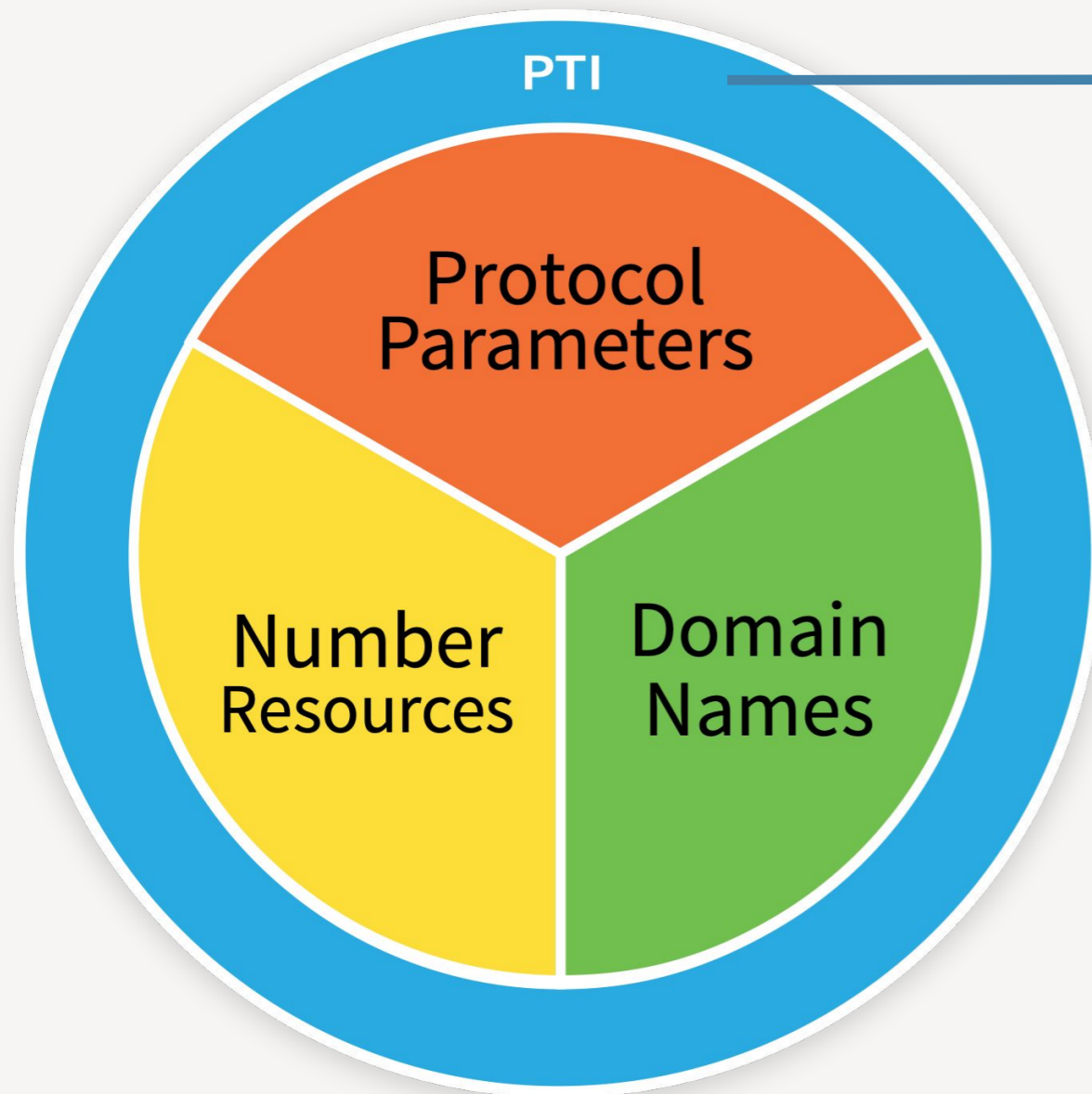
**TCP Connection Establishment:**

- Send SYN (SEQ=100 CTL=SYN)
- SYN received (SEQ=300 ACK=101 CTL=SYN, ACK)
- Send SYN, ACK (SEQ=101 ACK=301 CTL=ACK)
- SYN, ACK received (SEQ=101 ACK=301 CTL=ACK)
- Established (SEQ=101 ACK=301 CTL=ACK)

**Transmission Control Protocol (TCP) Header (20-60 bytes):**

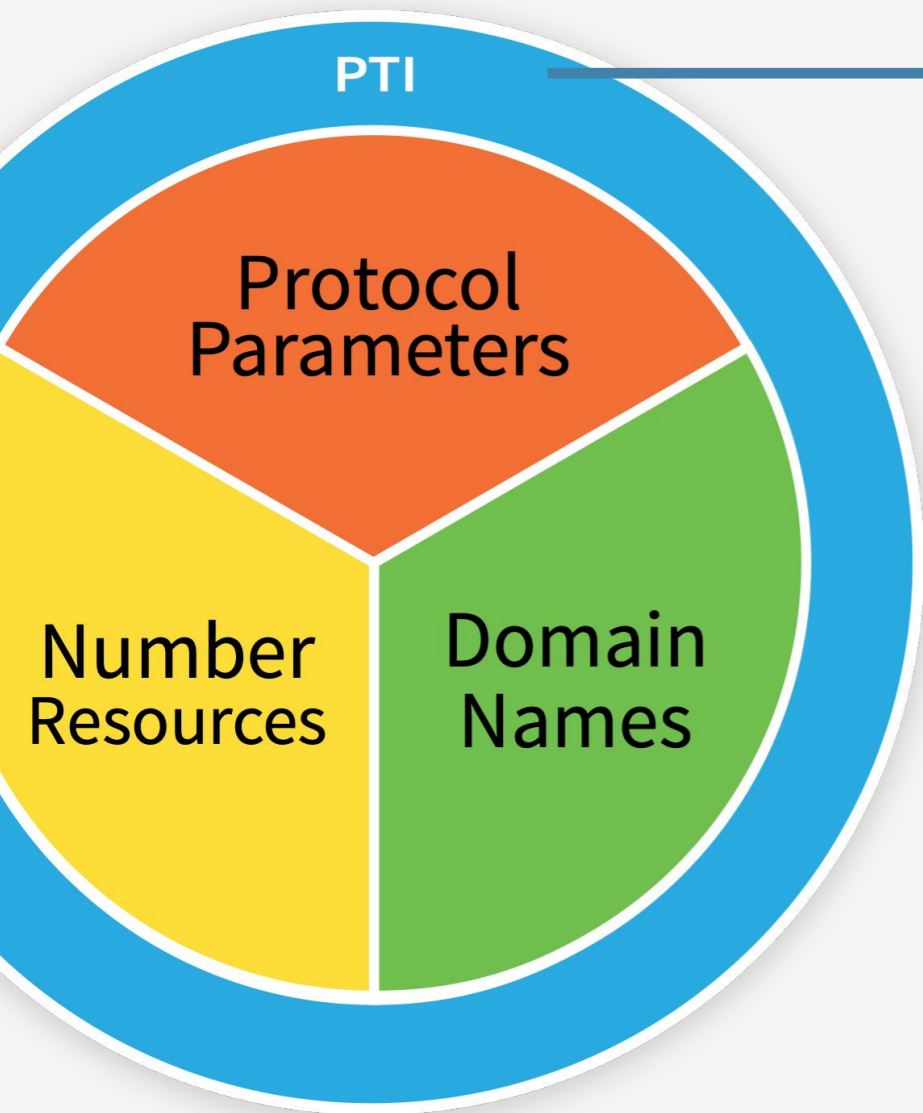
Field	Length
source port number	2 bytes
destination port number	2 bytes
sequence number	4 bytes
acknowledgement number	4 bytes
checksum	2 bytes
urgent pointer	2 bytes
optional data	0-40 bytes

# Oversight & Accountability



## Public Technical Identifiers

- Performs the IANA functions
- Is a non-profit organization created in 2016
- Hires the IANA staff
- ICANN is its sole member (i.e. affiliate of ICANN)



## IANA Staff



Shaunte Anderson



Amanda Baber



Dan Bougere



Tyler Carroll



Amy Creamer



Kim Davies



David Dong



Aaron Foley



Selina Harrington



Lawrence He



Marilia Hirano



Tania Hopkins



James Mitchell



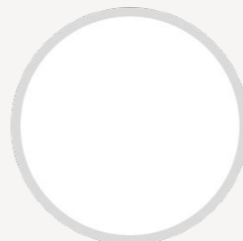
Ali Mohammadi



Candace Montoya



Andres Pavez



TBD



Seman Said



George Sarkisyan

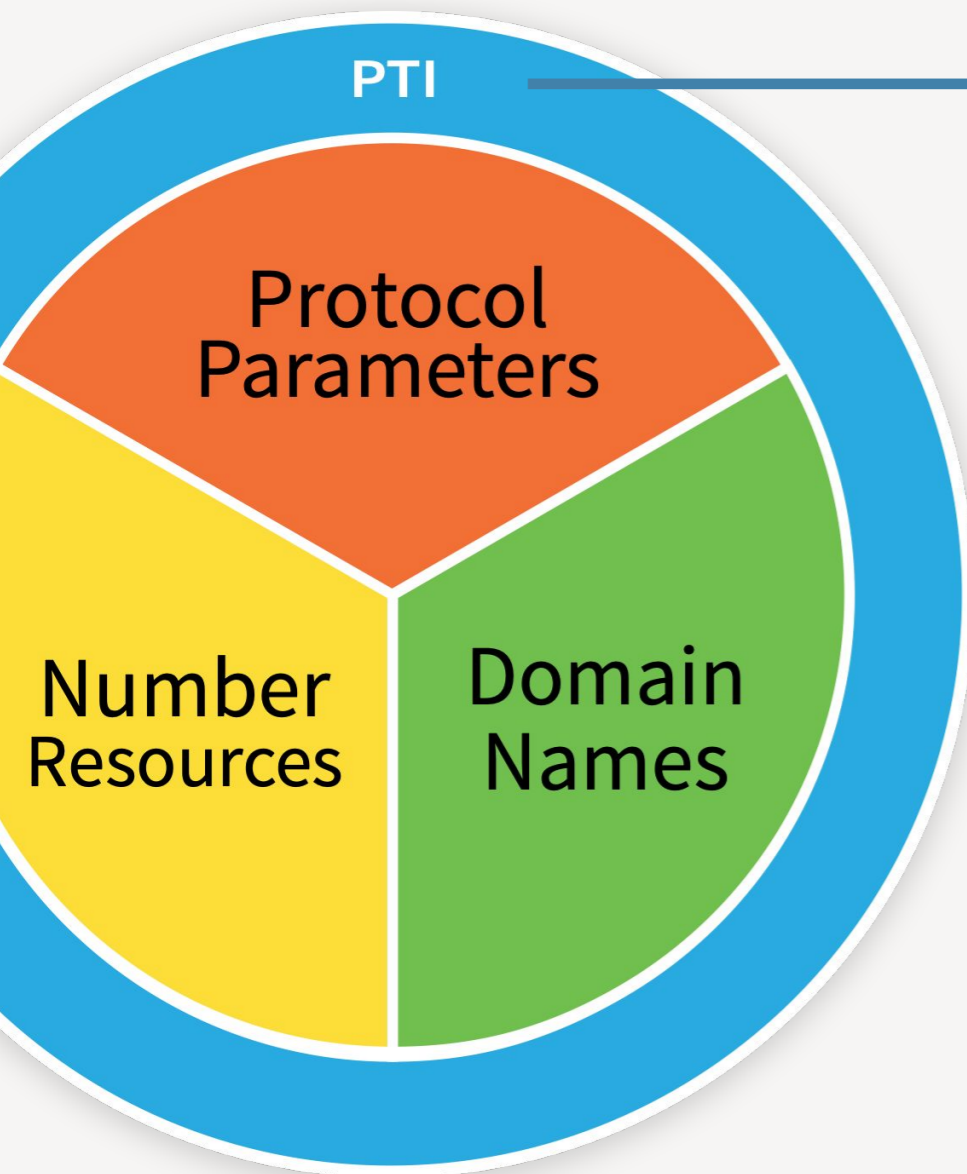


Sabrina Tanamal

● Operations

● Strategic Programs

● Technical Services



## PTI Board

Five-member board of directors including 2 Nomcom appointees



**Anupam Agrawal**  
NOMCOM APPTTEE



**Xavier Calvez**  
ICANN CFO



**Kim Davies**  
PTI PRESIDENT

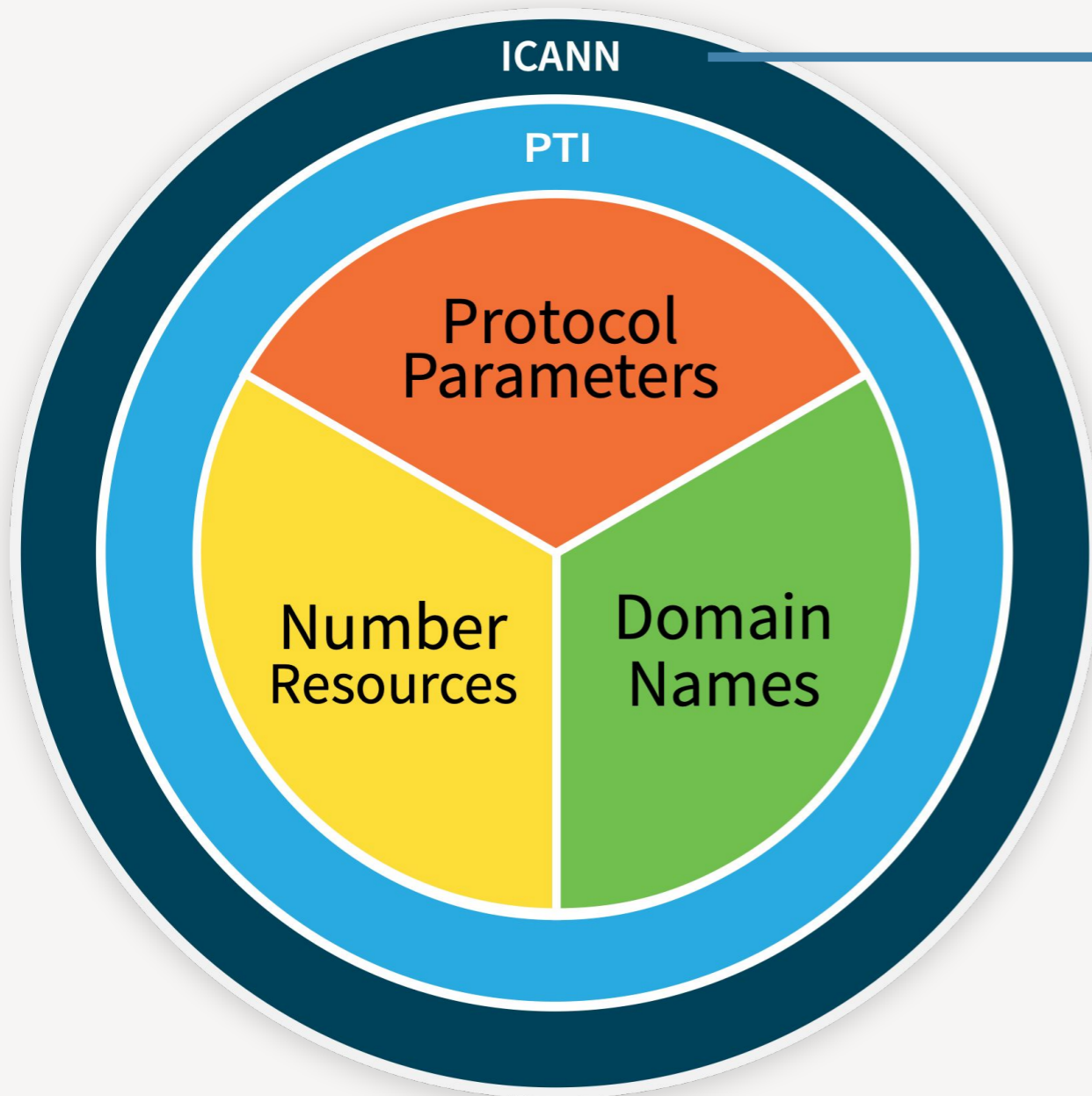


**Jia-Rong Low**  
ICANN VP, APAC



**Tobias Sattler**  
CHAIR  
NOMCOM APPTTEE



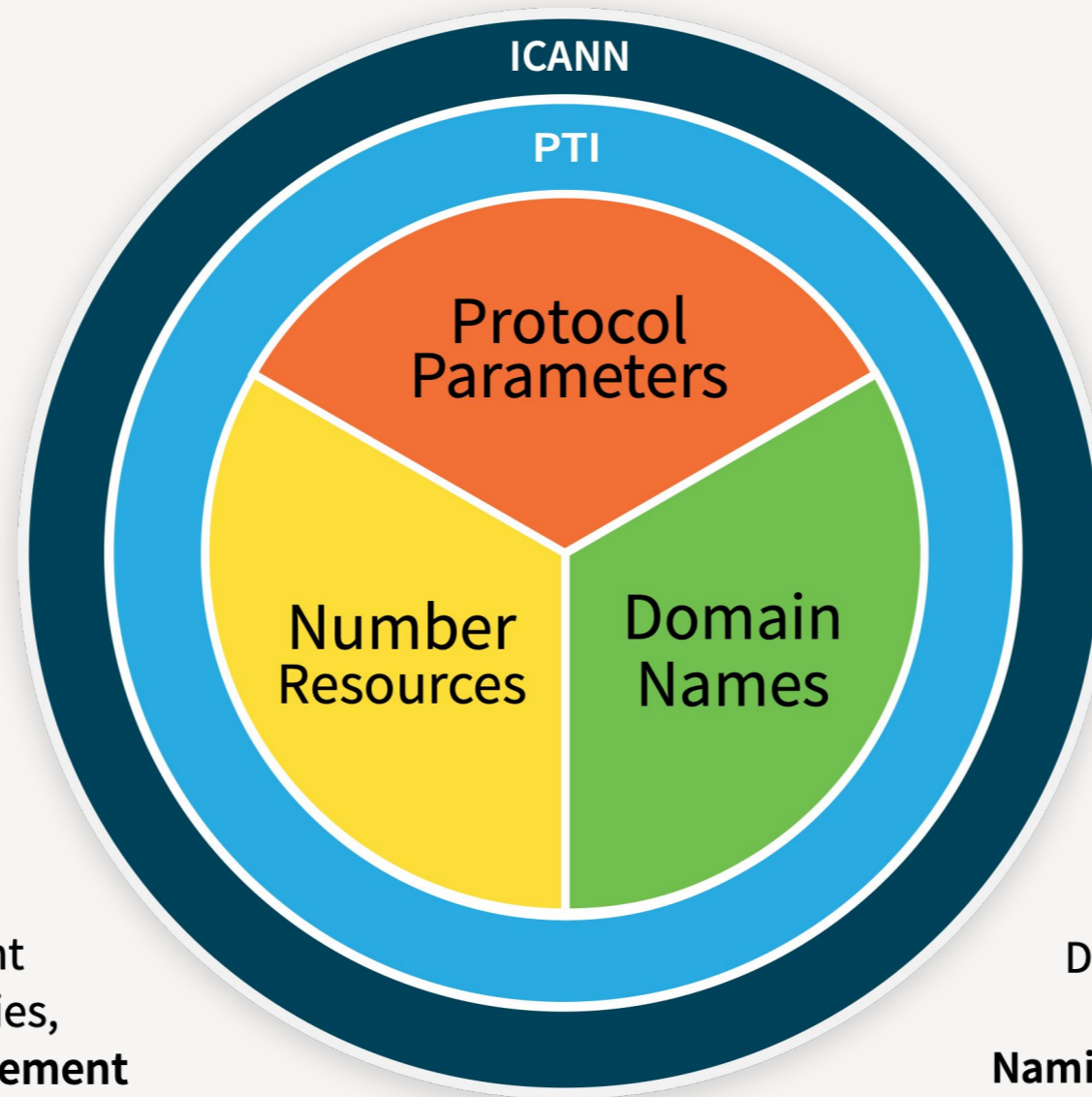


## ICANN

- Responsible for the IANA functions
- Contracts PTI to perform the IANA functions
- Oversees PTI's performance
- Provides shared resources (Legal, IT, HR, Finance and many others)
- Provides all funding to PTI
- Supports additional accountability mechanisms such as Customer Standing Committee, IANA Naming Function Reviews

# Contracts

Protocol Parameter oversight  
through **Memorandum of Understanding**  
between IETF and ICANN,  
subcontracted from ICANN to PTI

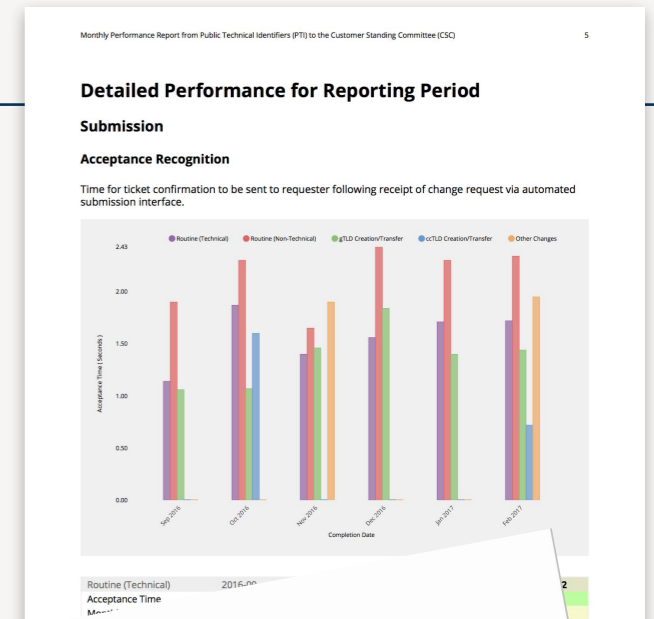


Number resource oversight  
by Regional Internet Registries,  
governed by **Service Level Agreement**  
between ICANN and RIRs,  
subcontracted from ICANN to PTI

Domain Name oversight by ICANN;  
governed by  
**Naming Contract** between ICANN and PTI;  
performance oversight by  
**ICANN Customer Standing Committee**

# Accountability

- Each function has service level expectations defined and reported against
  - Reports against KPIs to the IETF for protocol parameters
  - Around 70 measurement categories to the Customer Standing Committee for naming functions
  - Performance reporting to the numbering community for IP address and AS number allocations
  
- These figures are reviewed through various processes
  - Monthly Customer Standing Committee meetings, plus IANA Naming Function Reviews
  - Regular meetings and dialogue with IETF leadership
  - Reports to RIRs and an annual IANA Review Committee process



IANA Protocol Parameter Service  
Monthly Report  
October 15, 2019

For the Reporting Period of  
September 1, 2019 – September 30, 2019

Prepared by: Amanda Baber  
amanda.baber@iana.org

- Executive Summary ..... 1
- Statistics ..... 2
- IESG approved documents (a) ..... 3
- Reference Updates (b) ..... 4
- Last Calls (c) ..... 5
- Evaluations (d) ..... 6
- Media (MIME) type requests (e, f) ..... 7
- New Port number requests (g) ..... 8
- Modification to and/or deletions of Port number requests (h) ..... 8
- New Private Enterprise Number (PEN) requests (i) ..... 8
- Modifications to and/or deletions of PEN requests (j) ..... 8
- New TRIP ITAD Numbers (k) ..... 9
- Requests relating to other IETF-created registries for which the request rate is more than five per month (l) ..... 10
- Deliverables ..... 11
- Provide publicly accessible, clear and accurate periodic statistics ..... 11
- Track and publicly report on a monthly basis (monthly report) ..... 11
- Conclusions ..... 11

### Number Resource Performance

June 2019

#### Performance Summary

These performance targets are derived from section 4.3 of the Numbering Services for the allocation of unicast IP addresses a Internet Registries.

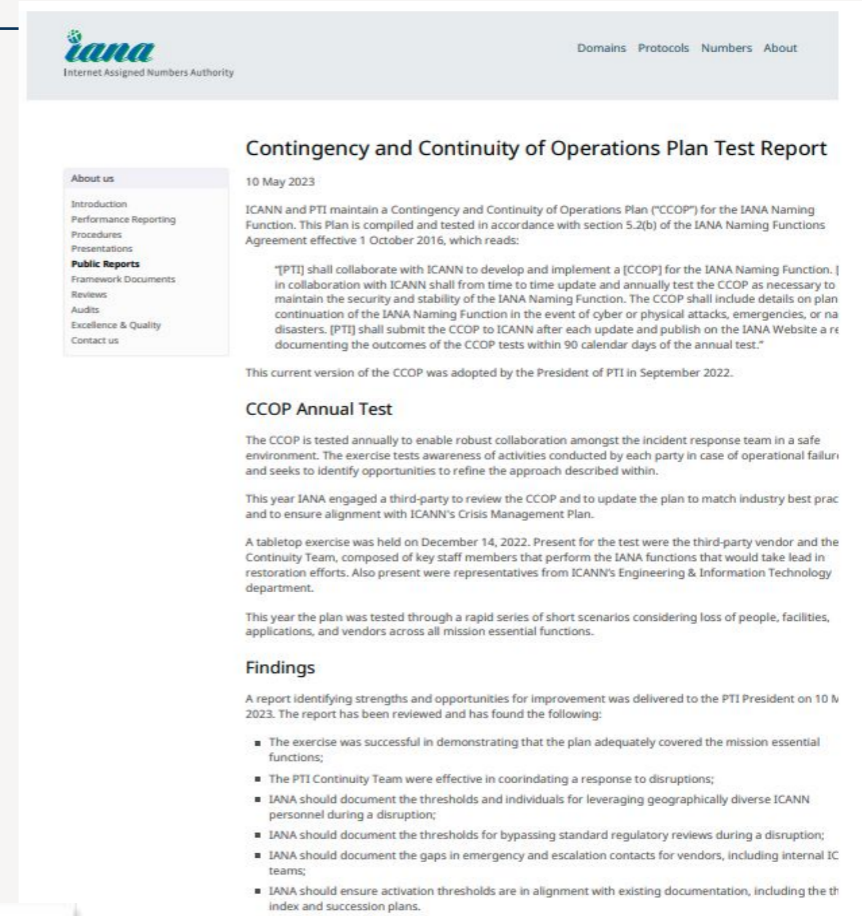
- ✔ Requests acknowledged on time (100%)
- ✔ Responded on time (100%)
- ✔ Implemented on time (100%)
- ✔ Implemented accurately (100%)

#### Individual Requests to Regional Internet Registries

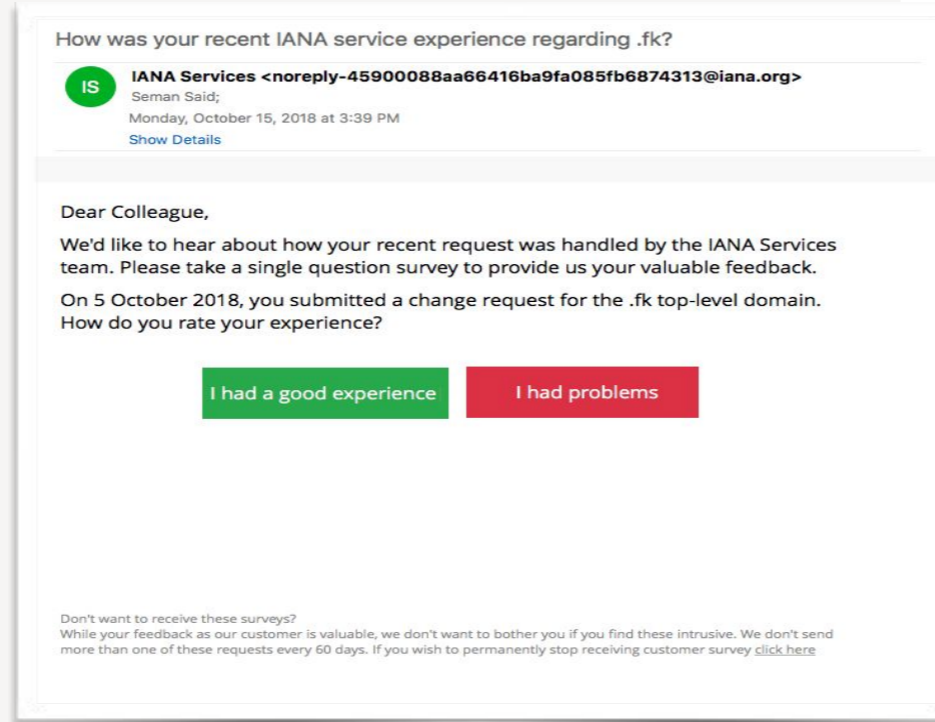
Date	Request Type	Request Processing Details
2019-05-13	IPv6 Unicast	<ul style="list-style-type: none"> <li>✔ Responded on time (0.3 days)</li> <li>✔ Implemented on time (0.2 days)</li> <li>✔ Clarification asked on time (2.1 days)</li> <li>✔ Accurately implemented</li> </ul> <a href="#">More info</a>
2019-06-11	AS Number	<p>2019-06-11 01:42:36 Request received from APNIC <a href="#">Less info</a></p> <p>⌚ 0.6 business days</p> <p>2019-06-11 15:12:36 Request acknowledged</p> <ul style="list-style-type: none"> <li>✔ Acknowledged on time (within 2 business days)</li> </ul> <p>⌚ 1.1 business days</p> <p>2019-06-12 18:03:29 Implemented using resource(s)</p> <ul style="list-style-type: none"> <li>✔ Implemented on time (within 4 business days)</li> <li>✔ Implemented accurately</li> </ul>

# Accountability

- Third-Party Information Security Audits
- Internal Audits
- Customer Satisfaction Surveys
- Regular Review & Updates of Business Processes
- Contingency & Continuity Plans
- Structured Project Management Framework
- Regular engagement with the community



The screenshot shows the IANA website header with the logo and navigation links: Domains, Protocols, Numbers, About. The main content area is titled "Contingency and Continuity of Operations Plan Test Report" dated 10 May 2023. It includes a table of contents on the left with sections like Introduction, Performance Reporting, Procedures, Presentations, Public Reports, Framework Documents, Reviews, Audits, Excellence & Quality, and Contact us. The main text describes the CCOP (Contingency and Continuity of Operations Plan) for the IANA Naming Function, its annual testing, and findings from a 2023 report. The findings list several areas for improvement, such as documenting thresholds and activation plans.



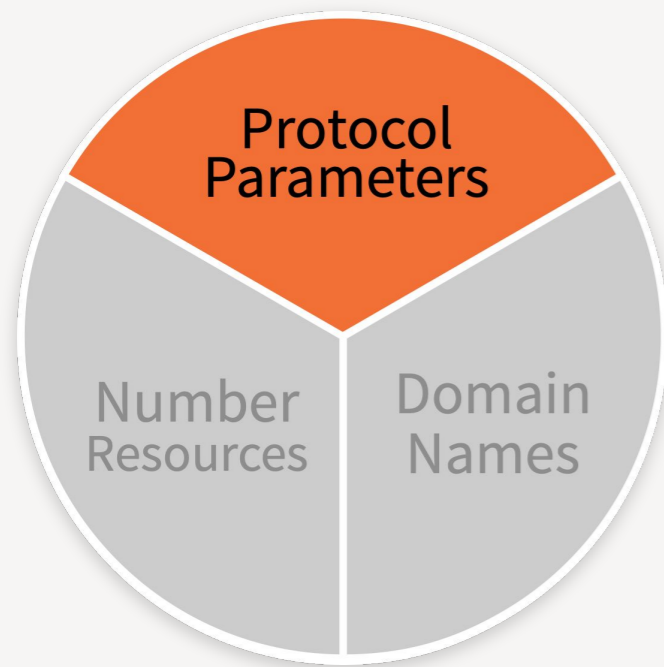
The screenshot shows an email survey from IANA Services. The subject is "How was your recent IANA service experience regarding .fk?". The sender is "Seman Said" on Monday, October 15, 2018 at 3:39 PM. The email content reads: "Dear Colleague, We'd like to hear about how your recent request was handled by the IANA Services team. Please take a single question survey to provide us your valuable feedback. On 5 October 2018, you submitted a change request for the .fk top-level domain. How do you rate your experience?" Below the text are two buttons: "I had a good experience" (green) and "I had problems" (red). At the bottom, there is a note: "Don't want to receive these surveys? While your feedback as our customer is valuable, we don't want to bother you if you find these intrusive. We don't send more than one of these requests every 60 days. If you wish to permanently stop receiving customer survey [click here](#)".



The banner features the ICANN logo at the top right. The main text reads "IANA Engagement Survey 2022" in large white font, with "January 2023" below it. The background is a dark blue gradient with a globe and keyboard keys. The "echo" logo is in the bottom right corner, and "echoresearch.com" is in the bottom left corner.

# Core IANA Functions

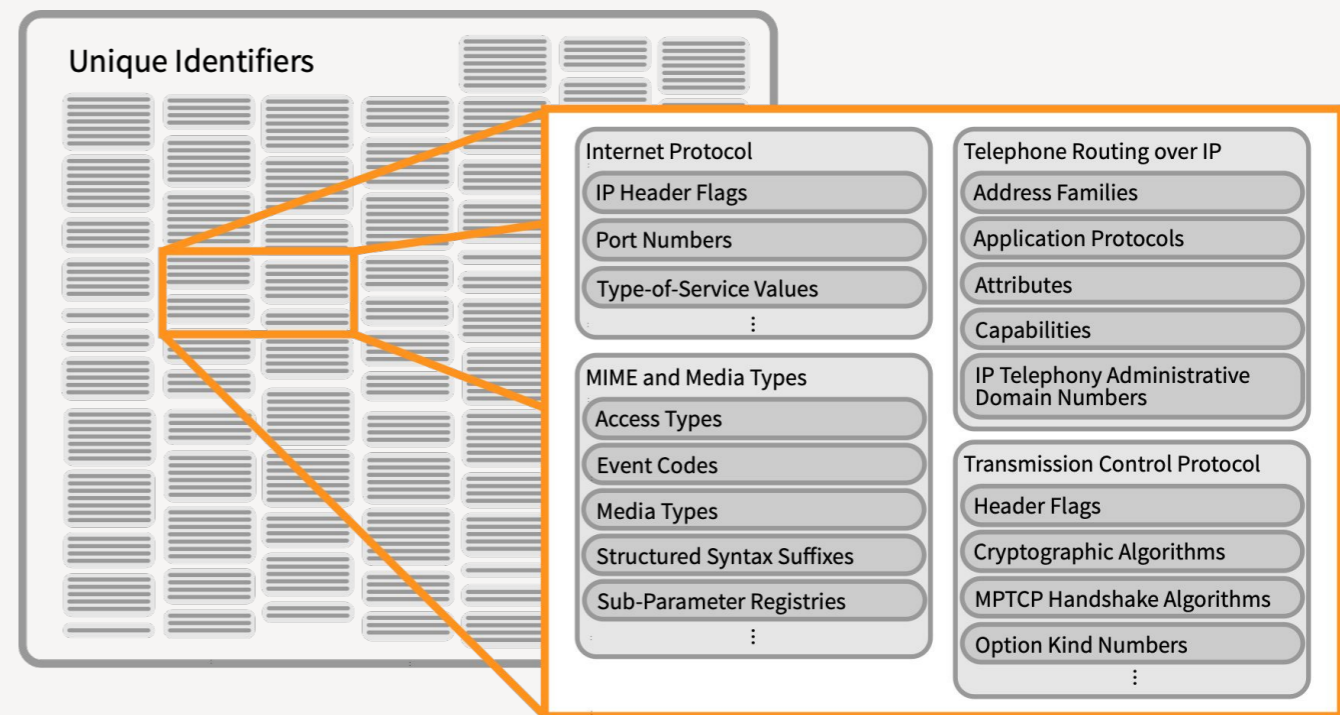
*Selina Harrington*

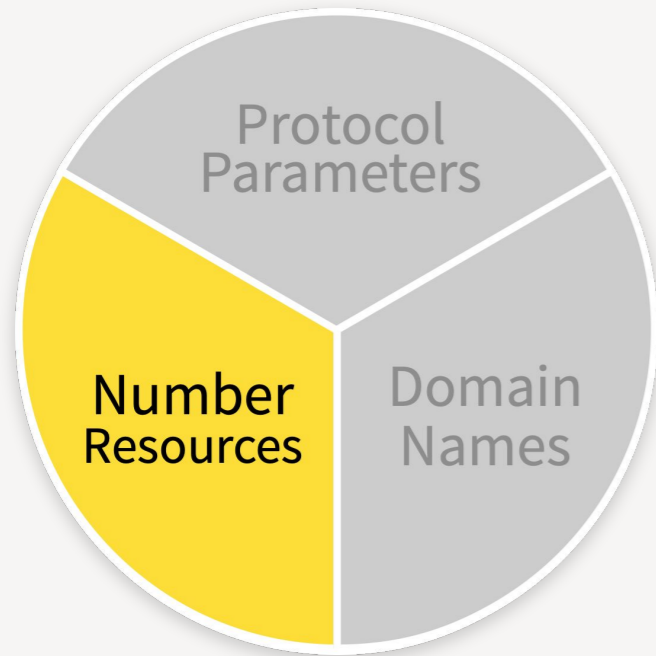


- **Protocol Parameters** are used everywhere and are directly issued by IANA.
- Most protocol parameters' visibility is **limited** to software implementers (i.e. inside software code).
- The **Internet Engineering Task Force (IETF)** develops the Internet standards that define protocol parameter systems.

### IANA's role:

- Receiving and evaluating requests to create new registries and to add new values to registries
- Maintaining and publishing registry data
- Providing advice on upcoming standards efforts on how it would be implemented as part of the IANA functions



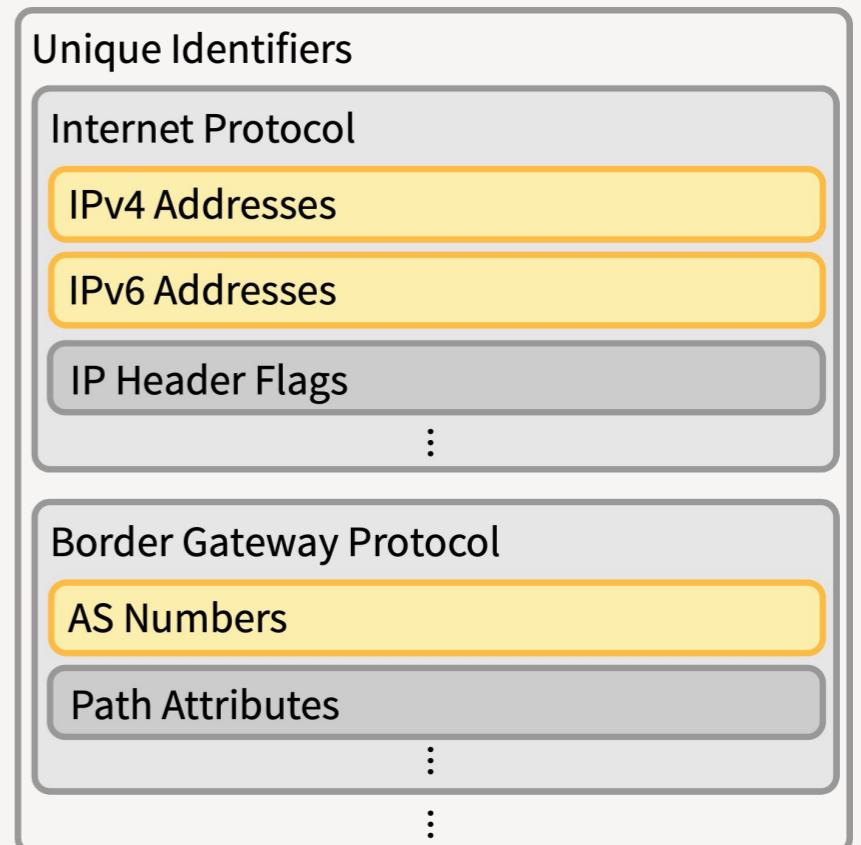


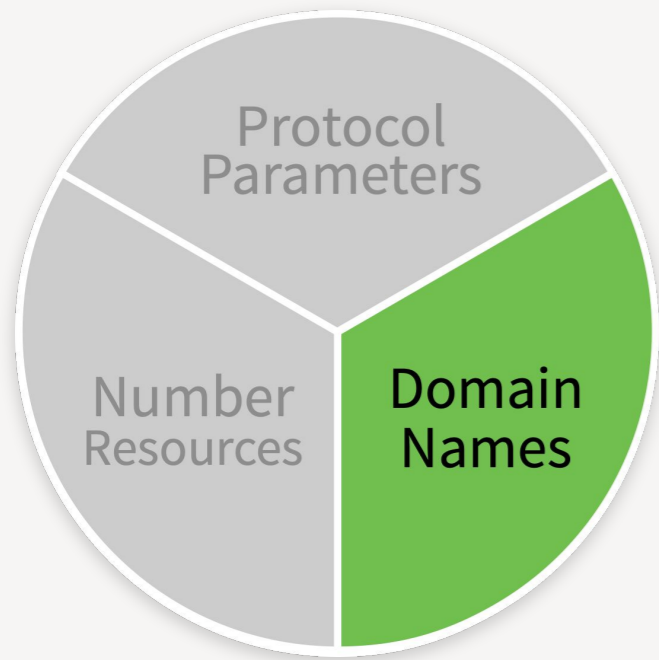
**Number Resources** are specialized forms of protocol parameters:

- IP Addresses: unique identifiers for devices on the Internet
- Autonomous System (AS) numbers: unique identifiers that group networks on the Internet

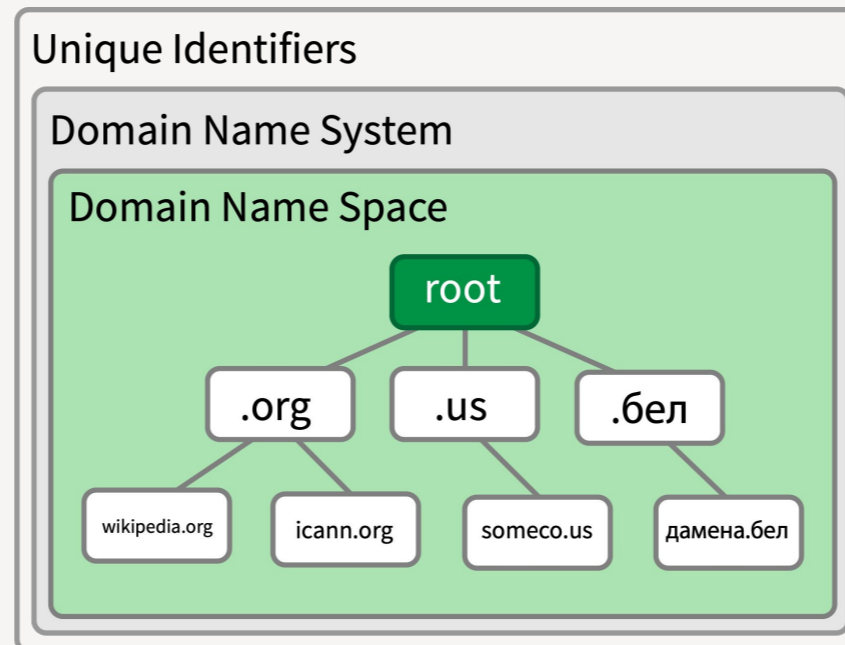
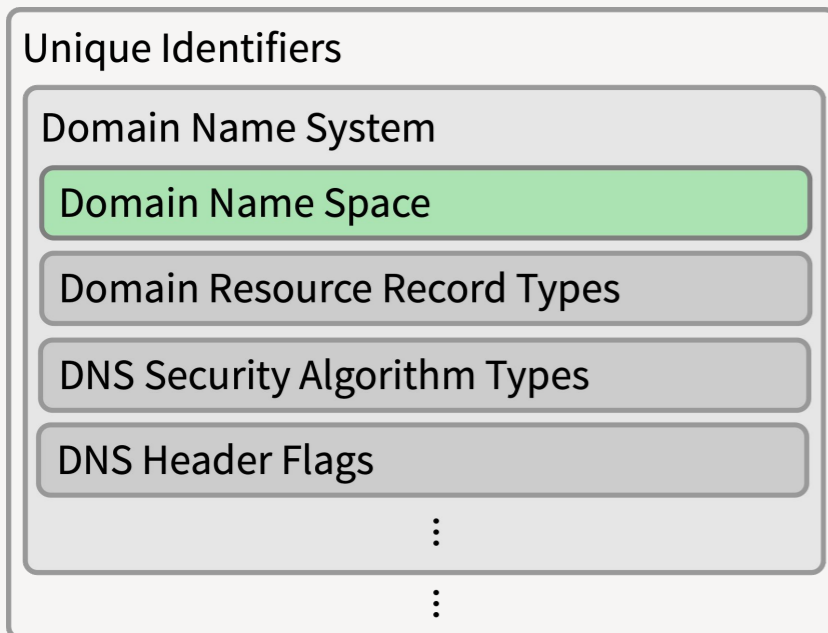
### IANA allocates Number Resources to five Regional Internet Registries

- RIRs in turn delegate them to ISPs and network operators in their region
- Some specialized allocations are made directly by IANA (e.g. multicast)
- Deterministic decision making is used.

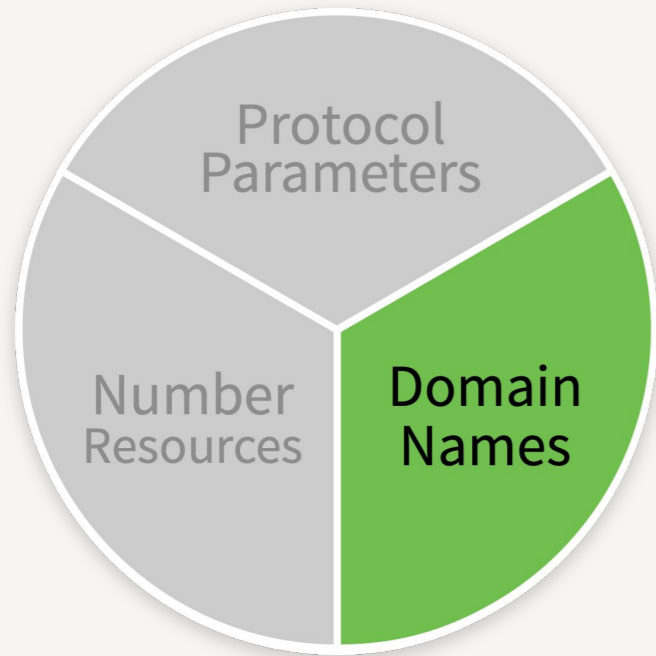




- Most notable IANA function is managing the DNS root zone, which defines top-level domains
- Like number resources, the domain name space is hierarchically delegated, with IANA responsible for the upper-most level of allocations.
- The IANA tasks include:
  - Receiving and evaluating root zone changes requests against policies and operational requirements:
    - Assignment and transfer of TLDs
    - Routine maintenance of name servers and other technical elements
    - Points of Contact
  - Transmitting vetted changes for implementation in the root zone and root servers.







## Domain Names — Other functions

# .INT Registry

---

- Intergovernmental treaty organisations
- Started in 1988. Historically also included some non-treaty purposes (“international databases”) but this was phased out in 2000.
- Approximately 200 domains registered
- A small registry with very few legitimate requests per month, most are rejections for applicants that are not intergovernmental treaty organizations

# .ARPA Registry

---

- For protocol-parameter uses, not used by end users of the Internet
- For uses prescribed by RFCs, therefore considered a protocol parameter registry in terms of oversight, not part of the naming functions

# Label Generation Rulesets

---

- LGR Repository (formerly “IDN tables”)
- Informal repository started by ICANN staff to share best practice for IDN deployment
- Contains the definitive code points and associated eligibility rules for which strings are permitted for registration within a TLD’s policy
  - Usually language-bound (e.g. Thai, Japanese, Urdu) or script-bound (e.g. Latin, Cyrillic, Arabic, Simplified Chinese)
- Became a contractual requirement for gTLD operators (not ccTLDs) to adhere to the “IDN Guidelines”, which in turn made it a requirement to submit these as they were part of the guidelines.
- Was not an IANA function under the NTIA, but became one post-transition due to the previous point.
- No initial SLAs, but a recent review suggested they be added, new SLAs now in place with the CSC
- IANA lead development of a standard (RFC 7940) and plans to migrate to it over time

## The IANA Department does

- ✓ Create registries based on policies from the community
- ✓ Maintain existing registries
- ✓ Allocate number resources
- ✓ Publish all registries for general public use

## The IANA Department doesn't

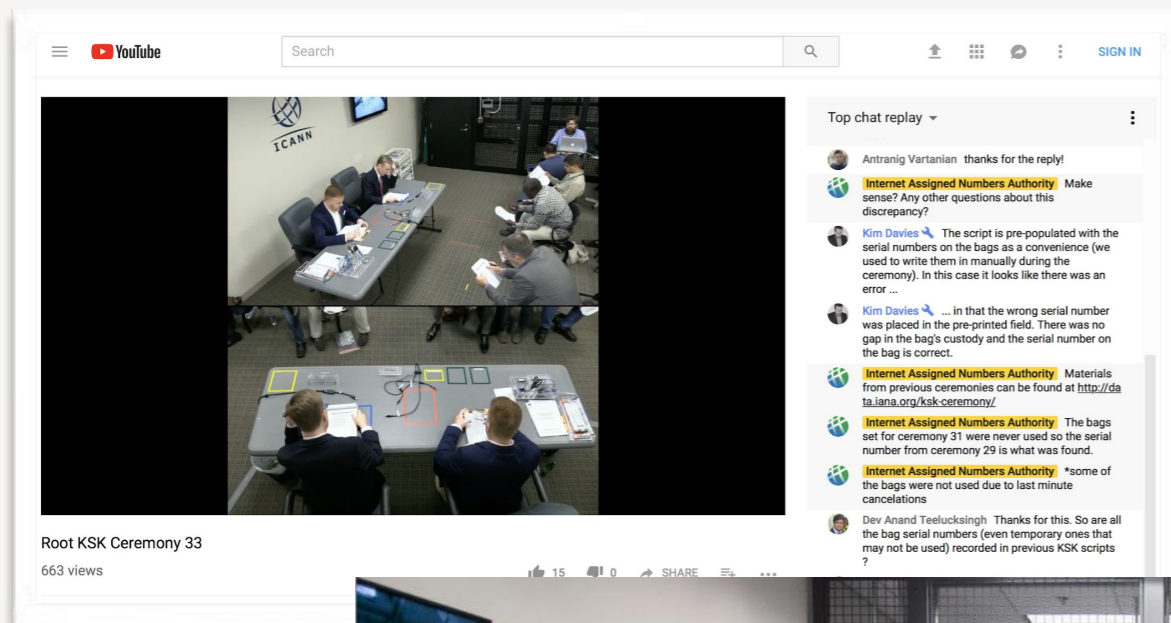
- ✗ Create nor interpret policy
- ✗ Determine what can be a domain name
- ✗ Choose TLD managers

# The Root Key Signing Key

Aaron Foley

# The Root Key Signing Key

- ▶ As part of its root zone related functions, IANA manages the **key signing key**, the trust anchor used to secure the DNS with the DNSSEC protocol.
- ▶ An auditable process of performing **key signing ceremonies** to use this key is conducted using members of the community as key participants.



## Root KSK Ceremony 52

This DNSSEC key signing ceremony is planned for  
14 February 2024, 2100 UTC

Location [Root Zone Key Management Facility West](#)  
El Segundo, California, USA

Ceremony Start  
2024-02-14 21:00:00 UTC  
Wednesday 14 February 2024, 1 p.m. (local time at facility)

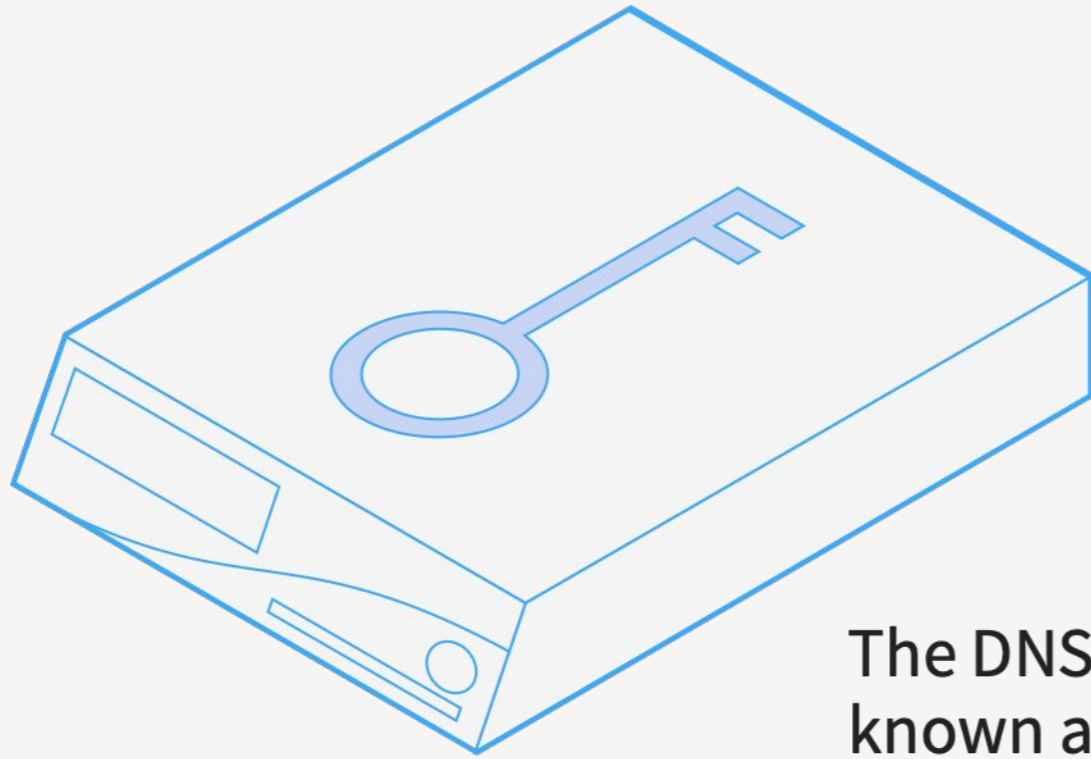
Objectives  
Sign the ZSK for 2024Q2  
Introduce Hardware Security Module 8W

### Observing the ceremony

The key signing ceremony is a public event, and you are welcome to observe. Due to space constraints, only a small number of persons are able to participate as observers at a ceremony in person. We also broadcast ceremonies as they happen, and will provide recordings after the ceremony is concluded. Prior to observing a ceremony, we recommend you review the ceremony materials (i.e. the draft script) in advance.

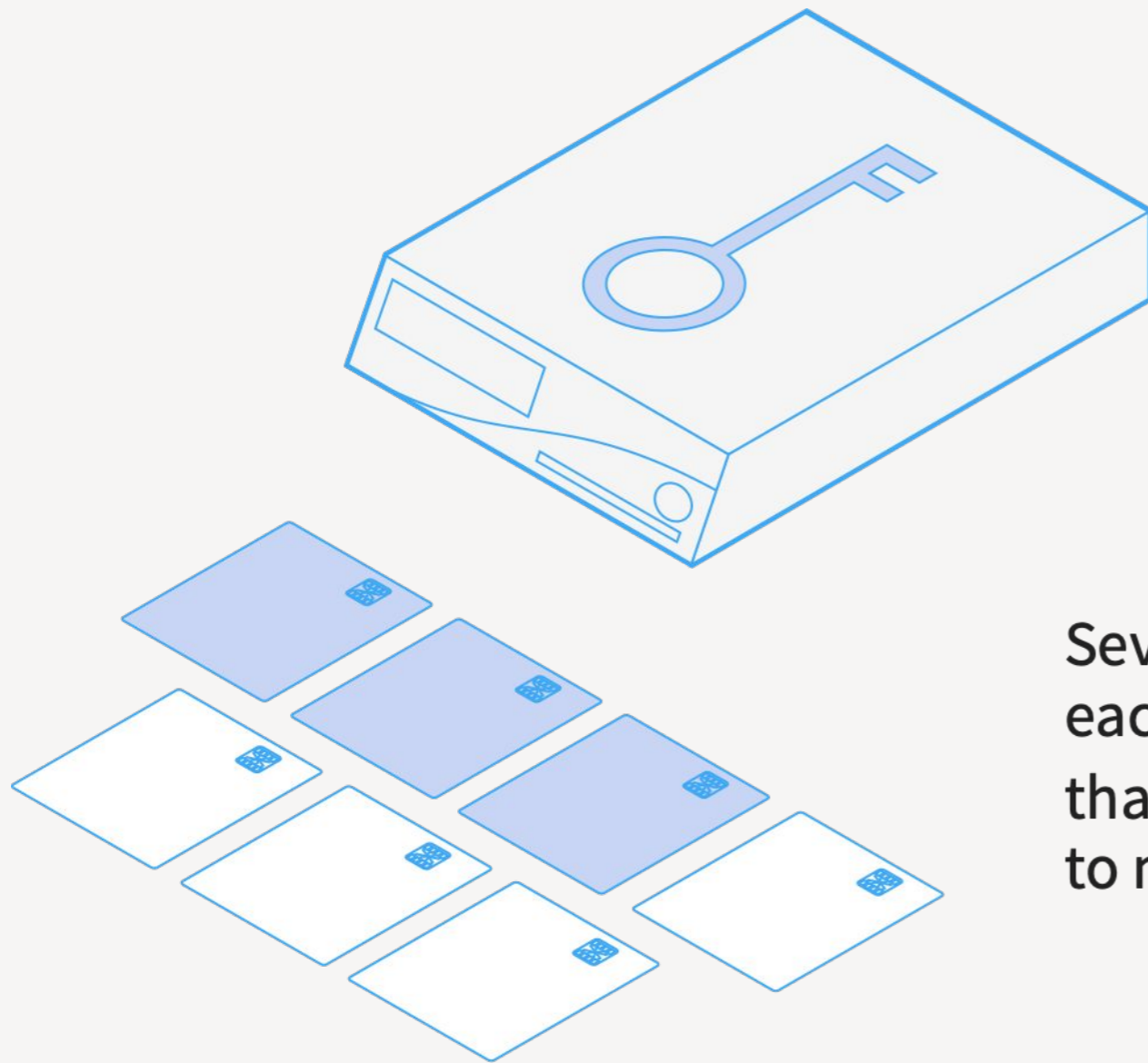
**In Person** If you wish to attend as an observer in person, this must be arranged in advance. Priority is given to those that have a formal role in the ceremony, and then on a first-come first-served basis. This ceremony will be held in El Segundo, California, USA, and observers must meet all costs in travelling to the ceremony. Requests should be submitted at least 45 days before the ceremony (i.e. by 31 December 2023)



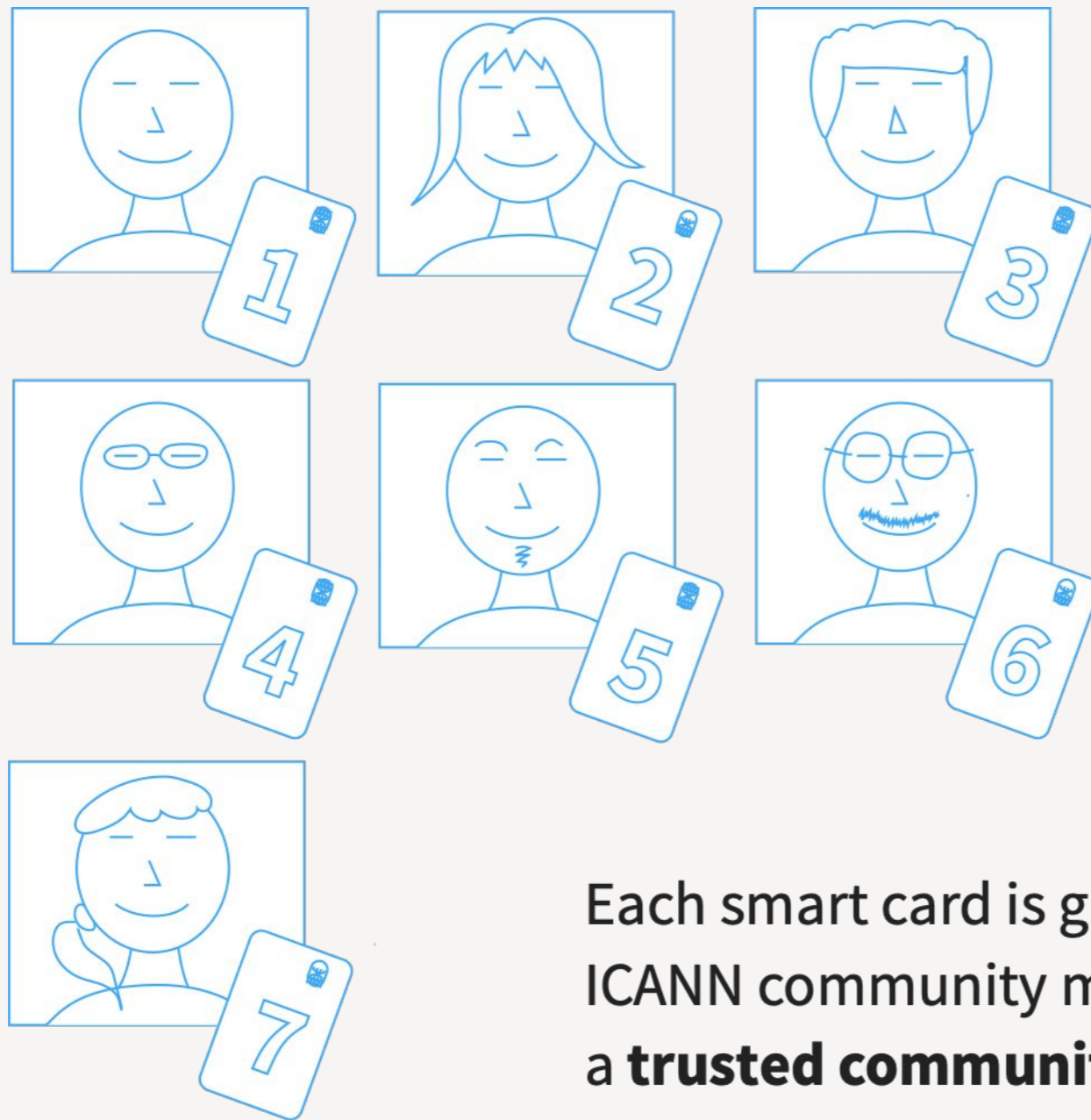


The DNSSEC root key is stored in a device known as a **hardware security module** (HSM) whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper proof. If there is an attempt to open it, the contents will self-destruct.

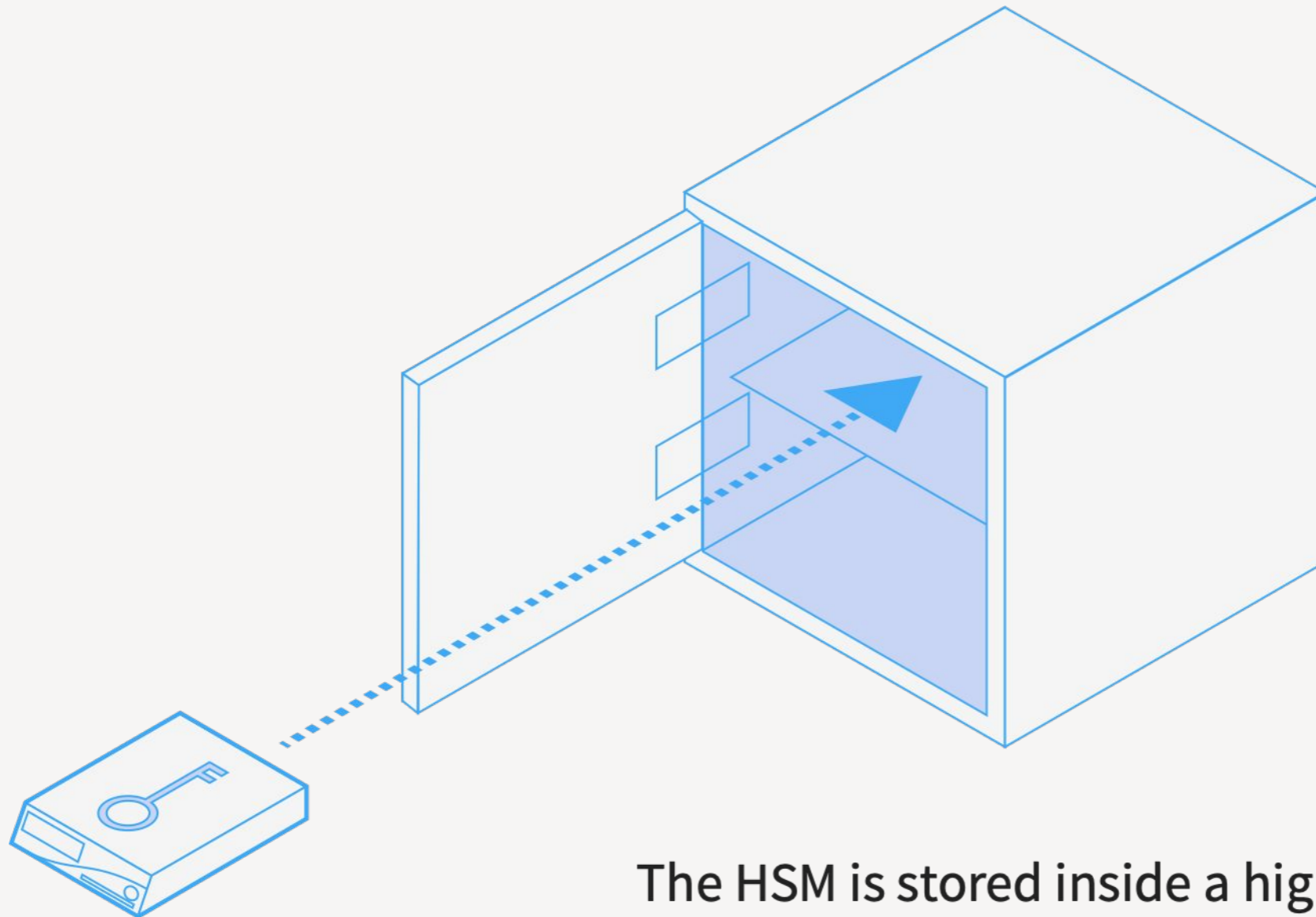




Seven smart cards exist that can turn on each device. The device is configured such that **3 of the 7** smart cards must be present to make it useable.

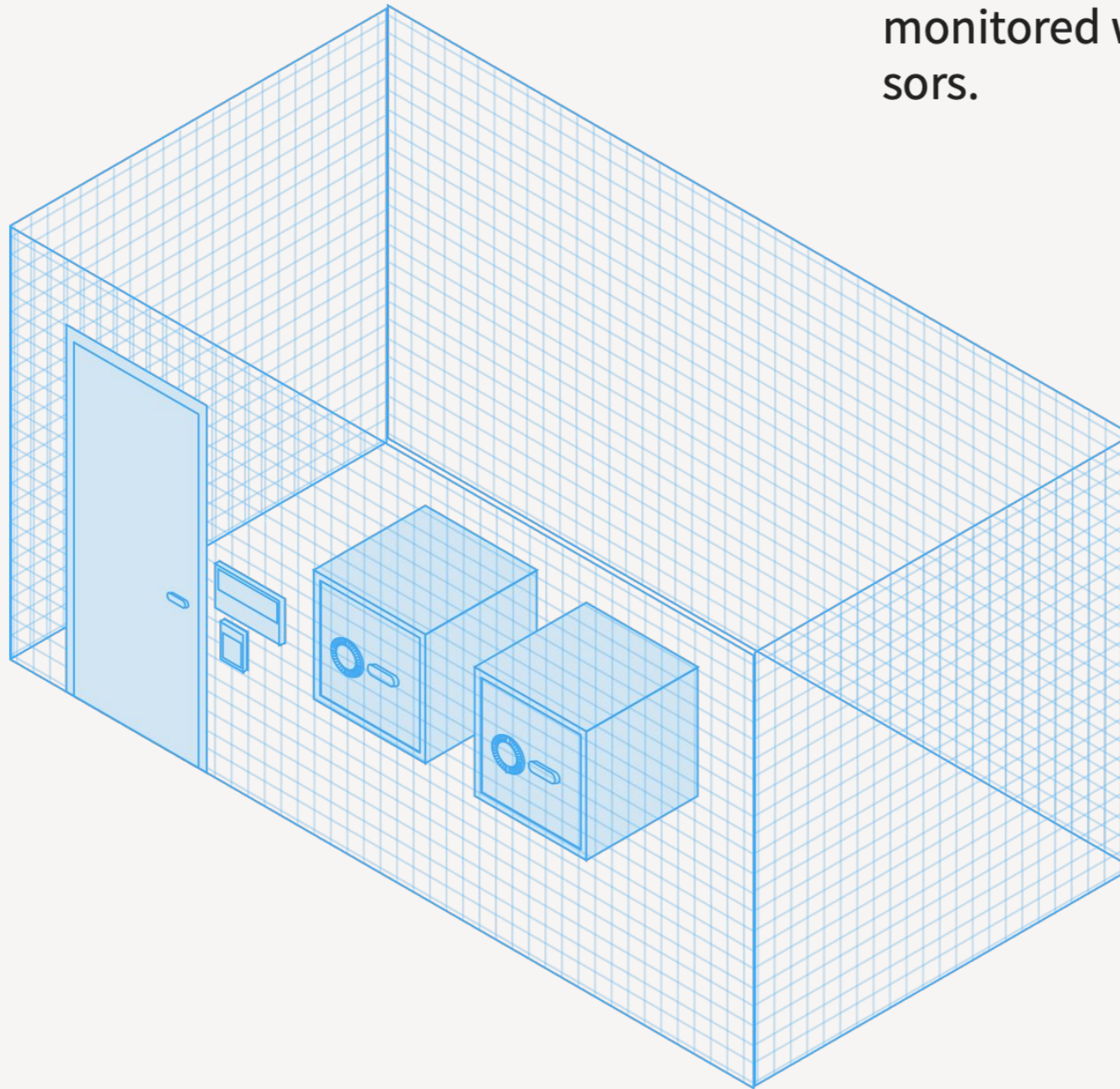


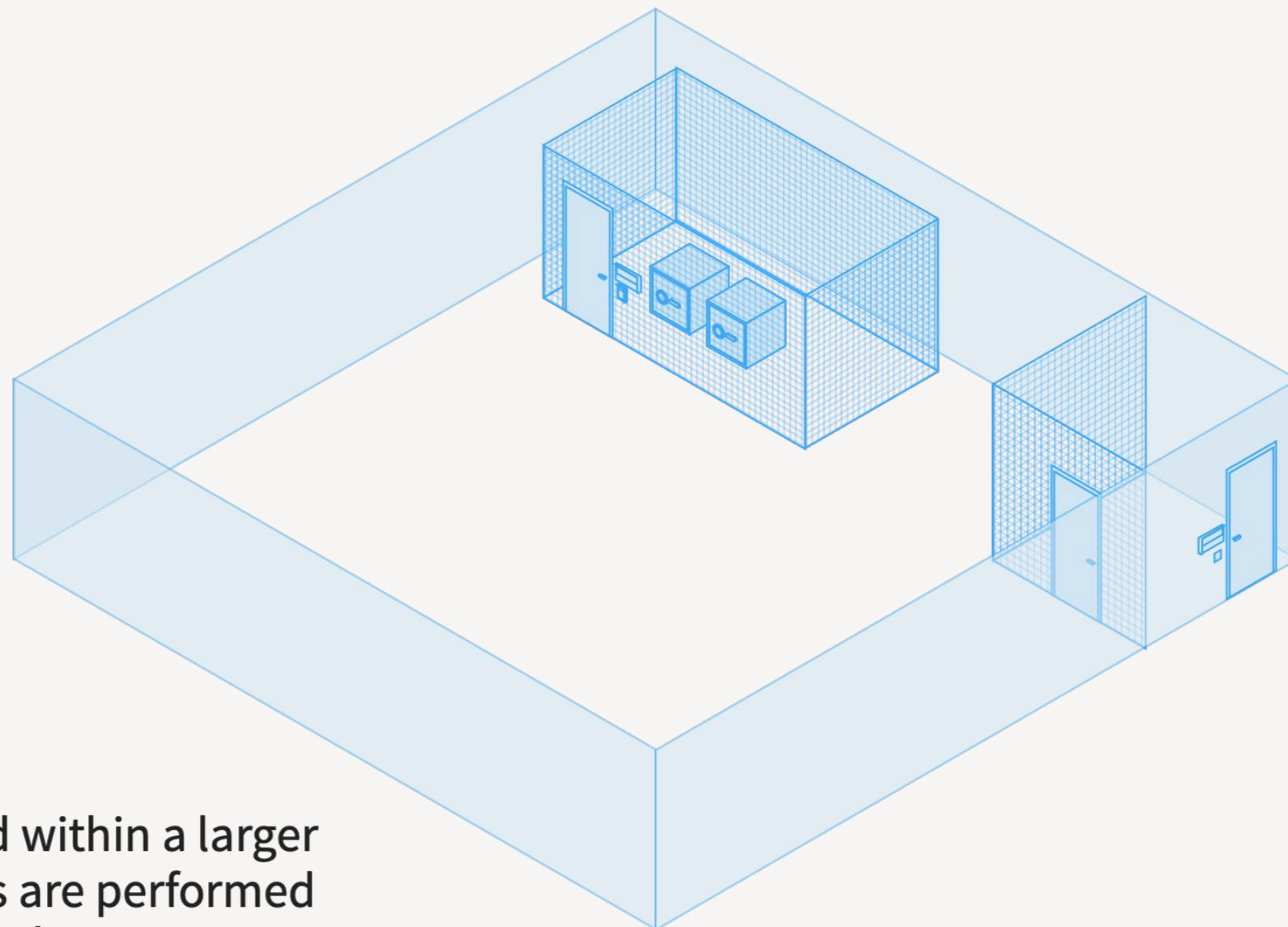
Each smart card is given to a different ICANN community member, known as a **trusted community representative**. To access the key signing key, therefore, at least three of these TCRs need to be present.



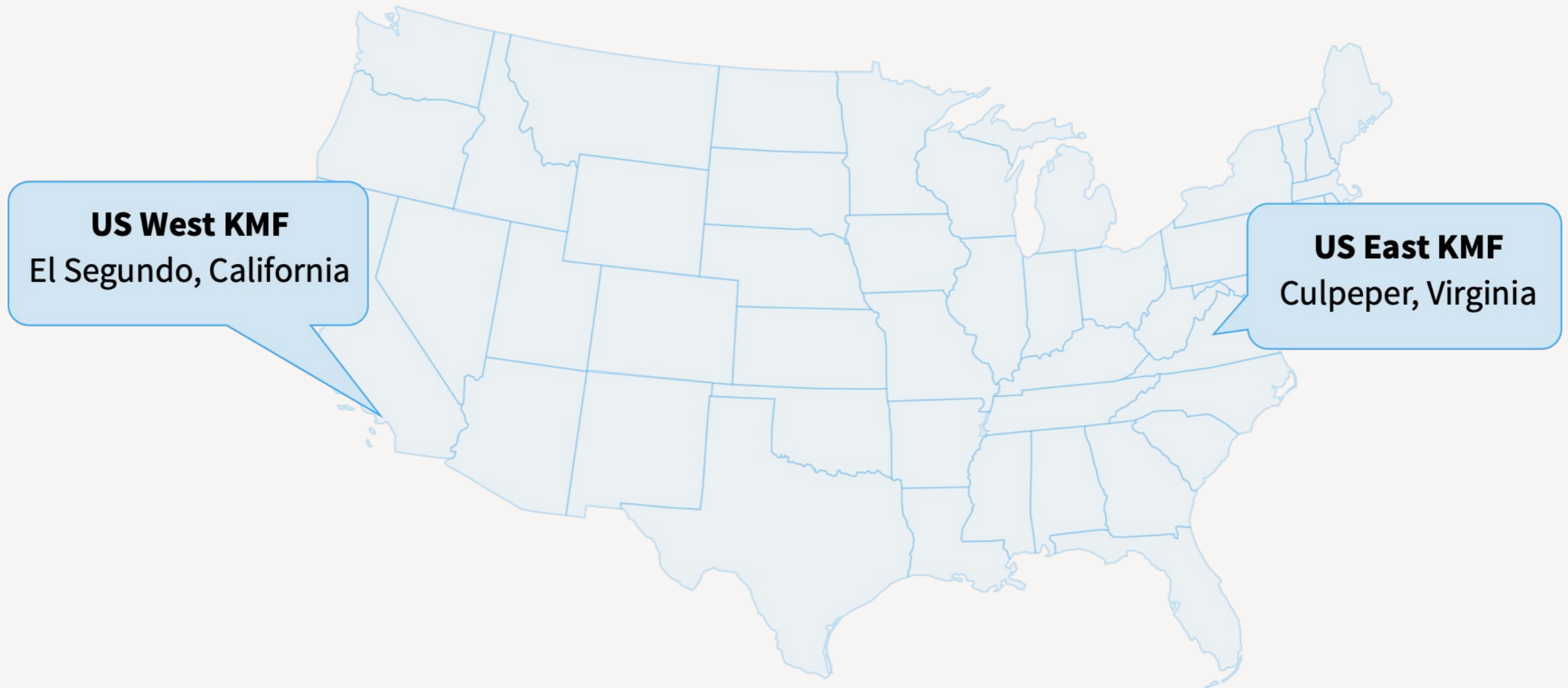
The HSM is stored inside a high-security safe, which can only be opened by a designated person, the **safe security controller**. The safe is monitored with seismic and other sensors.

The safes are stored in a secure room which can only be opened jointly by two designated persons, the **ceremony administrator** and the **internal witness**. The room is monitored with intrusion and motion sensors.





The safe room is located within a larger room where ceremonies are performed involving the TCRs and other persons. Ceremonies are recorded on video, witnessed by the participants and others, and audited by a third party audit firm. Access to the room needs to be granted by another designated person, the **physical access control manager**, who is not on-site.



The ceremony rooms, known as **key management facilities**, are located within two guarded facilities, one each on the US West and East coasts.

# The ceremonies

---

- ▶ Approximately four times a year, the TCRs and others meet to use the HSMs to sign keys to be used for the root zone.
- ▶ The process is streamed and recorded, with external witnesses watching every step. All materials (videos, code, scripts, etc.) are posted online at [iana.org/dnssec](http://iana.org/dnssec)
- ▶ The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the HSMs have not been compromised.
- ▶ Media presence:
  - ▶ The Guardian  
<http://goo.gl/JvPu62>
  - ▶ Vice News  
[https://video.vice.com/en\\_ca/video/this-is-the-nerdy-ceremony-that-keeps-the-internet-running/5a8ce4fbf1cdb31ab85c1221](https://video.vice.com/en_ca/video/this-is-the-nerdy-ceremony-that-keeps-the-internet-running/5a8ce4fbf1cdb31ab85c1221)

---

**Questions?**