
ICANN
ICANN | 52
Singapore
8-12 FEBRUARY 2015

IANA: Who, What, Why?

(or, *Why the IANA functions are less interesting than you thought*)

Elise Gerich, Kim Davies
IANA Department

IANA Department — Who Are We?

Elise

Kim

Naela

Michelle

Pearl

Amanda

Selina

Paula

Andres

Punky

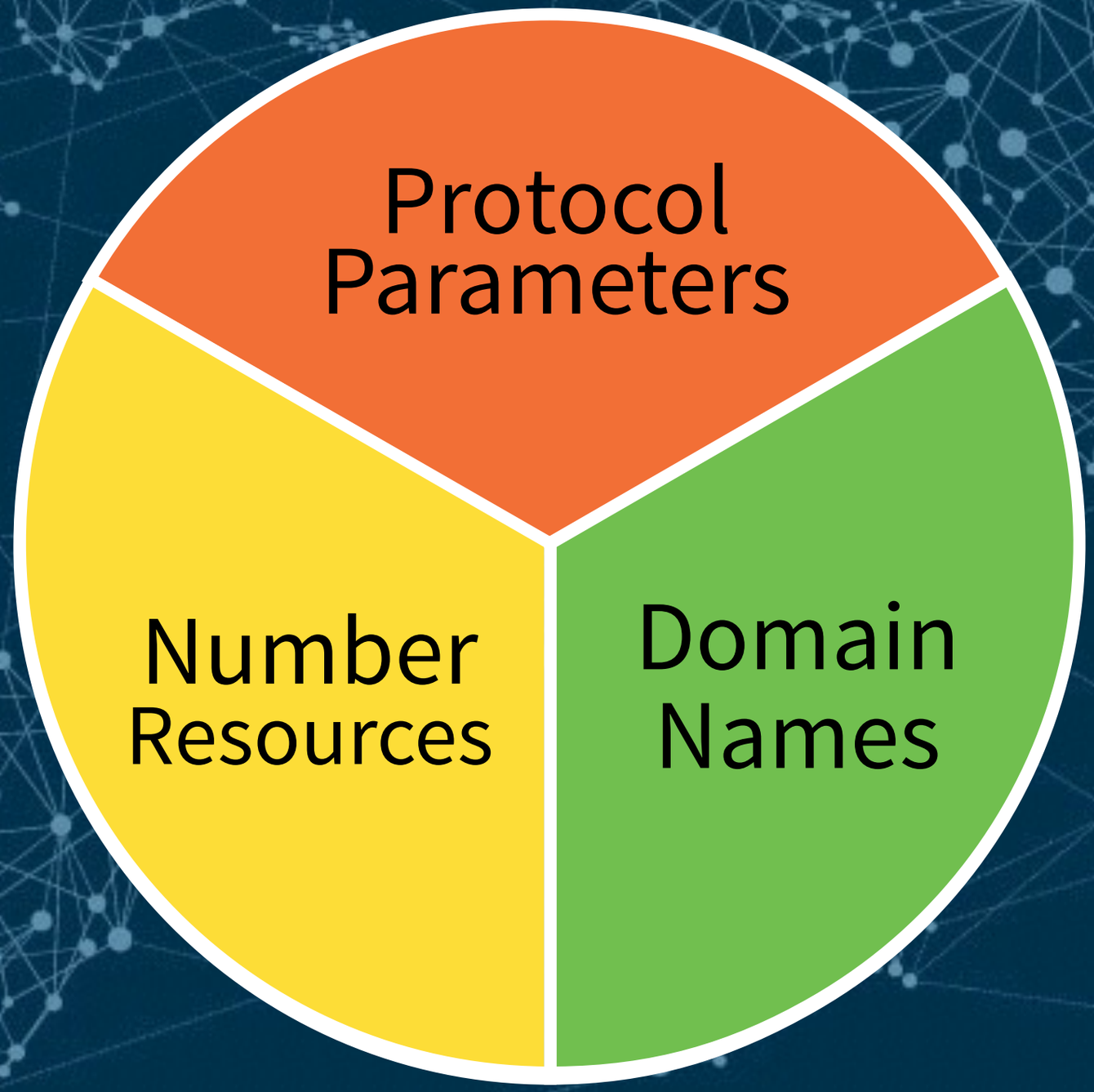
Marilia

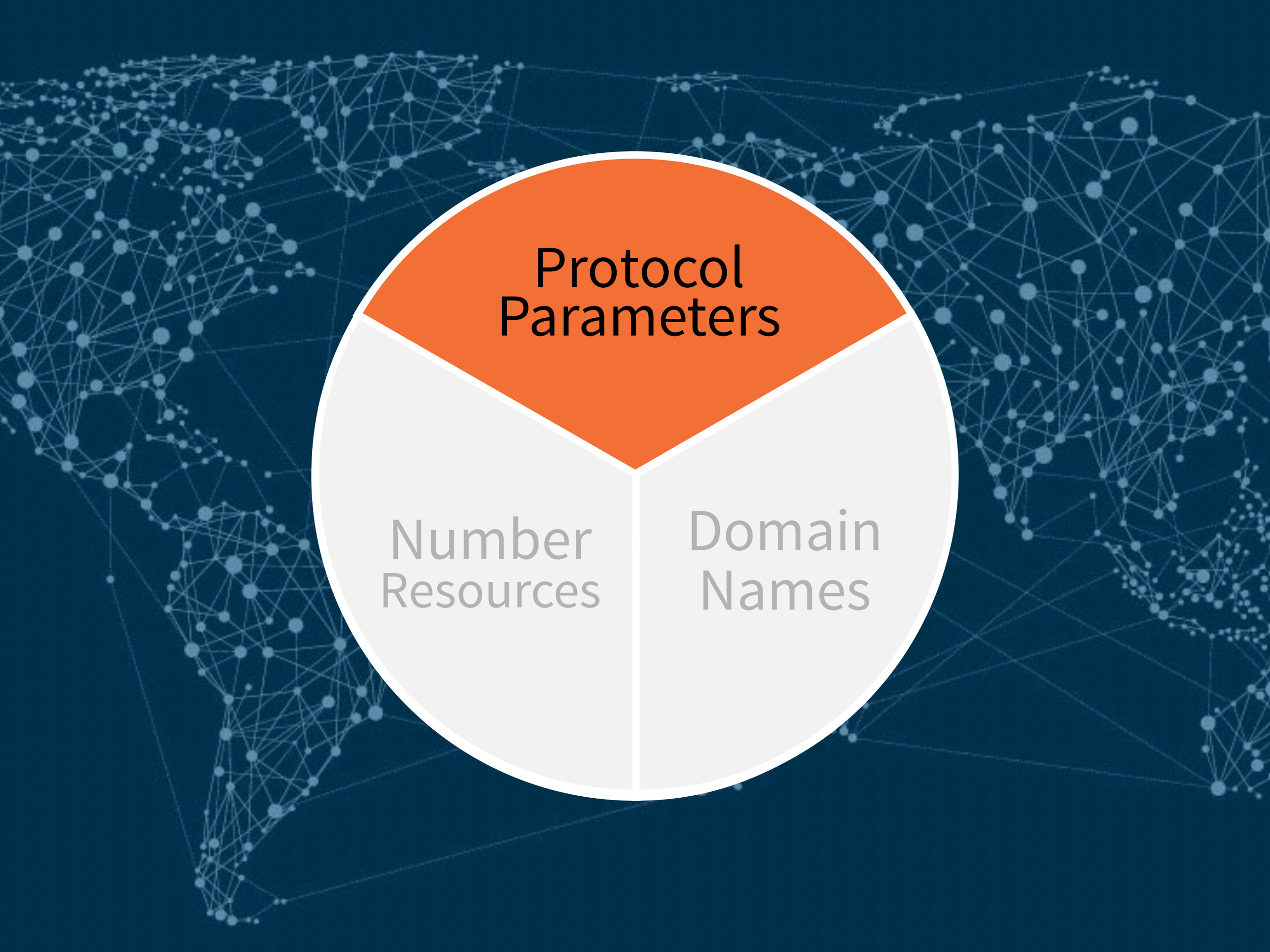
What Are the IANA Functions?

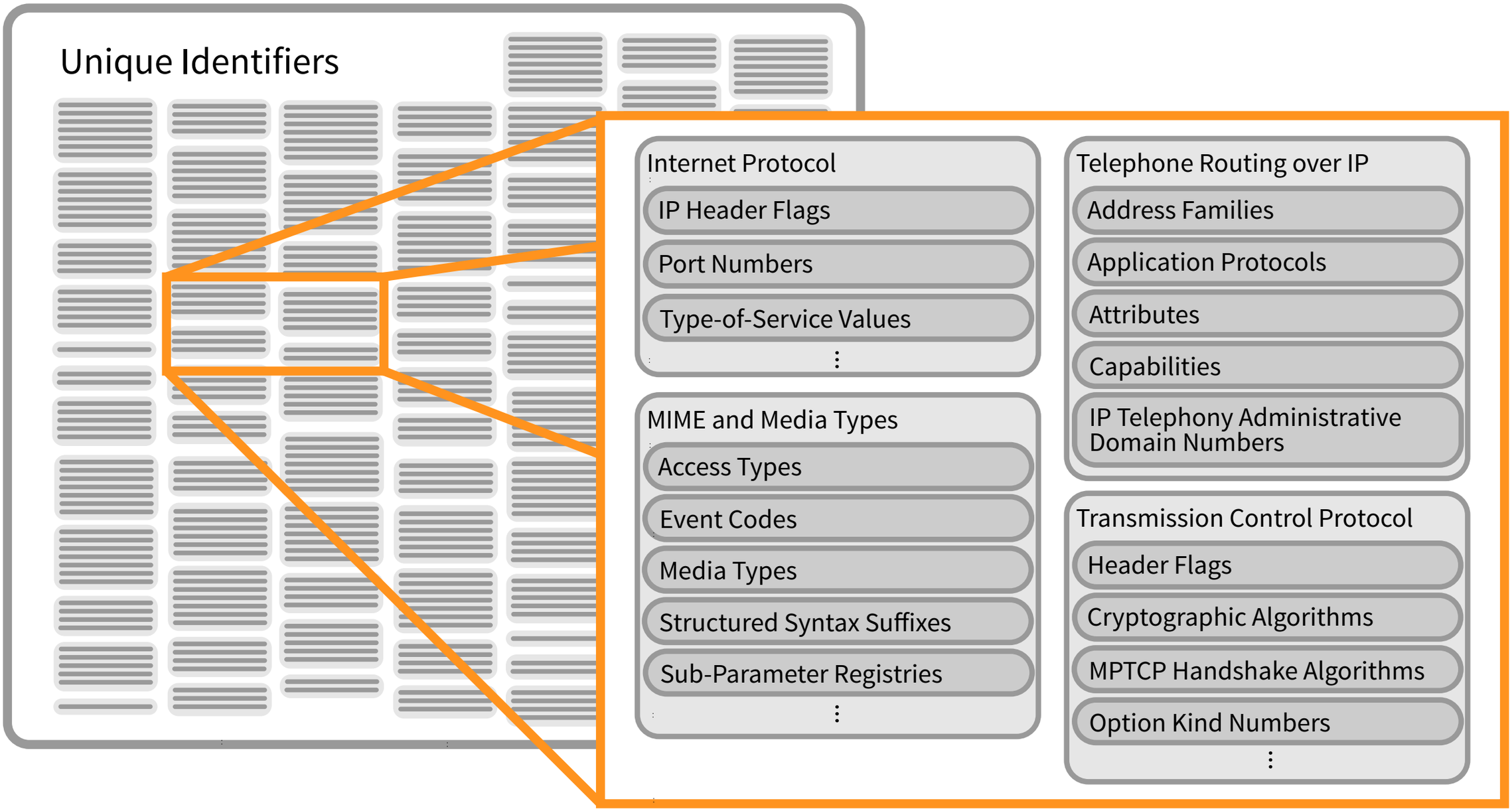
- In 1998, ICANN was established as the steward and operator of the IANA functions
- The IANA Department within ICANN maintains the registries of the Internet's unique identifiers
- The unique identifiers include protocol parameters, Internet numbers and domain names
- The IANA Department maintains these lists according to policies adopted by Internet names, numbers and protocol standards communities

Why Does the IANA Department Exist?

- The IANA Department within ICANN coordinates the Internet unique identifier systems needed to ensure the Internet interoperates globally
- If computers did not use the same system of identifiers and numbers to talk to one another, the system would not interoperate
- The authoritative registries are used by vendors, service providers, businesses, application developers and others to innovate and expand the use of the Internet


Protocol Parameters
Number Resources
Domain Names


Protocol Parameters
Number Resources
Domain Names



Comprehensive index of protocol parameter registries at **iana.org/protocols**

Where do protocol parameter registries come from?

- The Internet Engineering Task Force (IETF) community writes Internet Drafts (I-Ds)
- When approved by the leadership of the IETF, these I-Ds become official Requests for Comments (RFCs)
- Many RFCs contain guidance to the IANA Department:
  - Instructions on the creation of a unique registry for protocol parameters
  - Registration policy
  - Initial registrations and reserved values

What is the IANA Department's role with protocol parameter registries?

- **Before RFC approval:**
  - Review
- **After RFC approval:**
  - Implementation
  - Maintenance

Reviewing Internet Drafts before RFC approval

```
7.  IANA Considerations

7.1.  Registry for the fedfsAnnotation Key Namespace

   This document defines the fedfsAnnotation key in Section
4.2.1.6.  The fedfsAnnotation key namespace is to be managed by
IANA.  IANA is to create and maintain a new registry entitled
"FedFS Annotation Keys".  The location of this registry should
be under a new heading called "Federated File System (FedFS)
Parameters".  The URL address can be based off of the new
heading name, for example:
http://www.iana.org/assignments/fedfs-parameters/ ...

   Future registrations are to be administered by IANA using the
"First Come First Served" policy defined in [RFC5226].
Registration requests MUST include the key (a valid UTF-8 string
of any length), a brief description of the key's purpose, and an
email contact for the registration.  For viewing, the registry
should be sorted lexicographically by key.  There are no initial
assignments for this registry.
```

Work closely with the IETF community to make sure the “IANA Considerations” section of I-Ds is clear

Implementation and Maintenance for protocol

- After RFC approval:
  - **Creation** of new registries and/or **updates** to existing registries
  - **Maintain** through accepting registration requests from the Internet community
  - Follow the registration policy for new registrations and modification to existing registrations
  - Update references

How many registries does the IANA Department maintain?

over **2,800** protocol parameter registries and sub-registries

iana
Internet Assigned Numbers Authority

DOMAINS NUMBERS PROTO

Protocol Registries

Protocol Registries
Time Zone Database
IANA's Performance
IETF Draft Status

Protocol Registries

IANA is responsible for maintaining many of the codes and numbers contained in a variety of Internet protocols, enumerated below. We provide this service in coordination with the Internet Engineering Task Force (IETF).

For more information on how to create registries, please see RFC 5226, Section 4. This document also covers the requirements for IANA Considerations in RFCs.

To view the various protocol registries, just click on their titles. To apply to modify a registry, use the relevant form. The qualifications for changing a protocol vary depending on the governing standards documents.

A B C D E F G H I J K L M N O P Q R S T U V W X Y

Protocol/Registry	Defining Document/Comments
	A
Access Node Control Protocol (ANCP)	
ANCP Capability Types	RFC 6320 Standards Action
ANCP Command Codes	RFC 6320 Standards Action
ANCP Message Types	RFC 6320 Standards Action
ANCP Port Management Functions	RFC 6320 Standards Action
ANCP Result Codes	RFC 6320 0x0-0xFFF: IETF Review. 0x1000-0xFFFFFF: Specification Required.
ANCP Technology Types	RFC 6320

ICANN

Processing Protocol Parameter Requests

Request

What type of protocol parameter is being requested?

Registration Policy

Look at the named registry to determine which registration policy to follow. **Defining RFC determines the policy.**

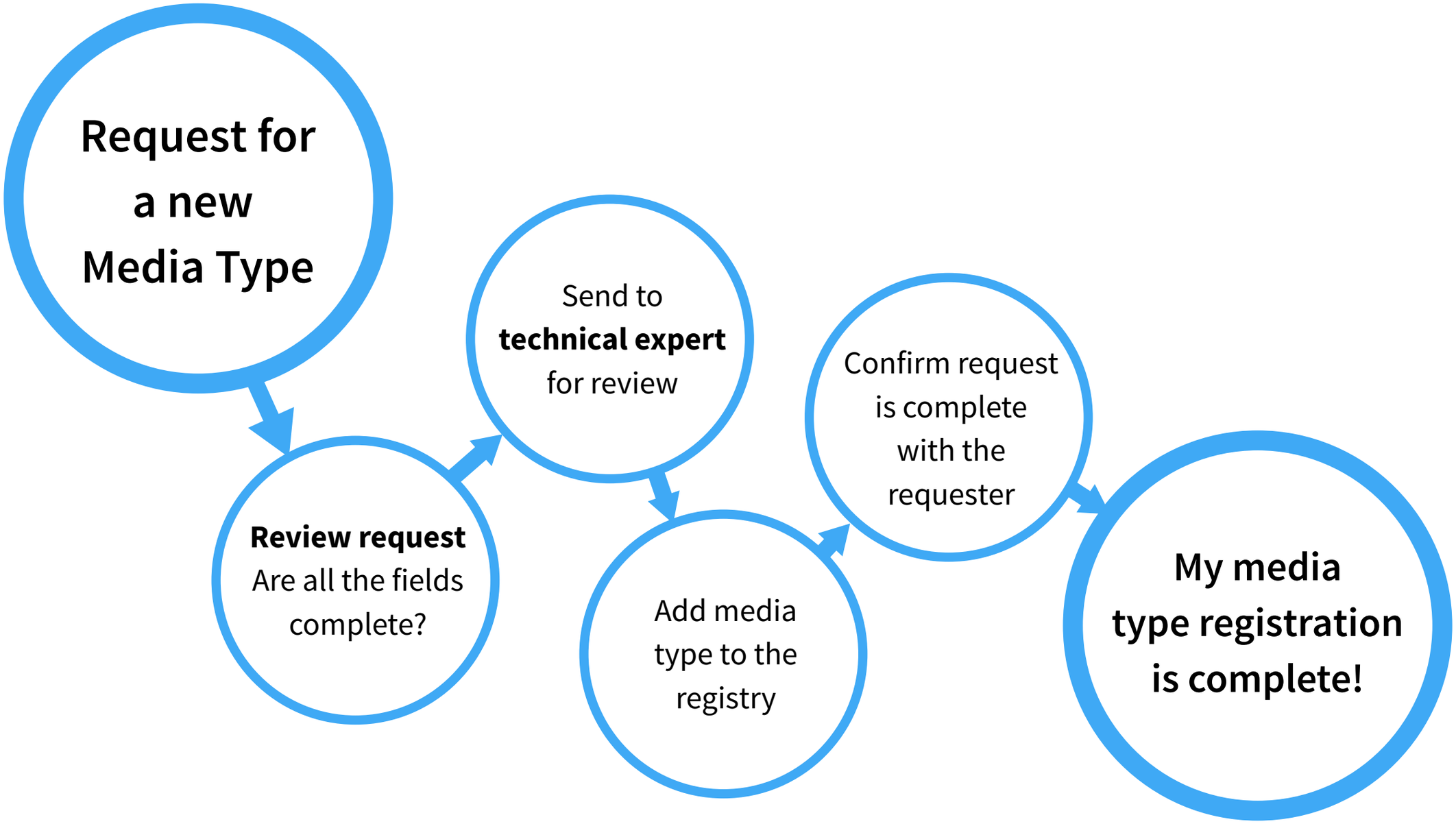
Processing and Evaluation

- Follow the appropriate process according to registration policy
- Consult with experts if required
- Gather more information from requester if needed

Update Registry

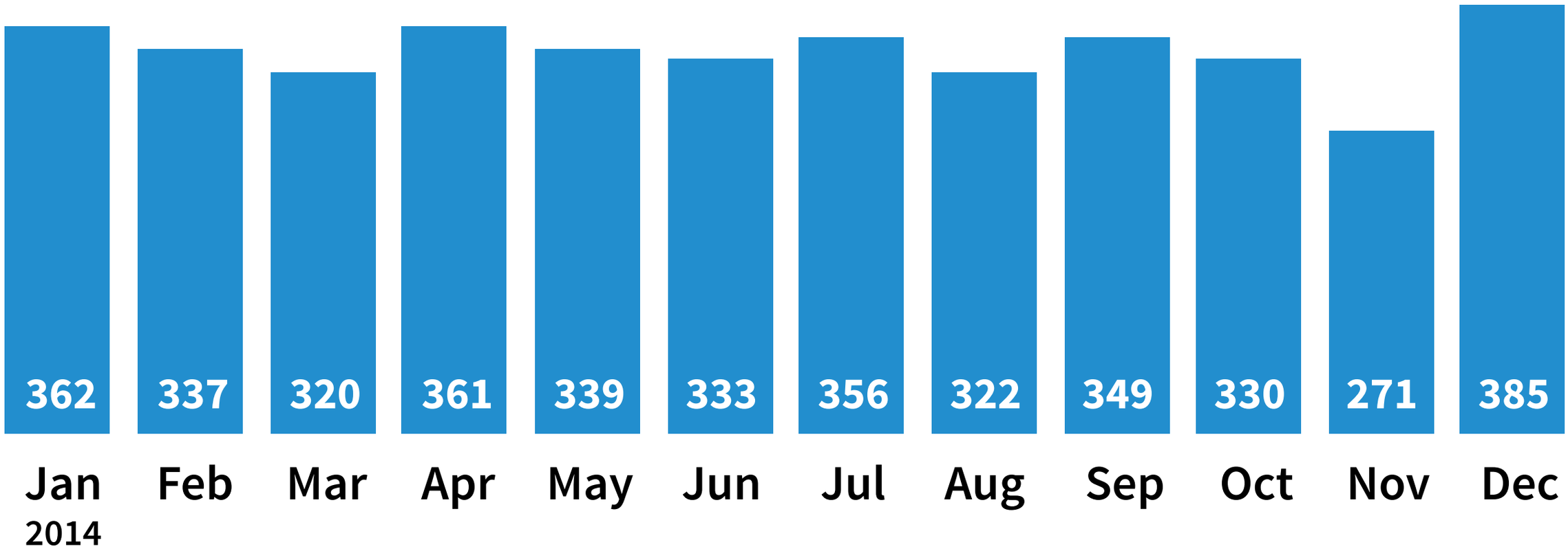
- Make protocol parameter assignment in registry
- Notify the requester the registration is complete

Processing Protocol Parameter Requests



Requests per month

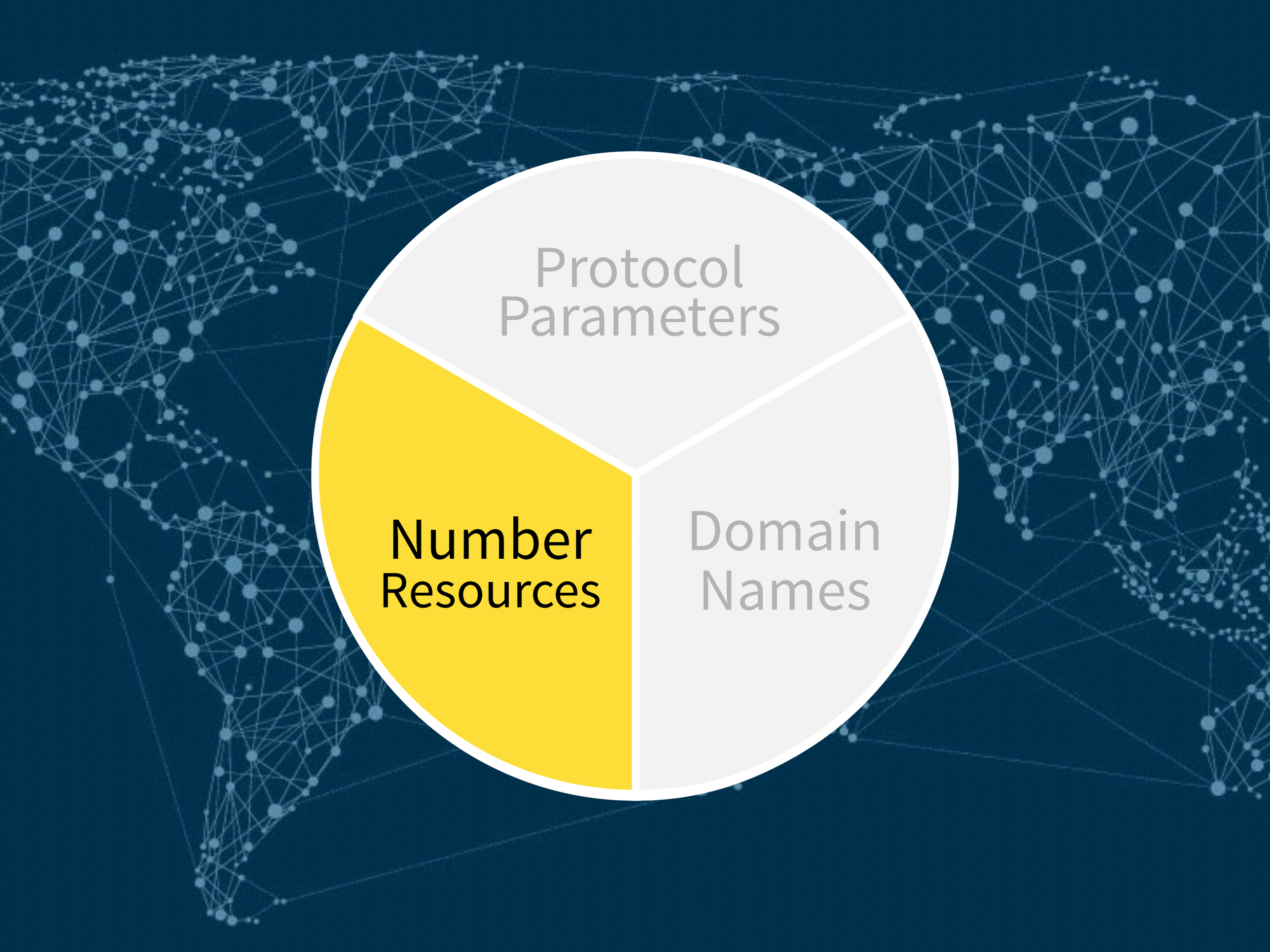
ICANN processes approximately 4,000 protocol parameter requests per year

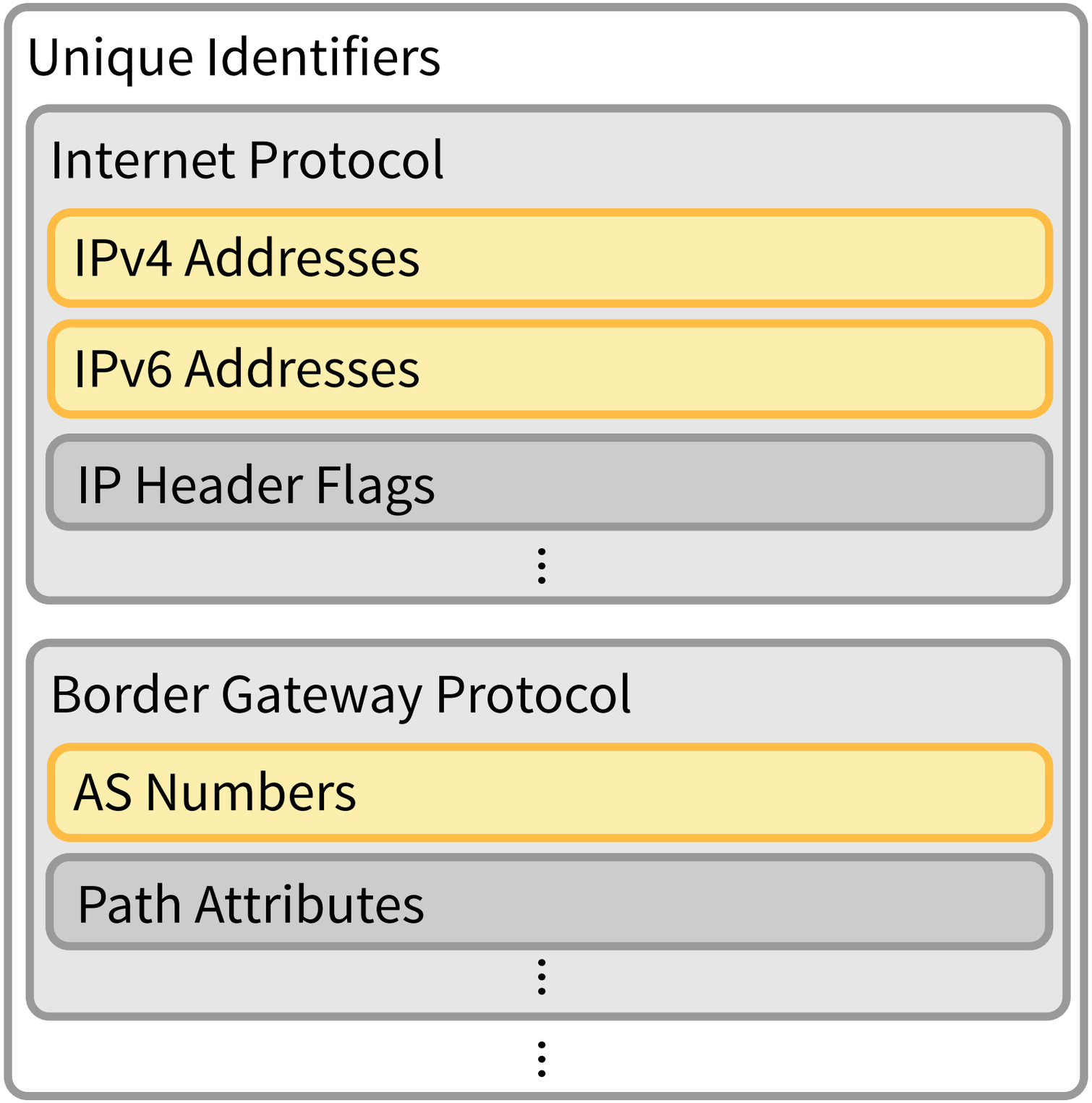


Performance Targets

- Performance standards were developed collaboratively with the IETF to supplement the existing MoU between ICANN and the IETF
- Began reporting in 2007 on the Service Level Agreement deliverables
- SLA is reviewed, modified and approved annually

2014	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
SLA Met	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
KPIs Met	99%	98%	99%	99%	100%	99%	100%	99%	100%	99%	100%	99%


Protocol Parameters
Number Resources
Domain Names


Unique Identifiers
Internet Protocol
IPv4 Addresses
IPv6 Addresses
IP Header Flags
Border Gateway Protocol
AS Numbers
Path Attributes

Deterministic Decision Making

- The policies have deterministic formulas governing **when** an RIR can get more and **how much** they can get
- IPv4 is allocated on a schedule and not by request
- IPv6 and AS Numbers are allocated on receipt of a justified request
- Staff validate what an RIR reports against what it publishes via its daily stats reports

Allocation Types

- Formula + Request
  (IPv6 and ASN allocations)
- Formula + Schedule
  (IPv4 allocations)
- IETF Allocation Procedures
  (Non-Unicast addresses)

Formula + Request

Request

✓ Comes from an RIR

Do they qualify?

✓ Less than half of a /12 in reserve

or

✓ Not enough to last 9 months

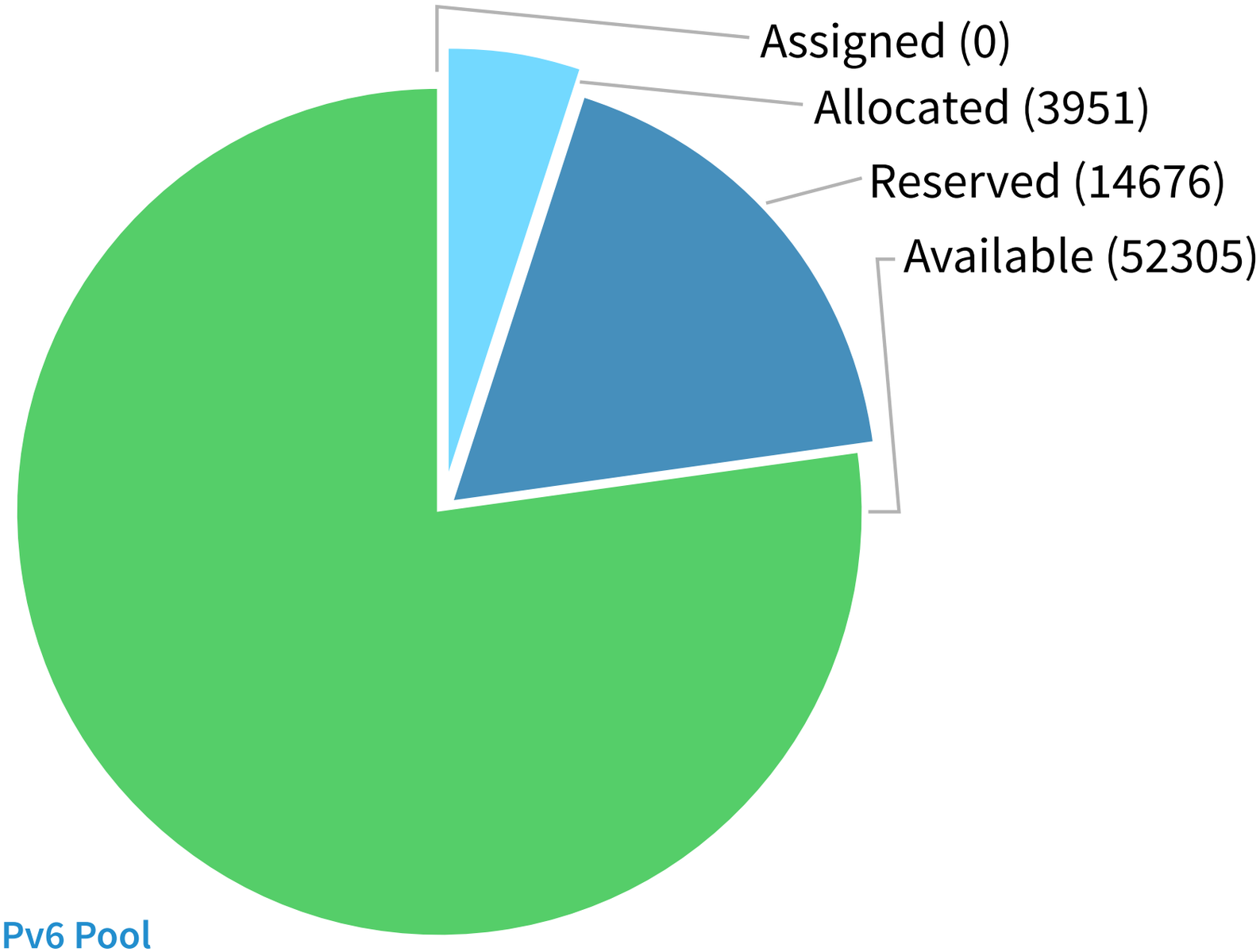
What do they get?

$$n = \frac{(\text{6mo usage}) \times 18}{\boxed{\text{/12 block}}}$$

$$n \leq 1 \rightarrow 1 \times \boxed{\text{/12 block}}$$

$$n > 1 \rightarrow \lceil n \rceil \times \boxed{\text{/12 block}}$$

Using input data from RIRs



RIPE NCC IPv6 Pool

(As at 2015-02-03; Millions of /48 addresses)

Allocate and Communicate (1)

PREFIX	DESIGNATION	DATE	STATUS
5F00::/8	IANA	2008-04	Reserved
3FFE::/16	IANA	2008-04	Reserved
2C00:0000::/12	AFRINIC	2006-10	Allocated
2A00:0000::/12	RIPE NCC	2006-10	Allocated
2800:0000::/12	LACNIC	2006-10	Allocated
2600:0000::/12	ARIN	2006-10	Allocated
2400:0000::/12	APNIC	2006-10	Allocated
2620:0000::/23	ARIN	2006-09	Allocated
2001:B000::/20	APNIC	2006-03	Allocated

Allocate and Communicate (2)

Communicate allocation to the RIR

Communicate allocation to the operations community

Formula + Schedule

Allocate twice per year

Allocations happen on a pre-defined schedule

Use formula posted online

ICANN publishes the formula used to make selection as open source available for anyone to inspect

github.com/icann/ipv4-recovery-algorithm

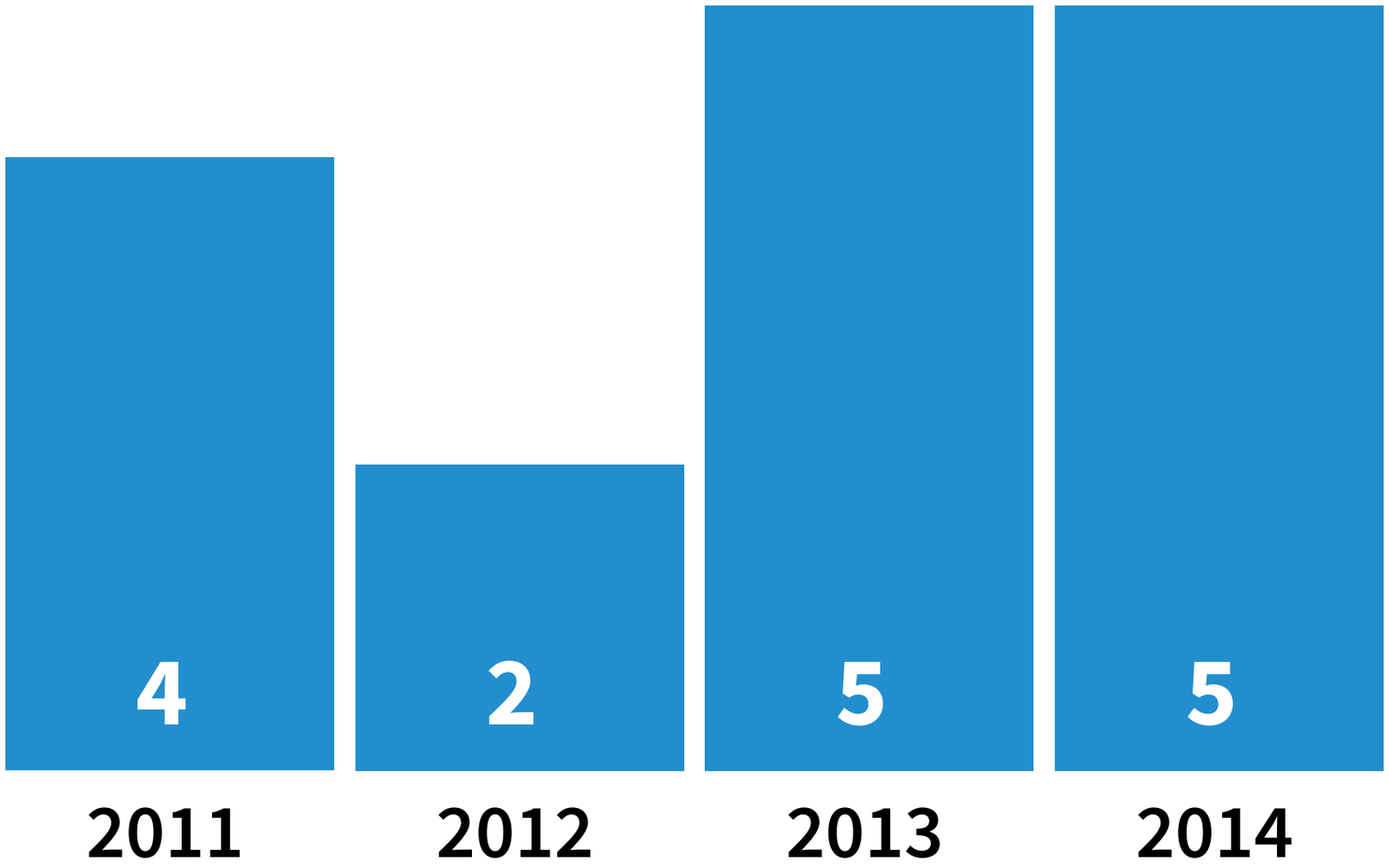
```
def find_best_match(self, amount, allocatee):

    candidates = {}
    for block in self.recovered.entries:
        score = float(math.log(len(block), 2))/32
        if block.preference == allocatee:
            score += 0.8
        if len(block) == amount:
            score += 0.2
        candidates[block] = score
    for block in reversed(sorted(candidates.iteritems(), key=operator.
        size = block[0].end - block[0].start + 1
        if size > amount:
            return (block[0].start, IPv4Address(block[0].start + amou
        else:
            return (block[0].start, block[0].end)
```

Communicate results

After the formula is applied per the schedule, the results are communicated to the RIRs and operations community, and the IANA registry is updated

iana.org/assignments/ipv4-recovered-address-space

Allocations per year

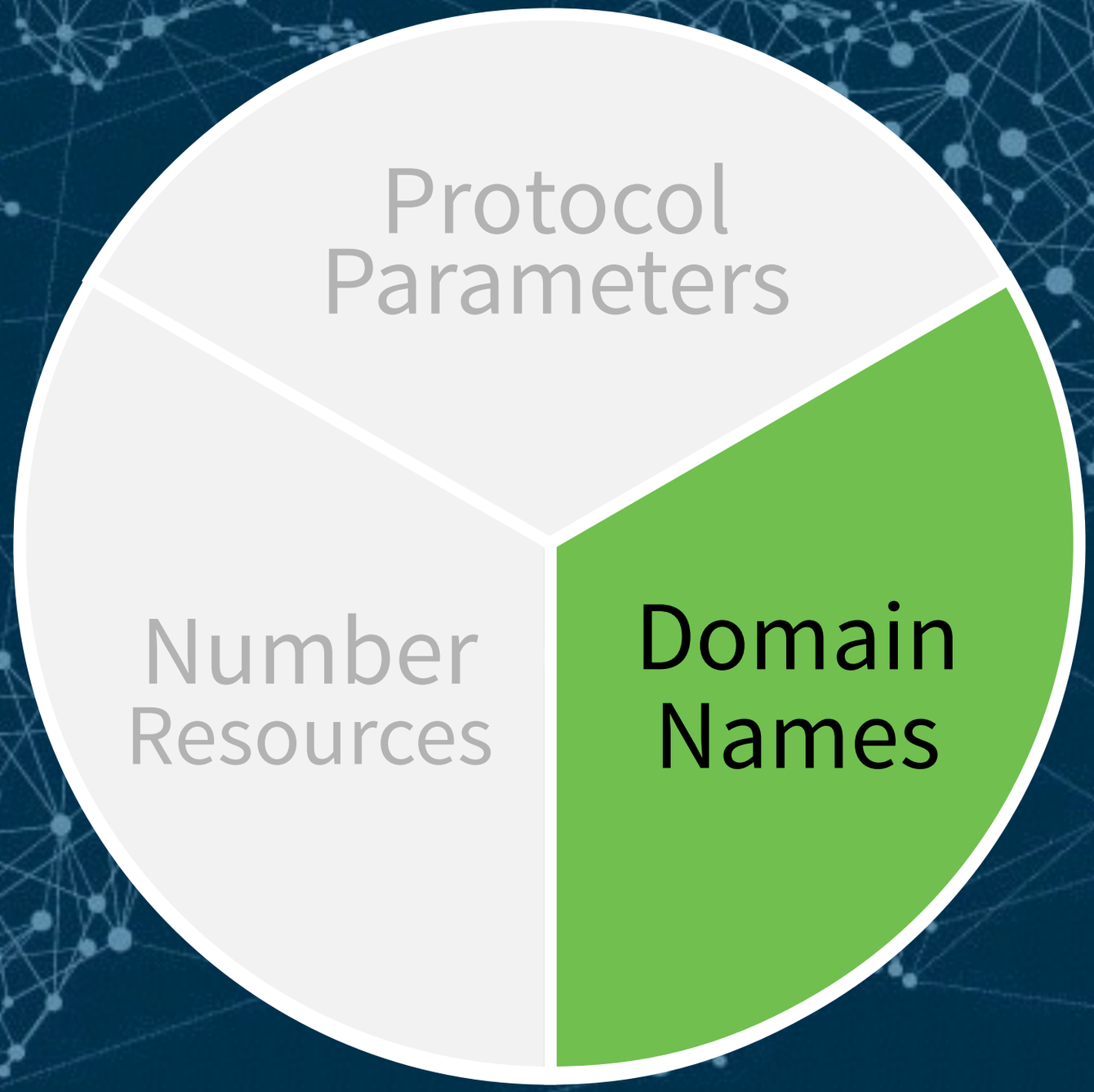


Performance Targets

- Formal performance standards consultation in 2012
- Have met or exceeded all targets in 15 of 16 months since public reporting began in 2013

Key Performance Indicators

Metric	Target	Actual	Target Met
Accuracy (1) — Policy is correctly implemented.	100%	100%	✓
Accuracy (2) — Registry is updated before notifying requestor of allocation.	100%	100%	✓
Timeliness and Process Quality (1) — For a specific request, ICANN does not need to seek more than two iterations of clarification from the requesting Regional Internet Registry in order to correctly apply the registration policy.	100%	100%	✓
Timeliness and Process Quality (2) — Requests are to be completed within 7 days.	100%	100%	✓
Transparency (1) — Public announcement of an allocation is made on the same day as the allocation being recorded in the IANA registry.	100%	100%	✓
Transparency (2) — An implementation schedule for a new global policies under C.2.9.3 will be posted following ratifications within 14 days for simple policies, and 30 days for complex policies.	100%	100%	✓


Protocol Parameters
Number Resources
Domain Names

Unique Identifiers

Domain Name System

- Domain Name Space
- Domain Resource Record Types
- DNS Security Algorithm Types
- DNS Header Flags

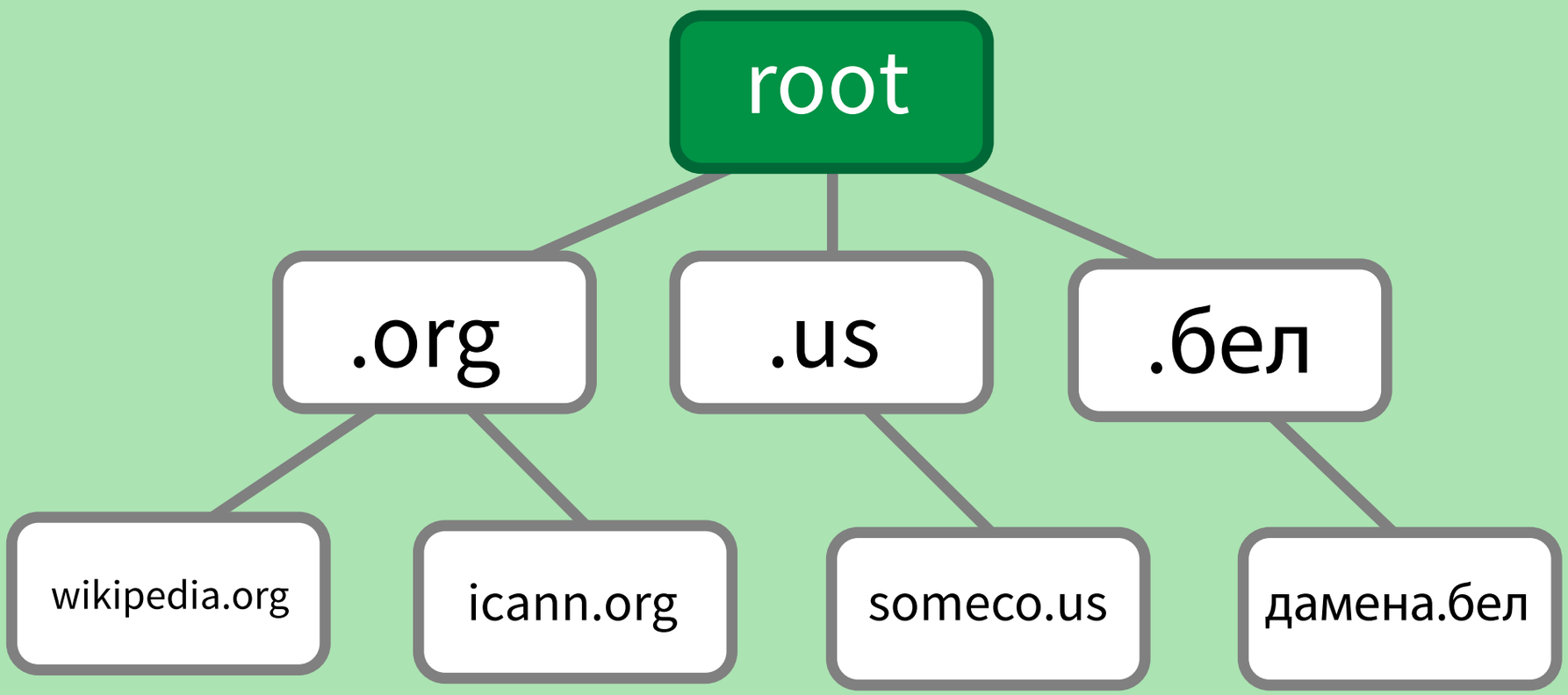
⋮

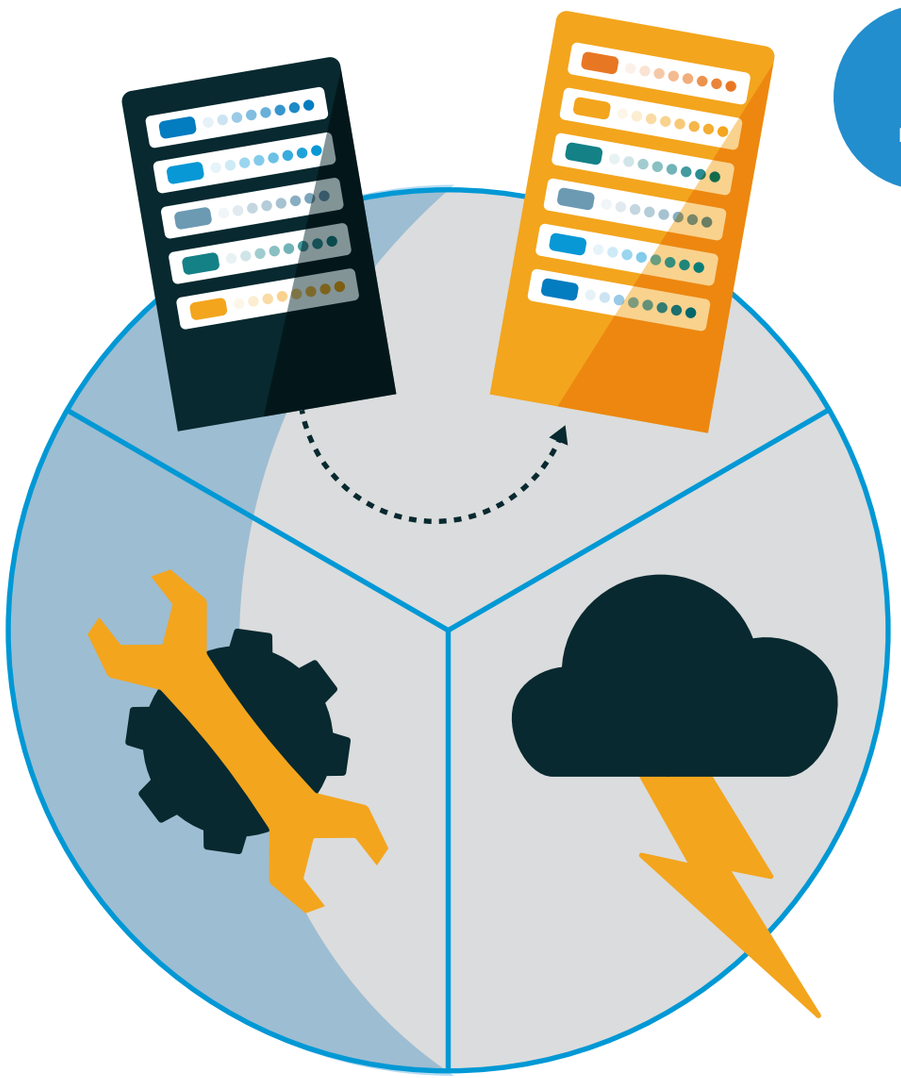
⋮

Unique Identifiers

Domain Name System

Domain Name Space





1

Event Triggers Request

An event such as a change in TLD operator, routine maintenance (technical or staffing change) or a natural disaster triggers the need for a change request.

REGISTRY ENTRY FOR A TOP-LEVEL DOMAIN

Operator

Recognized Company or Organization

Formal Legal Name, Physical Address

Contacts

Administrative Contact

Name, Job Title,
Company, Address,
Phone, Fax, Email

Technical Contact

Name, Job Title,
Company, Address,
Phone, Fax, Email

Technical configuration

Data that goes in the root zone

Authoritative name servers
IP addresses of name servers
DNSSEC (“DS”) records

Metadata

Courtesy information not tied to operations

URL to Operator’s website, location of WHOIS service, domain converted to A-label, language etc.

Operator

Hamburg Top-Level-Domain GmbH
Gertigstrasse 28, Hamburg, 22303
Germany

Contacts

Oliver Joachim Sueme
Hamburg Top-Level-Domain GmbH
Gertigstrasse 28, Hamburg, 22303
Germany
Email: os@dothamburg.de
Voice: +49 40 27806736
Fax: +49 40 380 89 810

Martin Schlicksbier
TLD-BOX Registrydienstleistungen
Jakob-Haringer-Strasse 8
5020 Salzburg
Austria
Email: iana@tld-box.at
Voice: +43 662 2345 48730

Technical configuration

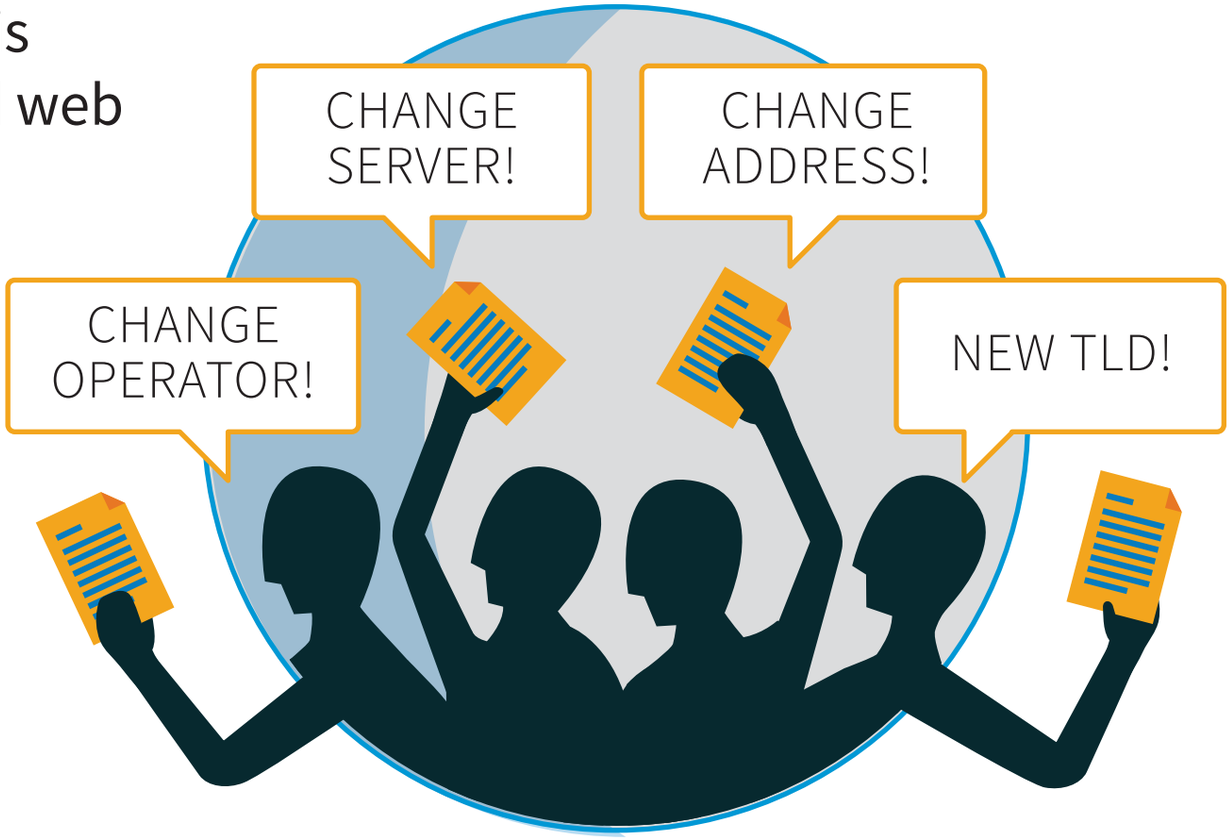
NS a.dns.nic.hamburg (194.0.25.21 2001:678:20:0:0:0:0:21)
NS b.dns.nic.hamburg (193.170.61.10 2001:62a:a:2000:0:0:0:10)
NS c.dns.nic.hamburg (193.170.187.10 2001:62a:a:3000:0:0:0:10)
DS 53866 8 2 AF2F53F6B523F31C04A741B3826D27CBAE16F4BA6F...
DS 26479 8 1 1C9F5D68C413E8A9A2C8E1C1637B8A4DA2CA6827
DS 26479 8 2 4A48334EF87D7FC156E886E5A2B2682FCF0679ED6FC...
DS 53866 8 1 D26808AE1E19086BCF5FC88D59066C3AD22F2E56

Metadata

http://www.dothamburg.de
whois.nic.hamburg

2 Change Request

A TLD operator submits a change request to IANA Department within ICANN. This is typically done through an automated web service ICANN provides called the Root Zone Management System (RZMS).



3 Policy Check

ICANN checks that the change request meets policy and technical requirements and confirms consent from the appropriate parties. If issues are found, ICANN clarifies with the TLD operator. Then, ICANN forwards the request to NTIA for authorization to proceed.

Technical

- ✓ Name Servers are responding
- ✓ Name Servers return correct data that matches the request
- ✓ DNS data can be verified using the supplied DNSSEC DS records
- ✓ Supplied email addresses work

Regulatory

- ✓ Request meets legal requirements

Well-formedness

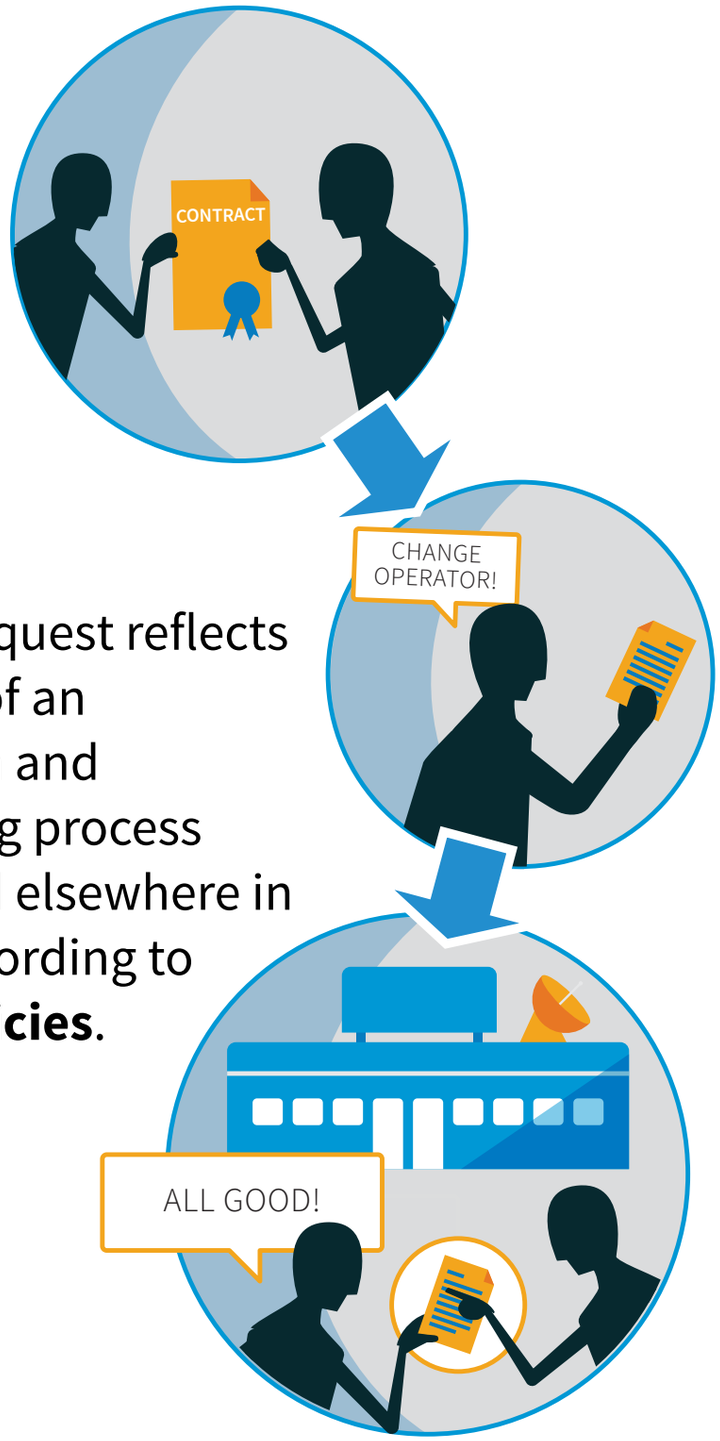
- ✓ Supplied data is clear, well-formed and consistent

Consent

- ✓ Existing contacts agree to change
- ✓ New contacts agree to their new responsibilities
- ✓ Other impacted TLDs agree

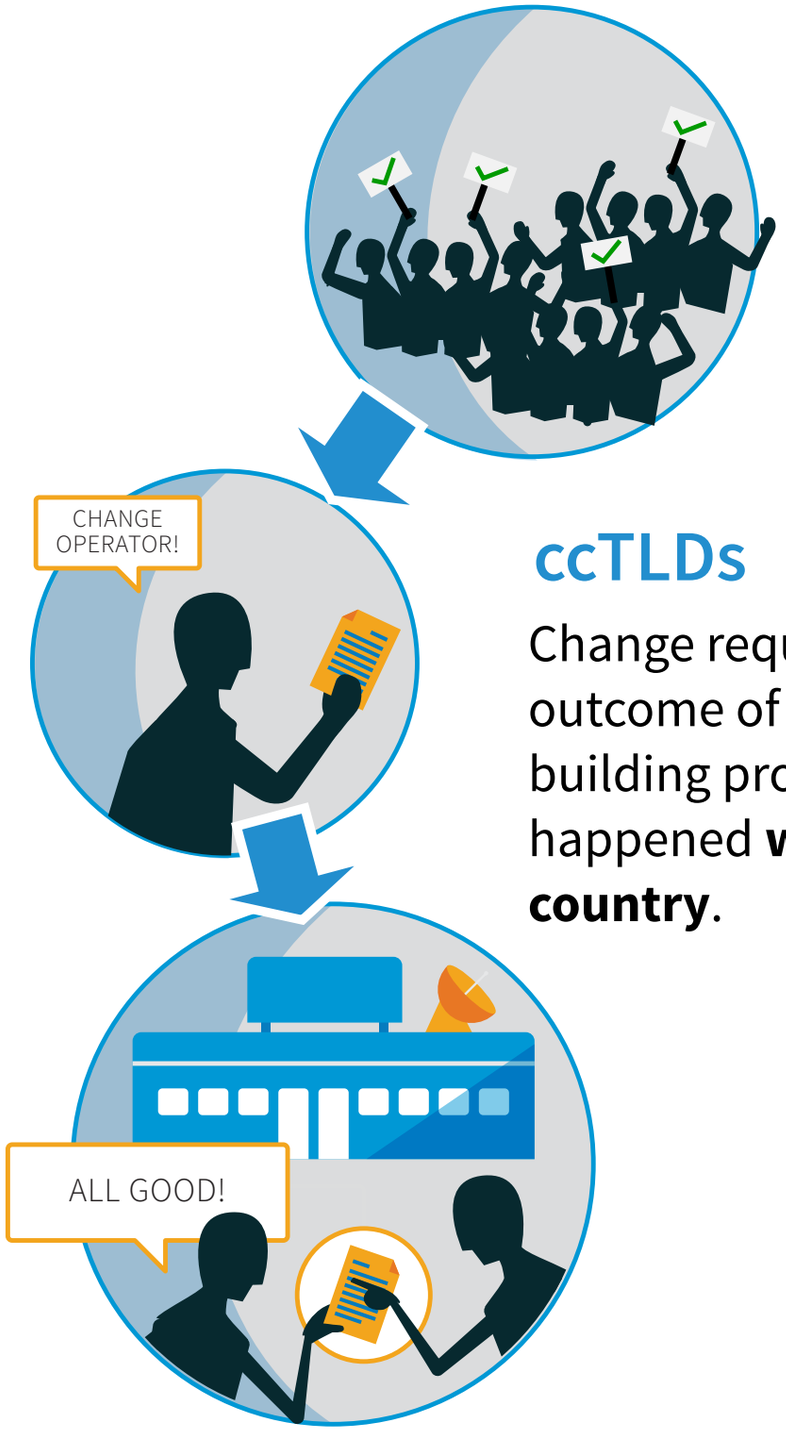
Transfer of responsibility

- ✓ Meets policy requirements for transfers (differs between ccTLDs and gTLDs)



gTLDs

Change request reflects outcome of an evaluation and contracting process conducted elsewhere in ICANN according to **GNSO policies**.



ccTLDs

Change request reflects outcome of a consensus building process that happened **within the country**.

4 Verification

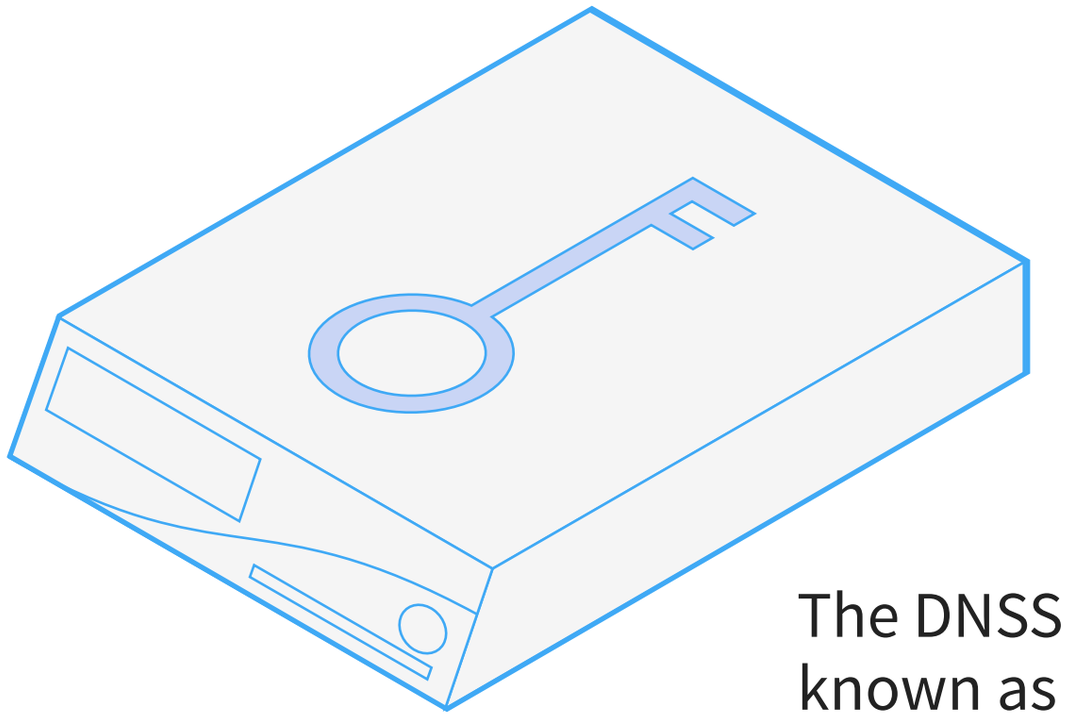
Changes that satisfy the policy requirements are transmitted to NTIA for verification. NTIA reviews the change and then gives authorization to proceed with publishing the change.

5 Implement changes

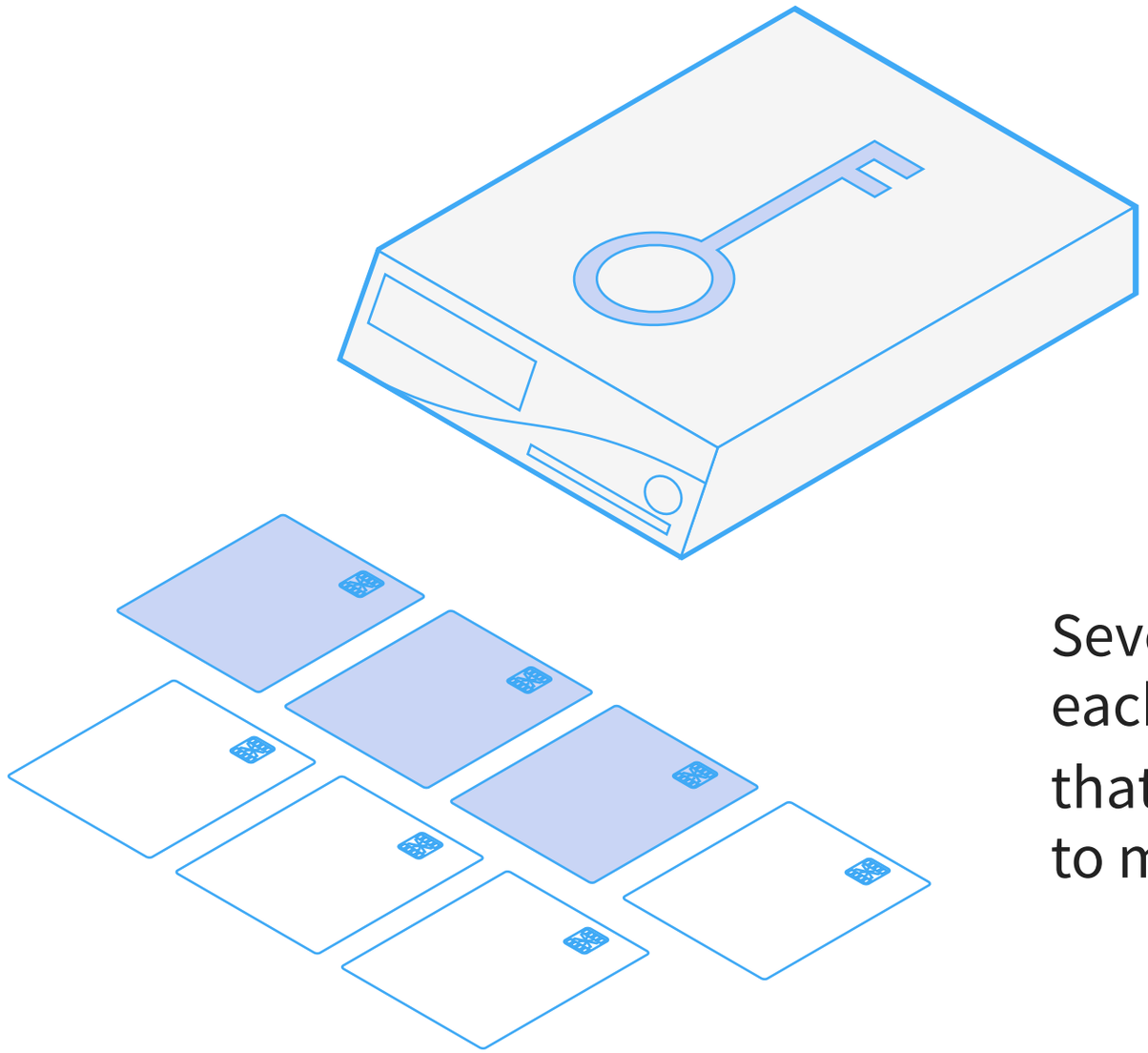
After authorization to proceed, any technical changes to the root zone are implemented. This includes applying a tamper-evident seal using DNSSEC, and distributing the updated root zone file to root server operators. The Root Zone Database is updated with the changes.

The Root Key Signing Key

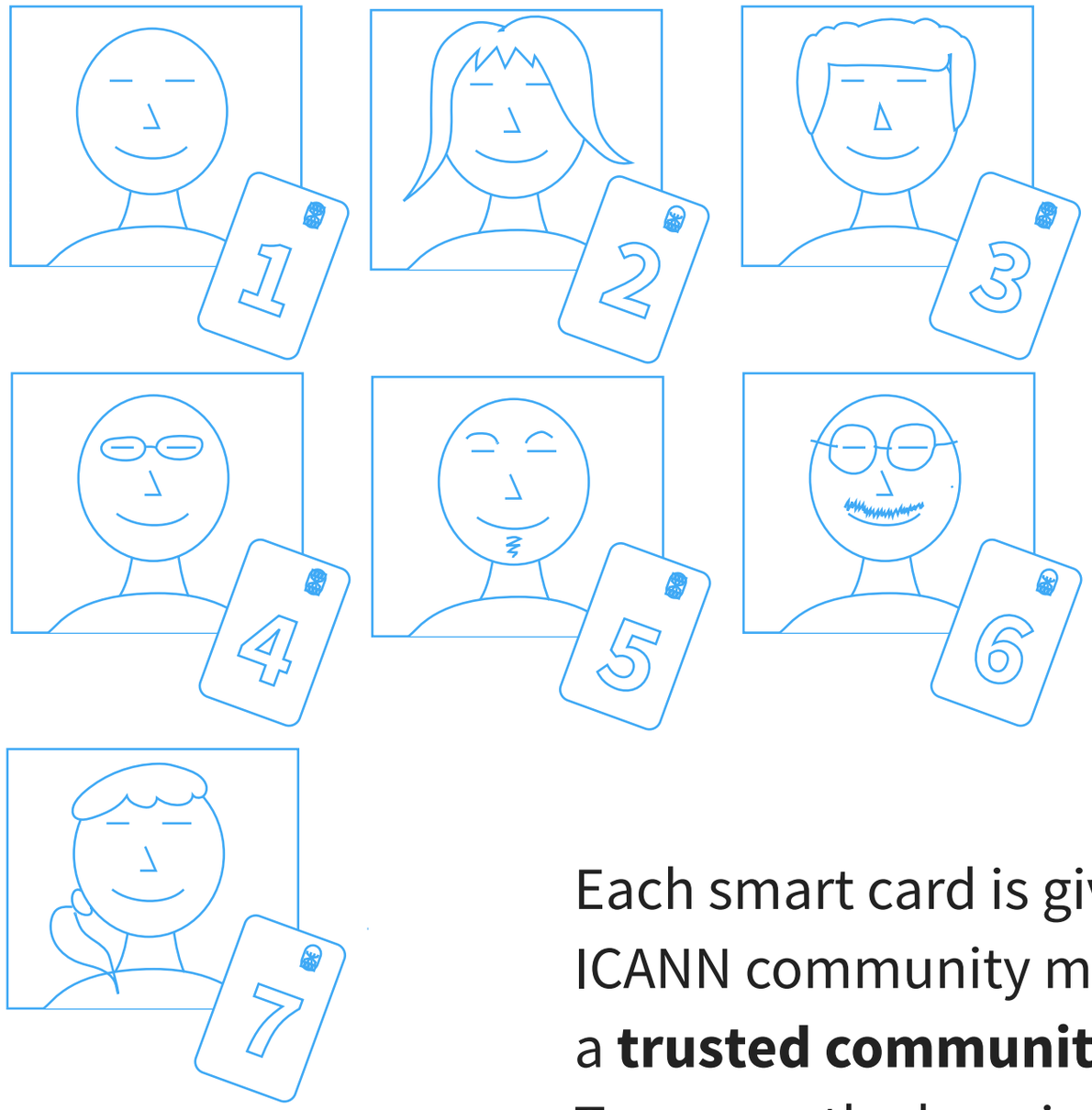
- As part of its root zone related functions, the IANA Department manages the **key signing key**, used to secure the DNS with the DNSSEC protocol.
- An auditable process of performing **key signing ceremonies** to use this key is conducted using members of the community as key participants.



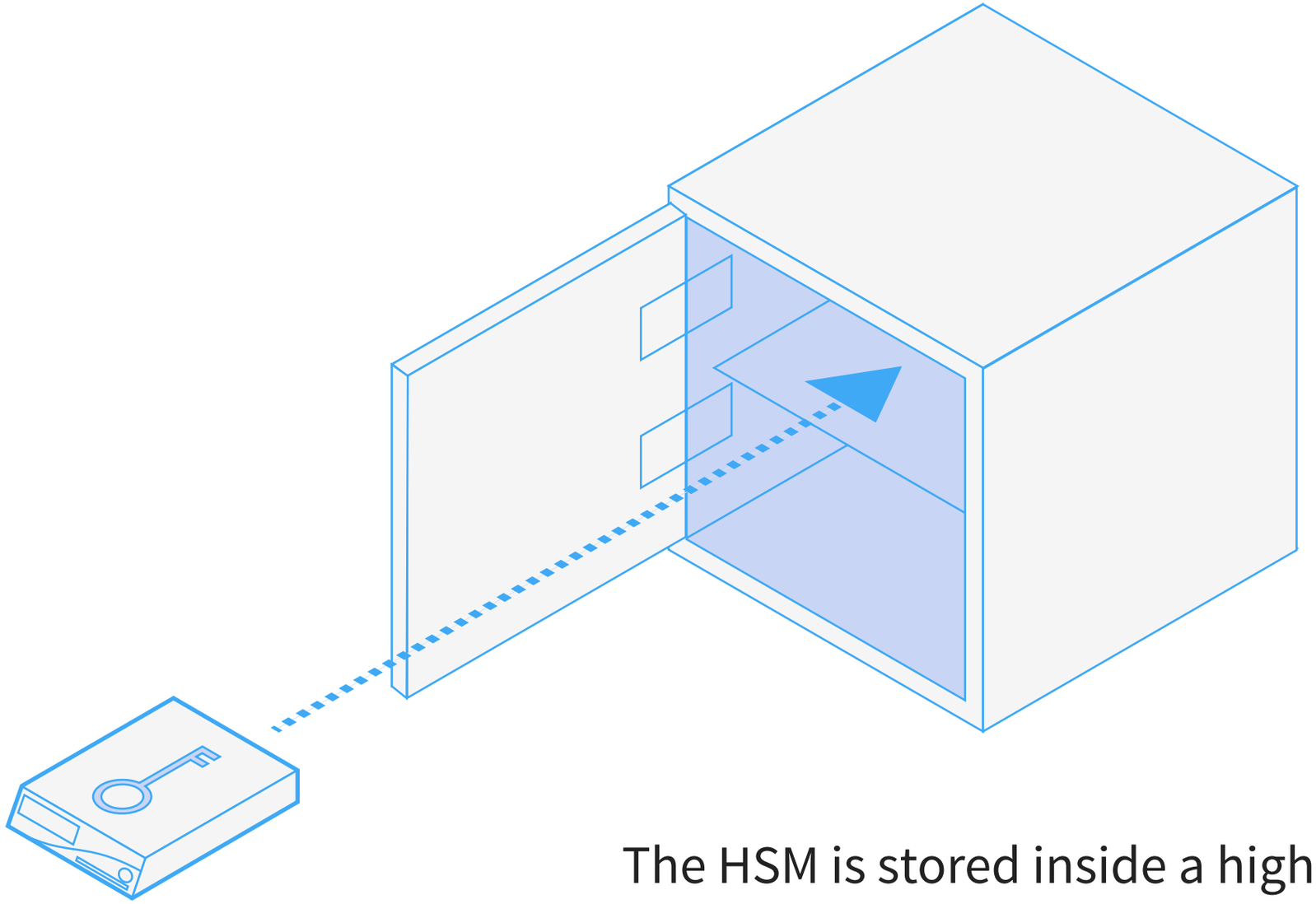
The DNSSEC root key is stored in a device known as a **hardware security module** (HSM) whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper proof. If there is an attempt to open it, the contents will self-destruct.



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.

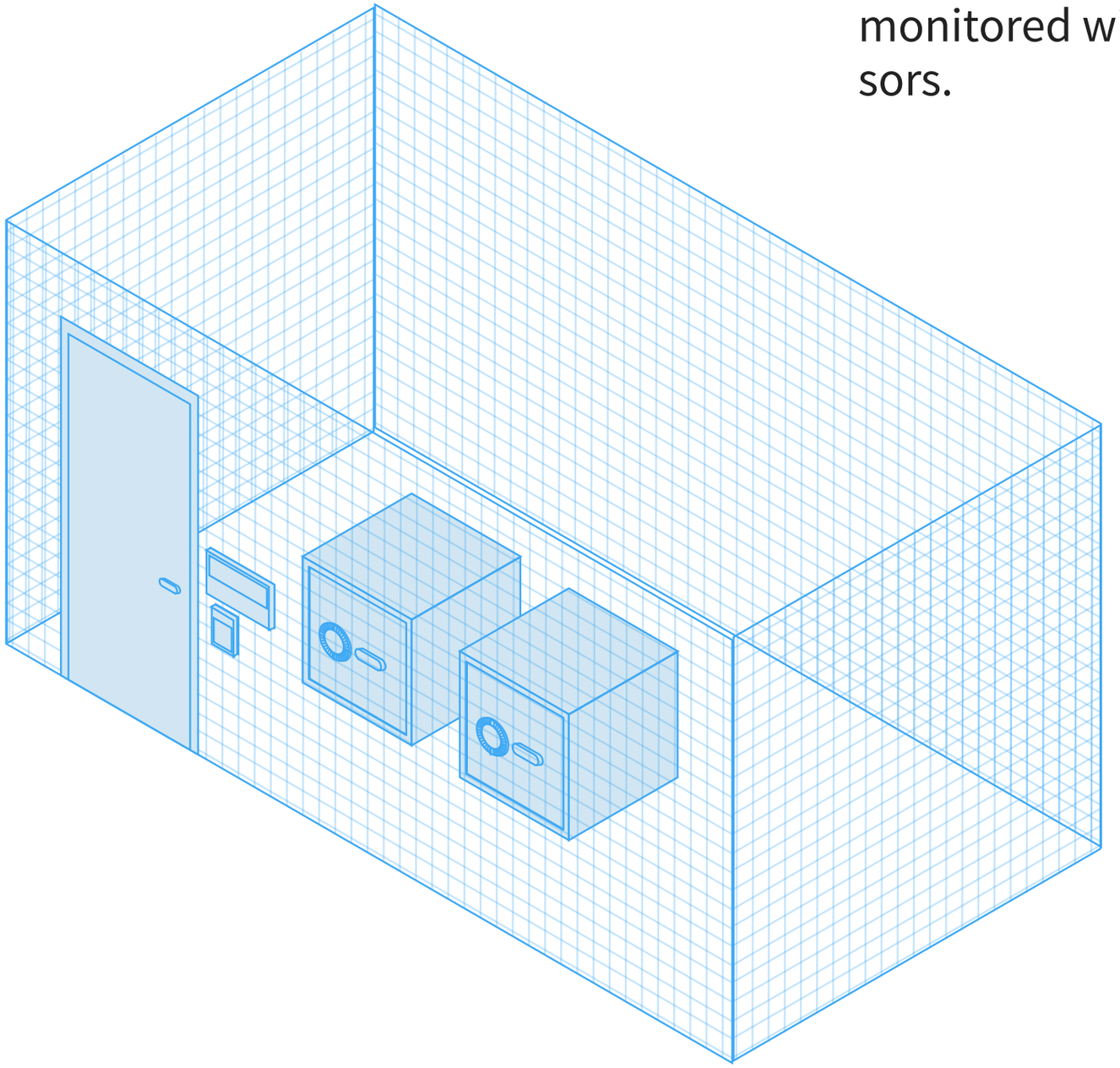


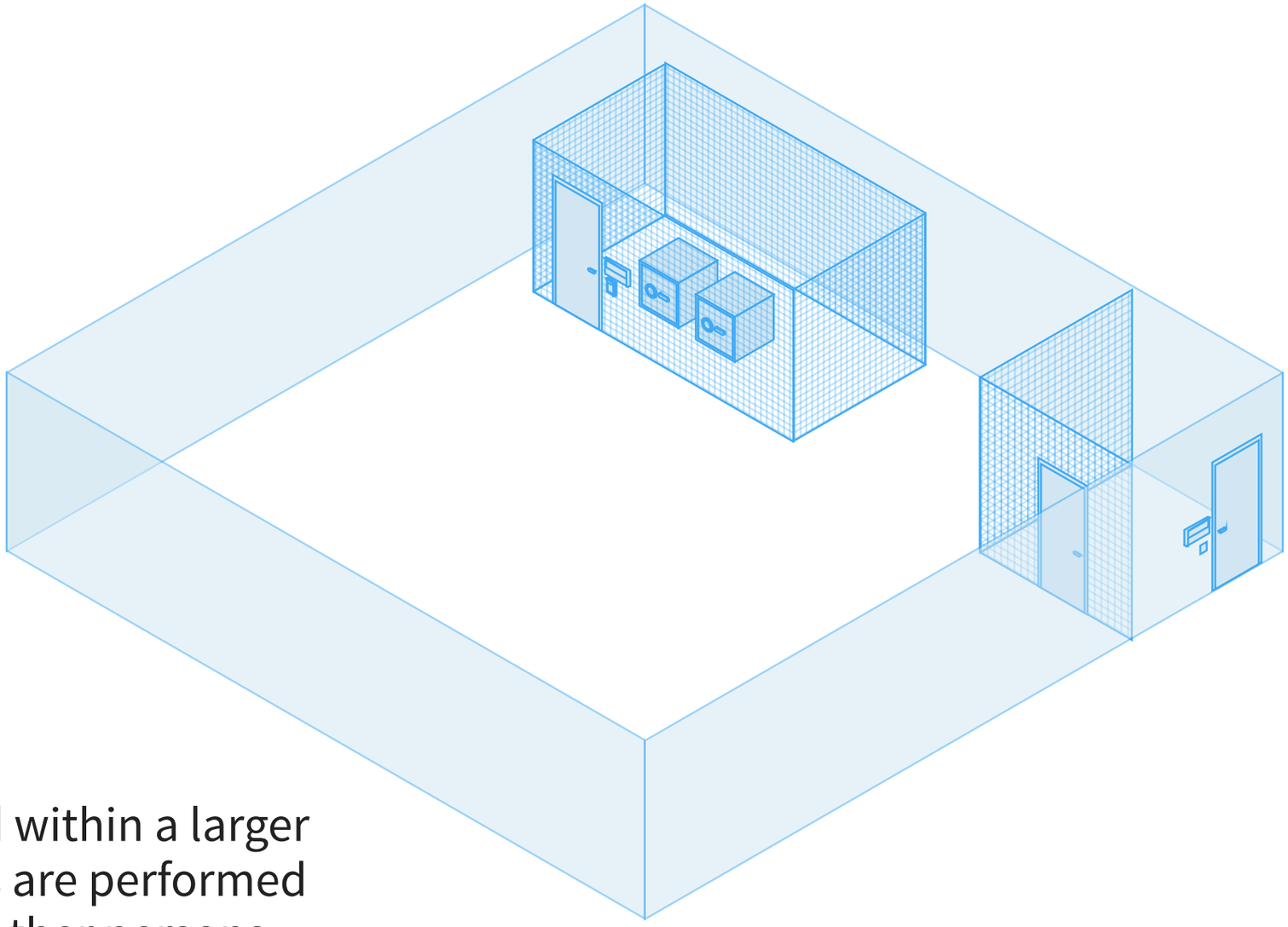
Each smart card is given to a different ICANN community member, known as a **trusted community representative**. To access the key signing key, therefore, at least three of these TCRs need to be present.



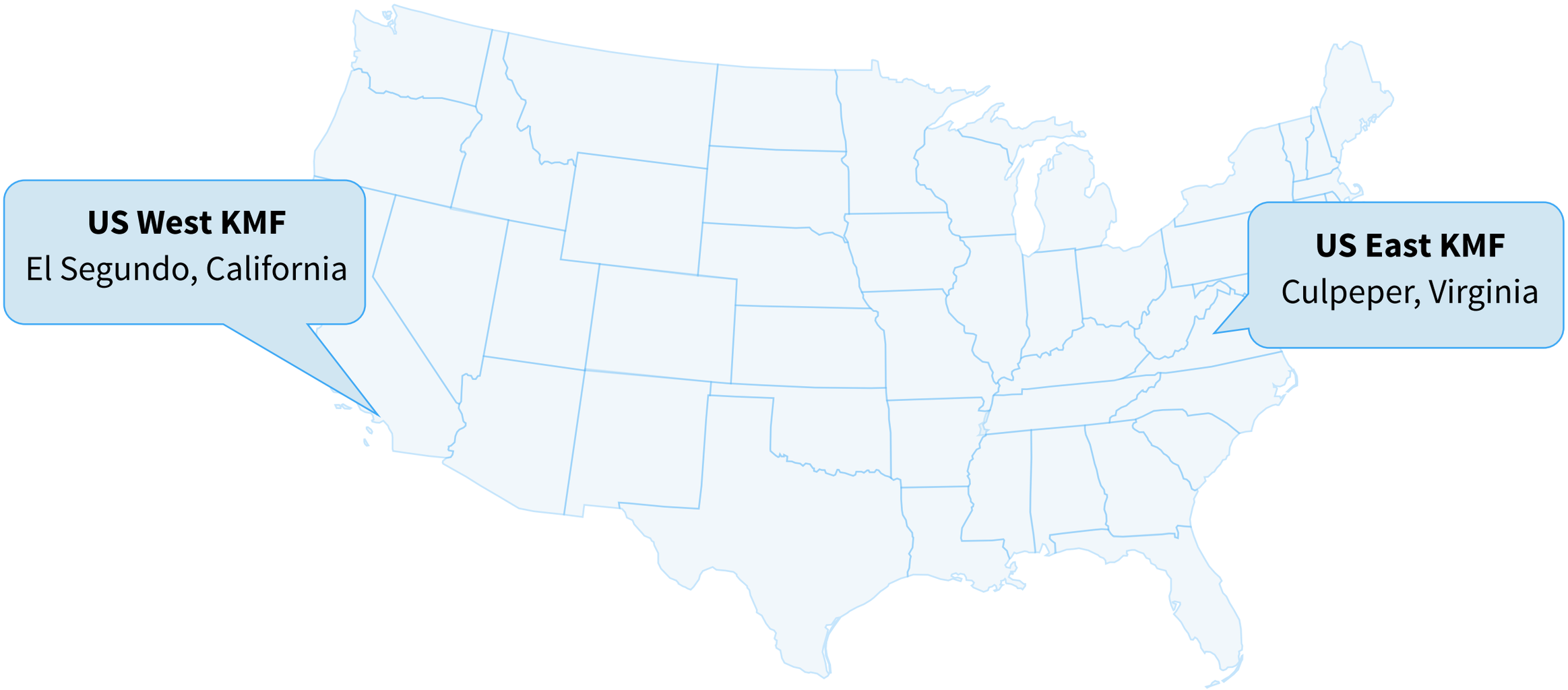
The HSM is stored inside a high-security safe, which can only be opened by a designated person, the **safe security controller**. The safe is monitored with seismic and other sensors.

The safes are stored in a secure room which can only 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**
- The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the HSMs have not been compromised.

Watch short documentaries:

The Guardian
http://goo.gl/JvPu62

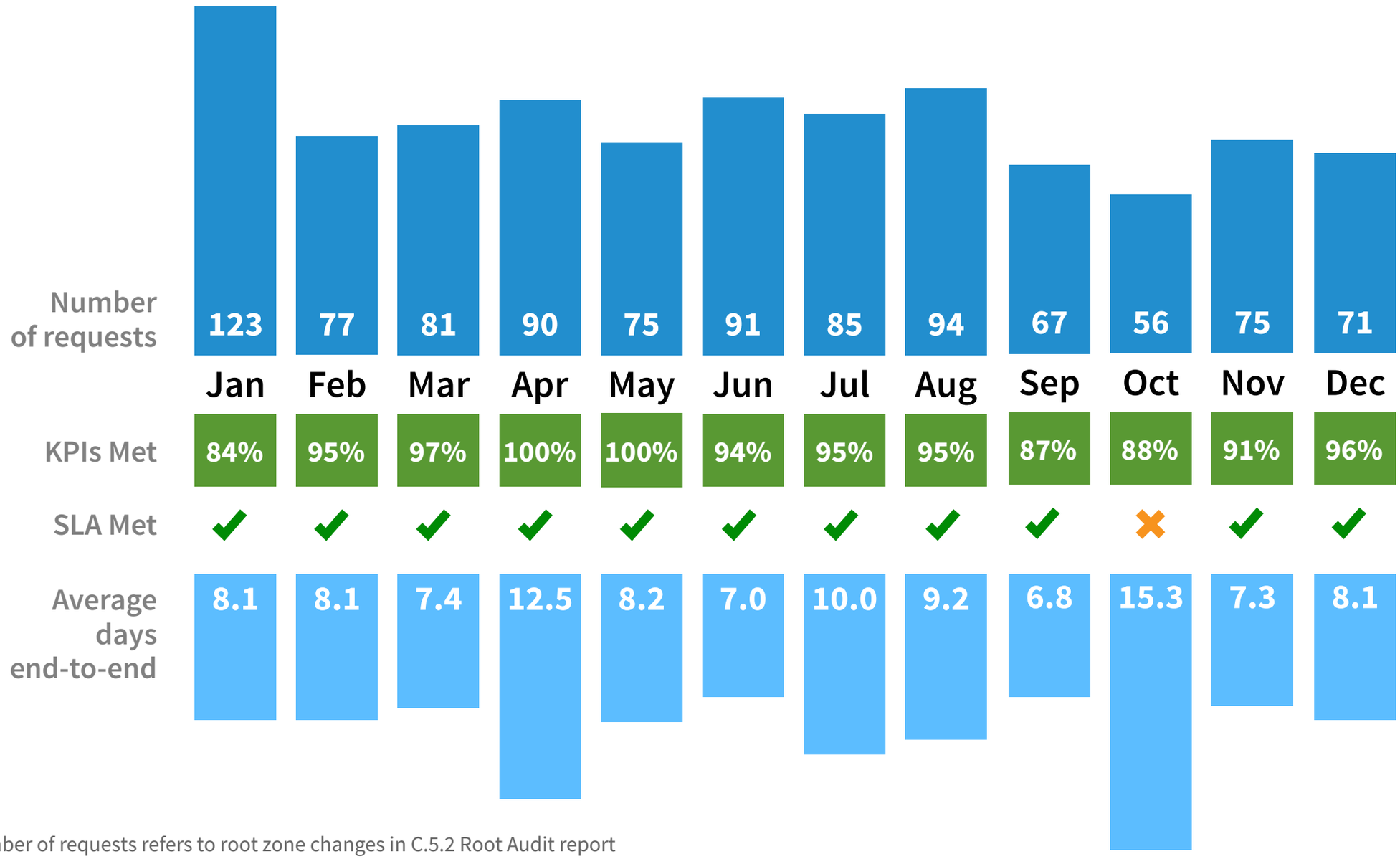
BBC *Horizon*
http://goo.gl/WAz1iV

ICANN

Security at IANA

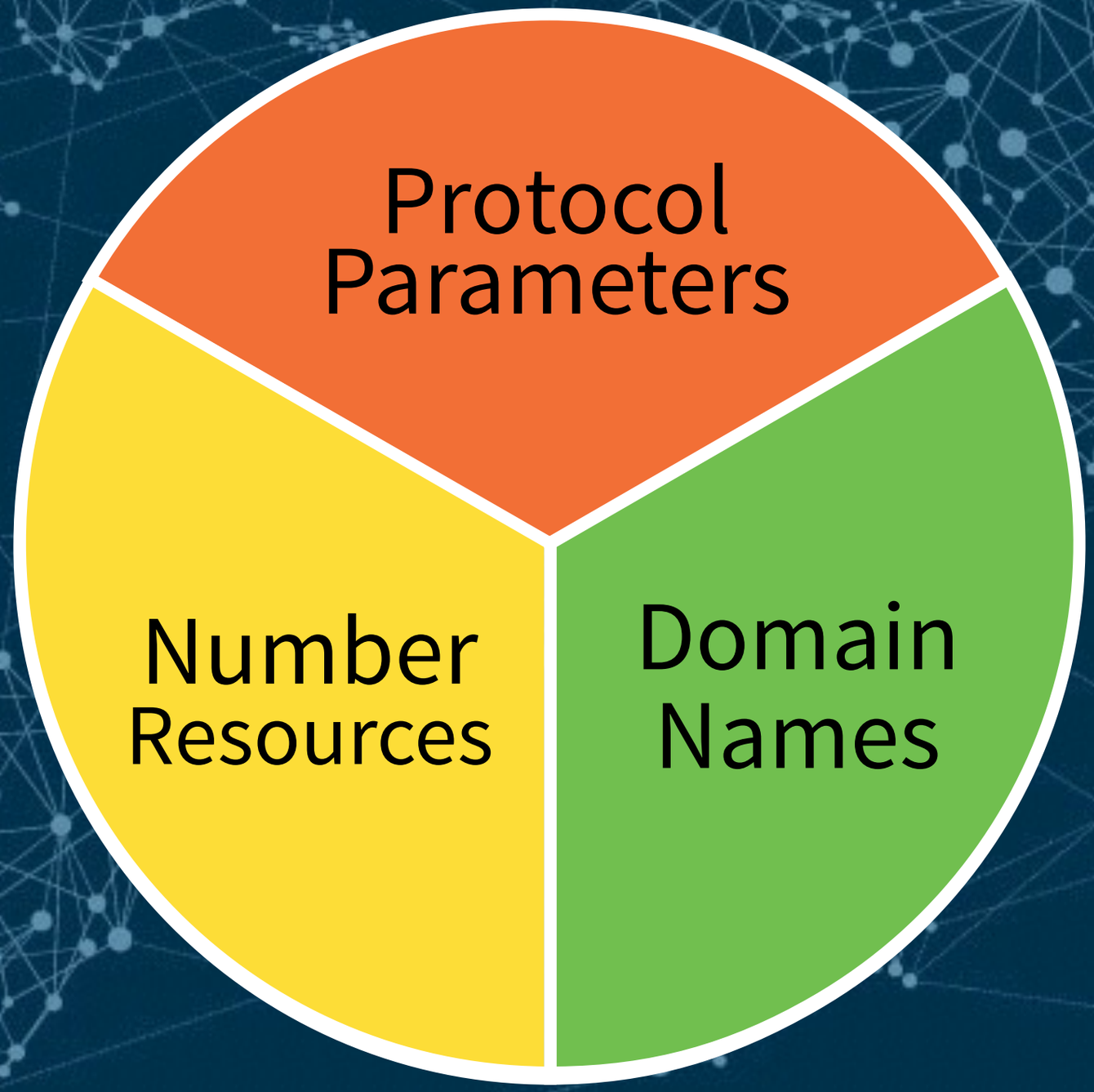
- Security at IANA is not just DNSSEC
- Dedicated workflow systems for IANA functions, independent of broader ICANN systems
- Access limited to IANA roles
- Separation of user-facing and staff-facing systems
- Regular third-party audits, including SOC2 audit by PwC of key IANA systems

Performance



Number of requests refers to root zone changes in C.5.2 Root Audit report
KPI refers to Timeliness metric for Root Zone File and WHOIS Database Change Requests
SLA refers to all targets for all domain-related metrics in the C.4.4 standards report

Comprehensive service level performance reporting at
iana.org/performance


Protocol Parameters
Number Resources
Domain Names

How big is the job?

4
Key signing ceremonies

810
Top Level Domain Delegations

2,800+
Protocol Parameter Registries

1,183
Domain-related requests

5
Number-related requests

4,065
Protocol-related requests

1,120
General enquiries

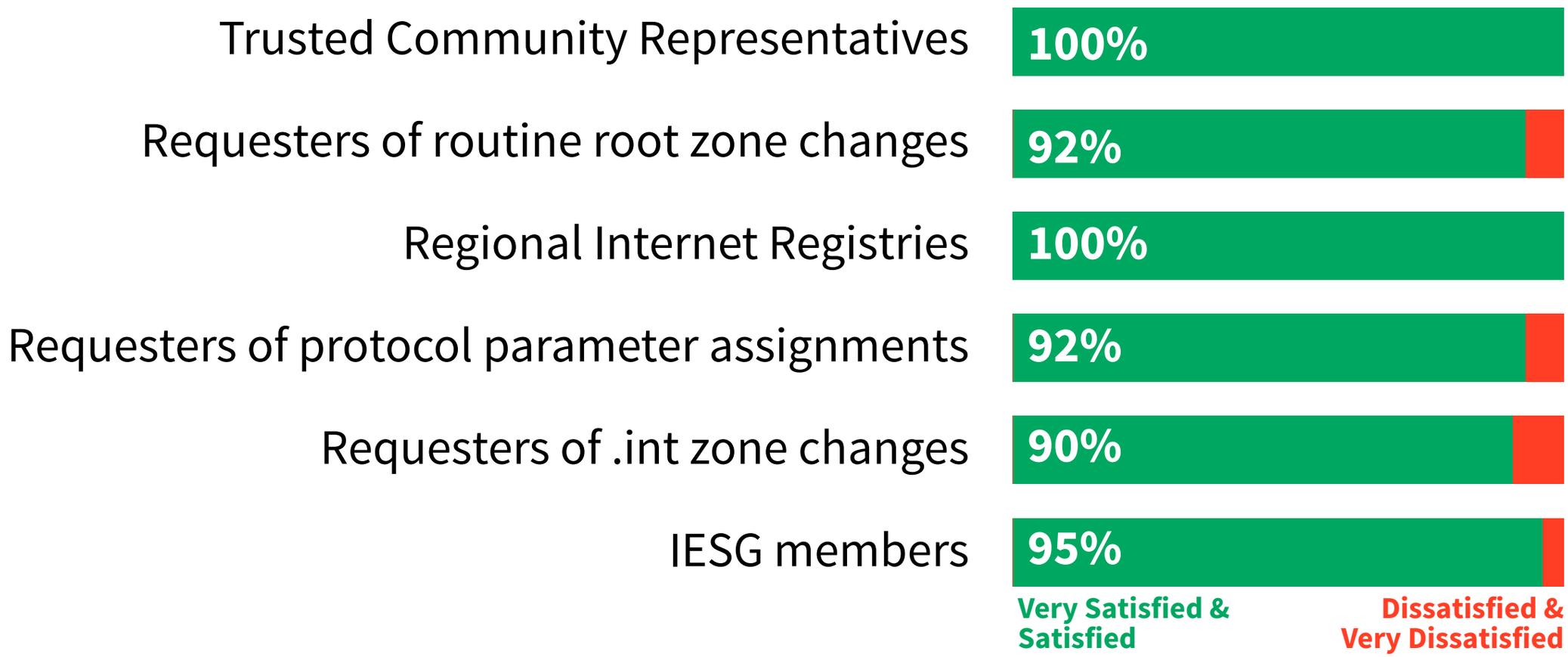
13
Number Resource Registries

2
Third party audits

Request count: 1 January 2014 — 31 December 2014
TLD count: As at 1 February 2015
Domain related requests include processing .int, .arpa and other non-root related requests

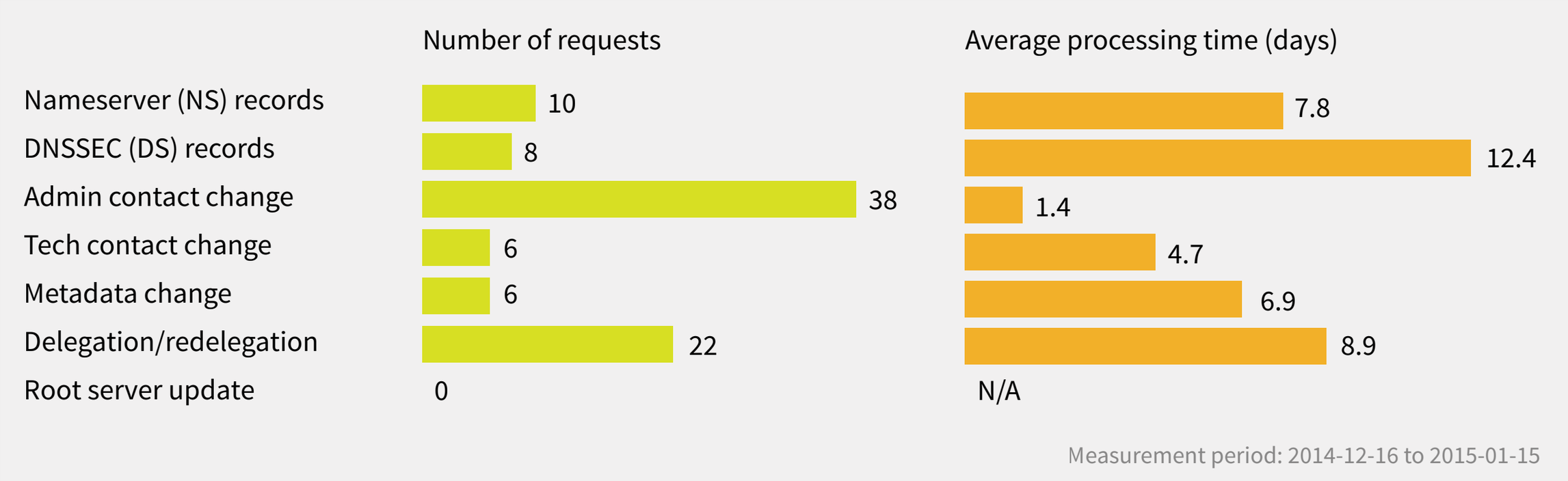
ICANN

Satisfaction by customer group



IANA Functions Customer Survey 2014
http://www.iana.org/reports/2014/customer-survey-20141217.pdf

Root Processing Times



IANA Monthly Root Dashboard — January 2015
http://www.iana.org/performance/root-processing-times

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

Summary

- IANA Department maintains the registries of unique numbering systems that keep the Internet interoperating.
- Most IANA registries are straightforward, and are not generally known to the end-user.
- High profile, hierarchically-delegated registries are used for the Domain Name System and Number Resources. IANA Dept. maintains the global “root” for these.

Thank you!

Website	**iana.org**
Service level reporting	**iana.org/performance**
Functional areas	**iana.org/protocols** **iana.org/numbers** **iana.org/domains**
More background	**iana.org/about**

ICANN