The Root Zone

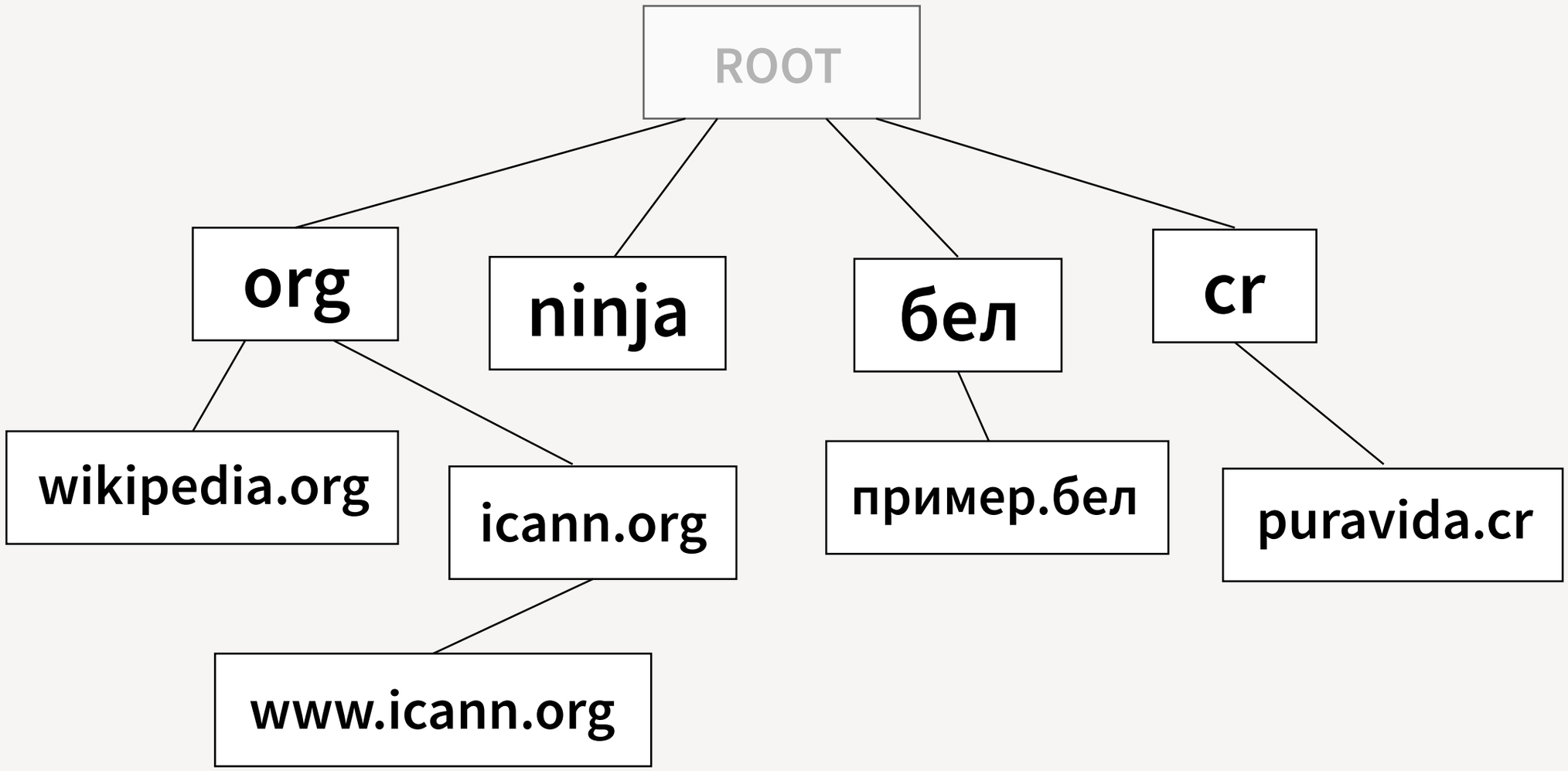
Kim Davies

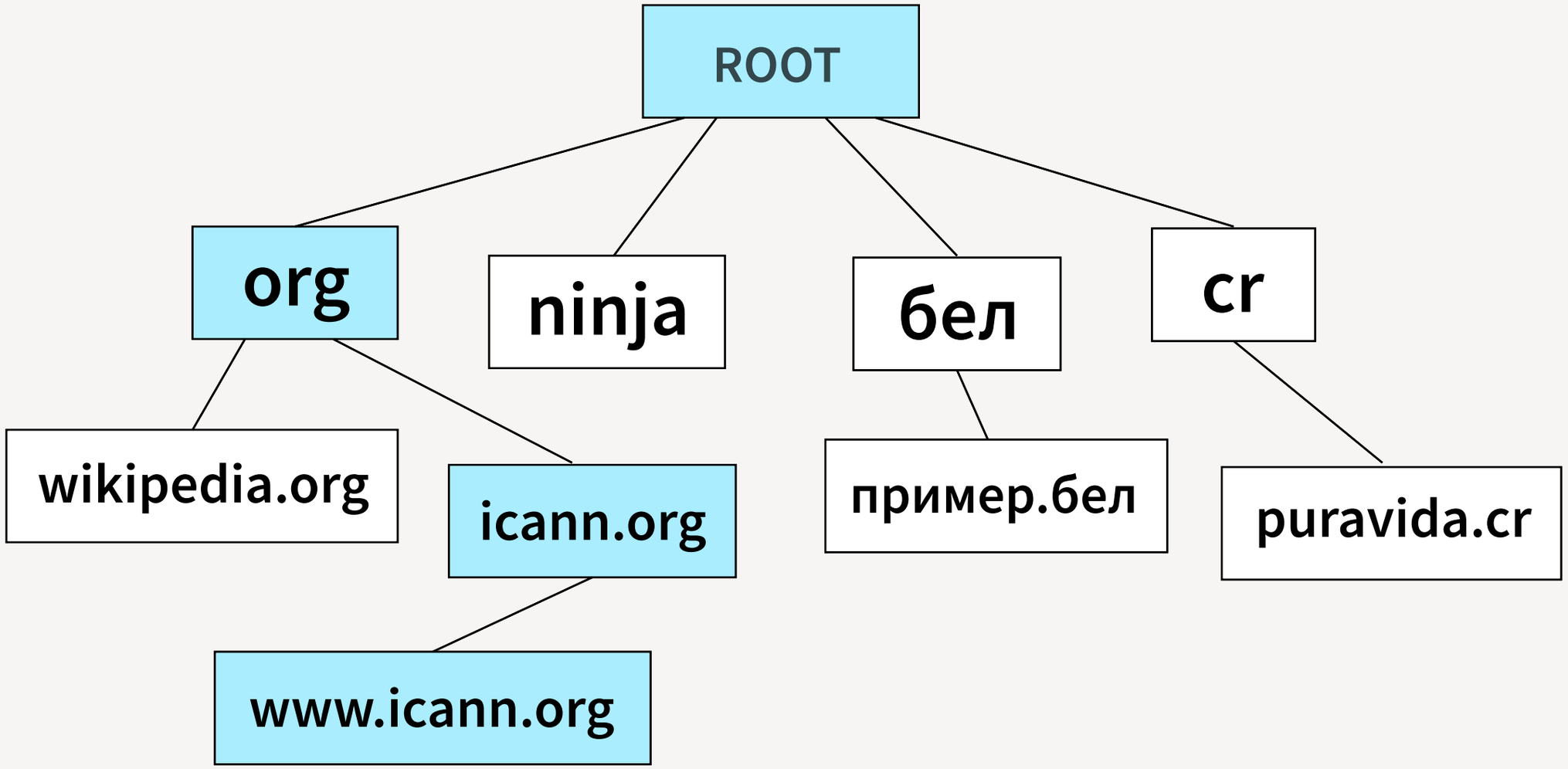
April 2021

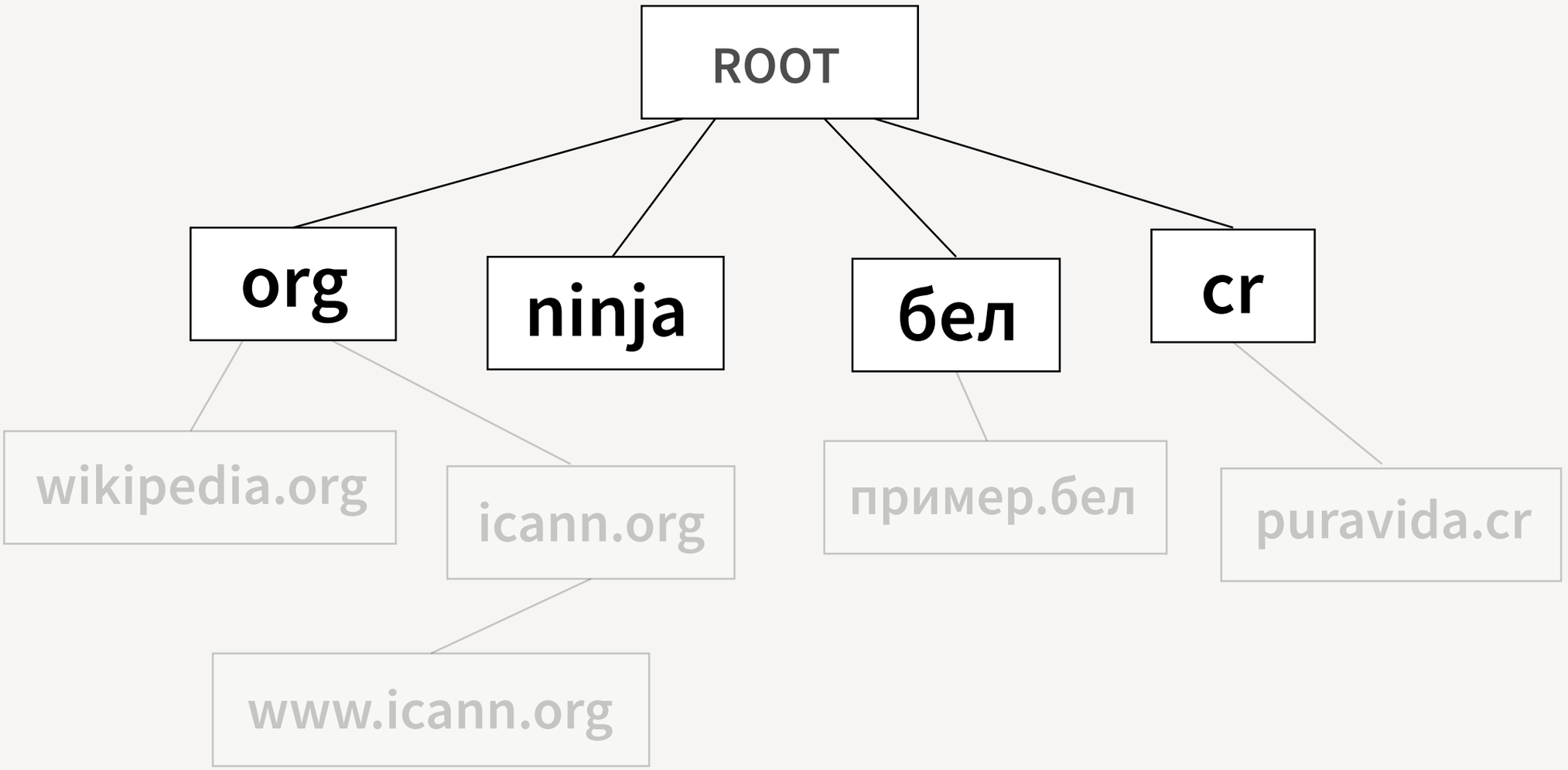
PTI|An ICANN Affiliate

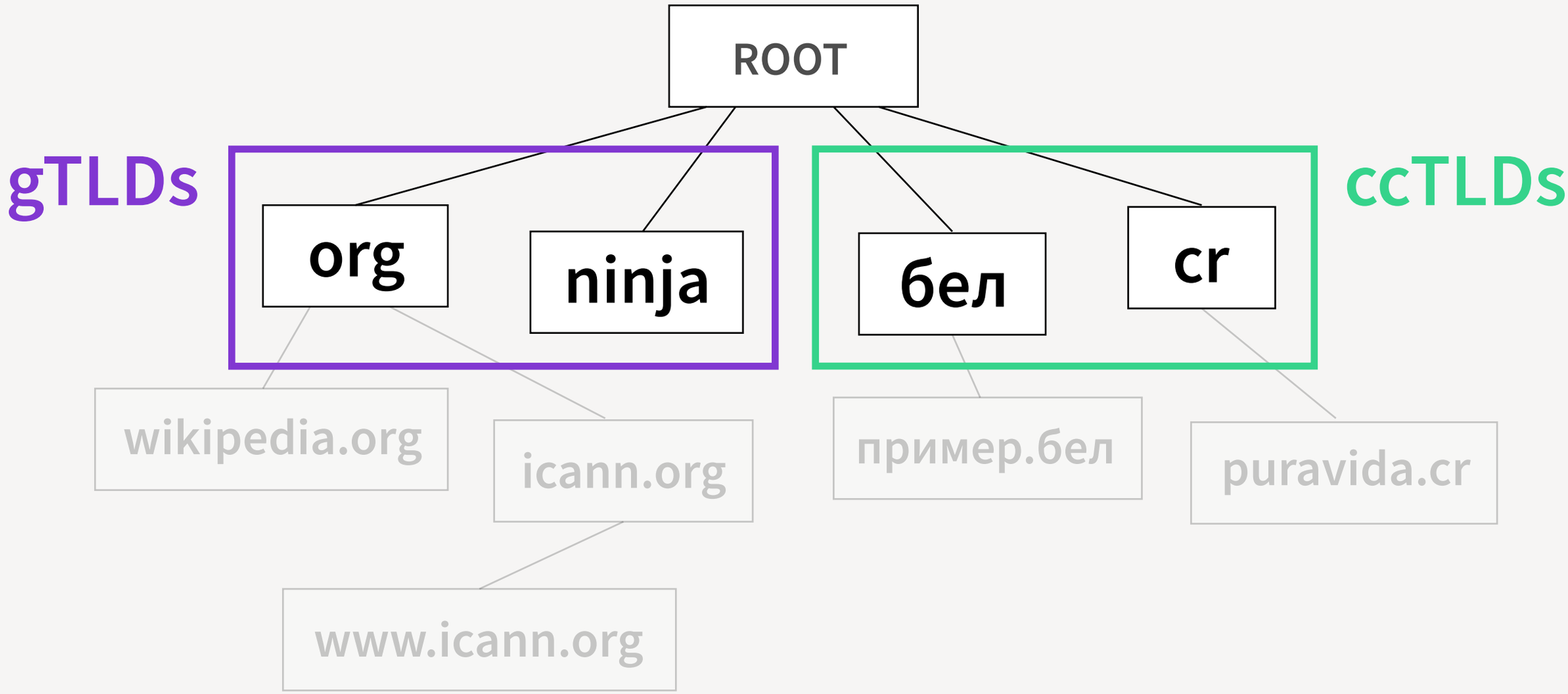
The Root Zone

- Upper-most level of hierarchy in the Domain Name System
- Authoritative record of what is and is not a top-level domain
- Logical starting point for name resolution


ROOT
org
ninja
бел
cr
wikipedia.org
icann.org
пример.бел
puravida.cr
www.icann.org

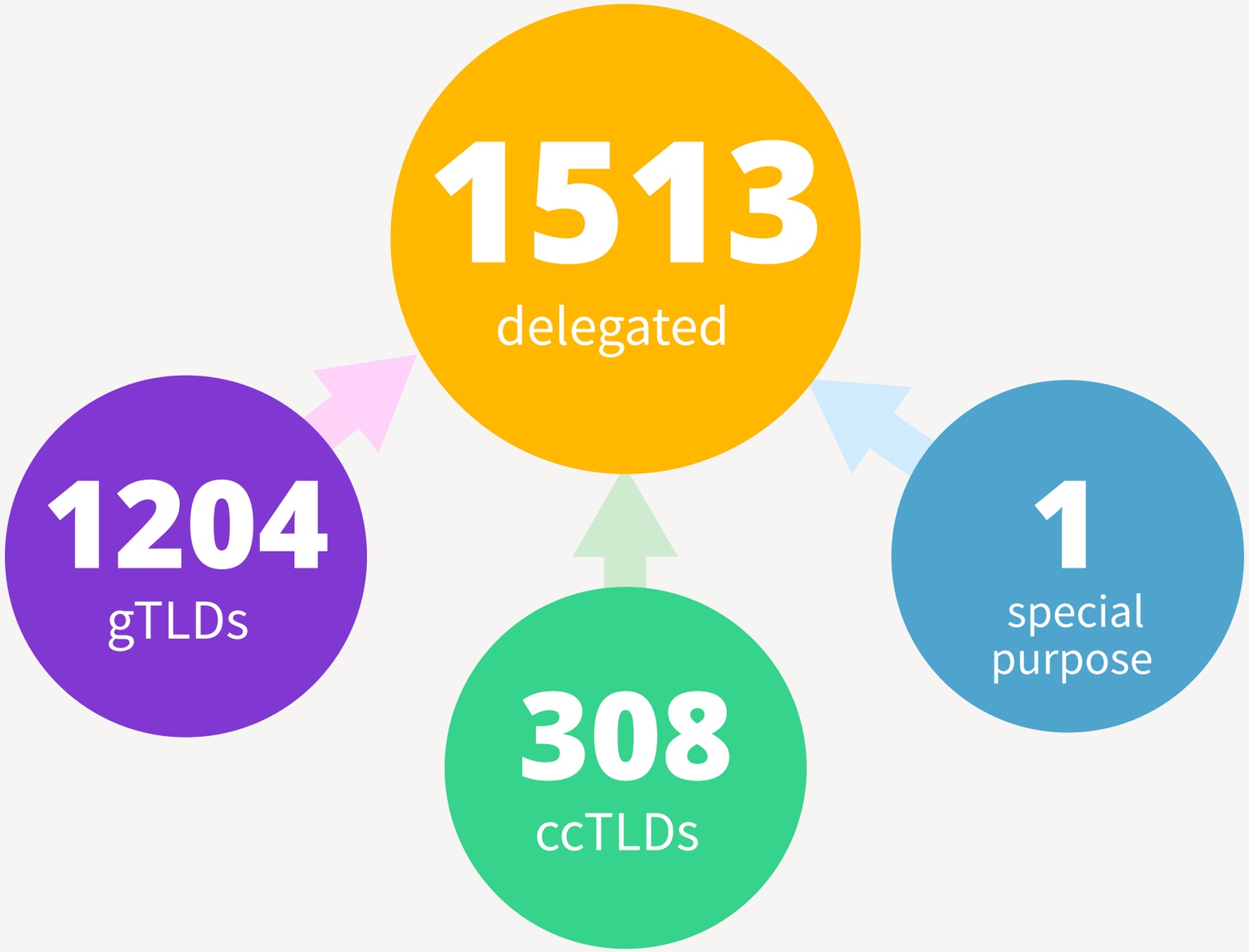

ROOT
org
ninja
бел
cr
wikipedia.org
icann.org
пример.бел
puravida.cr
www.icann.org


ROOT
org
ninja
бел
cr
wikipedia.org
icann.org
пример.бел
puravida.cr
www.icann.org



- Global scope
- ICANN policies

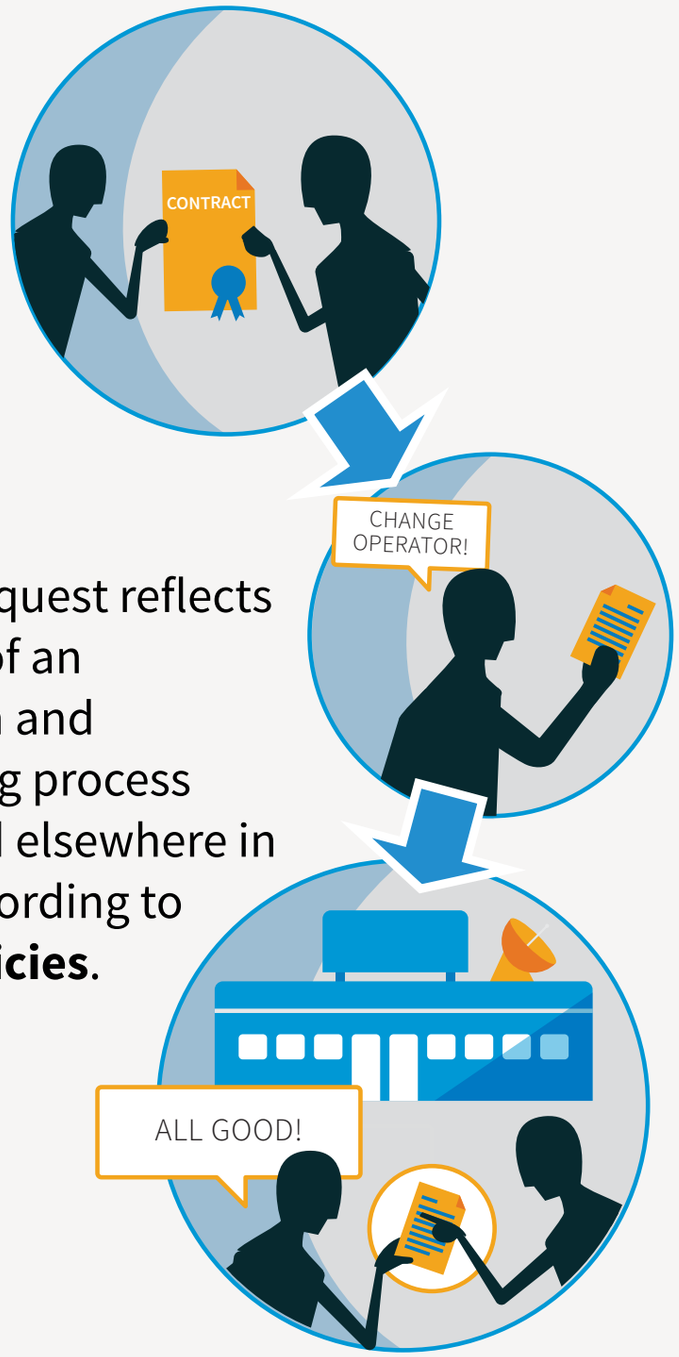
- Country scope
- Local policies


1513
delegated
1204
gTLDs
308
ccTLDs
1
special
purpose

Root Zone Management Tasks

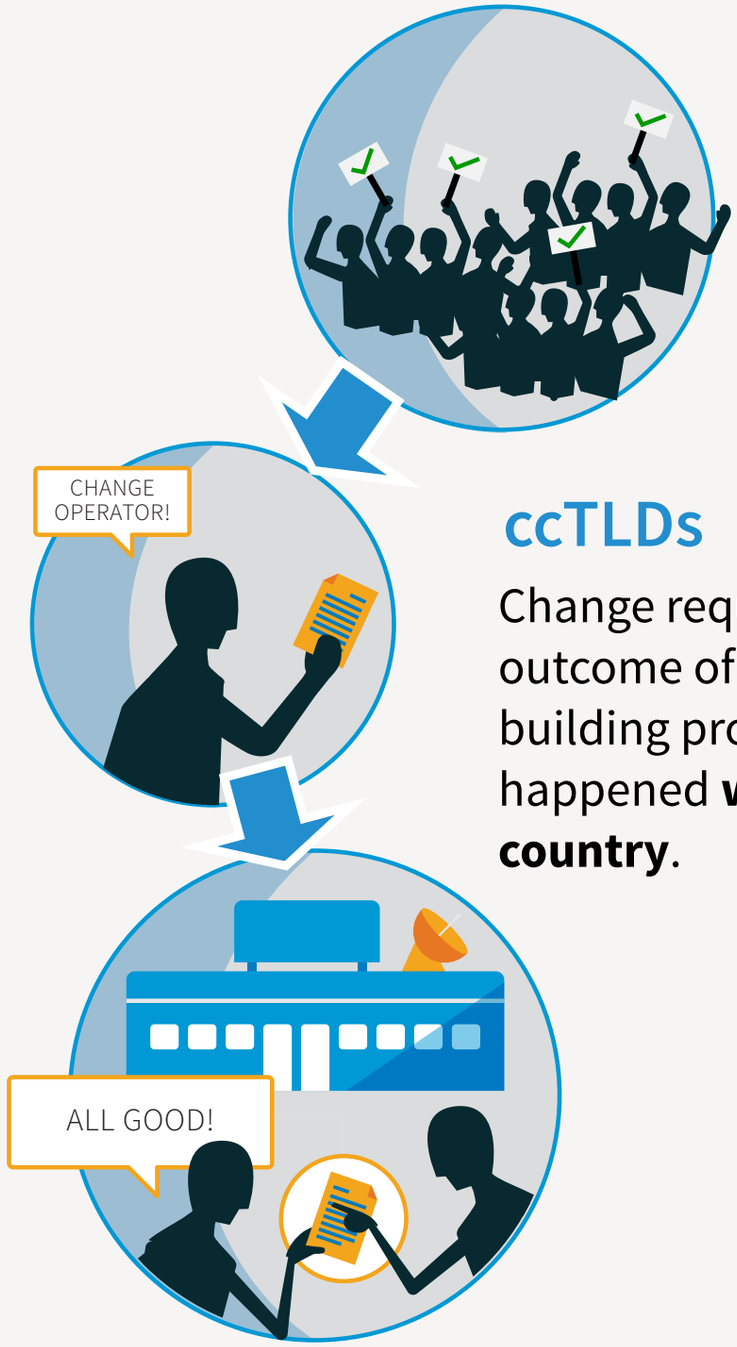
- Maintain the attributes of the root zone
  - Store and disseminate the content
  - Process change requests to the content
- Manage interactions with customers (the TLD managers)
- Work with partners to get content published and used
- Review requests against policies
- Check for consent to changes
- Ensure technical operative
- Additional checks for change-of-control

Changes of control



gTLDs

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



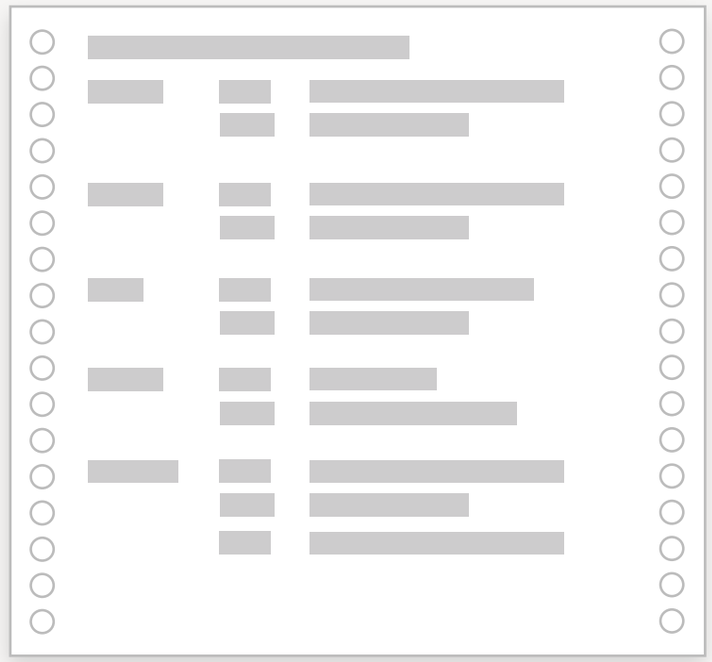
ccTLDs

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

Root Zone Database

- Which TLDs exists
- Who manages them
- The points-of-contact
- Technical delegation data
- Social metadata

Root Zone File



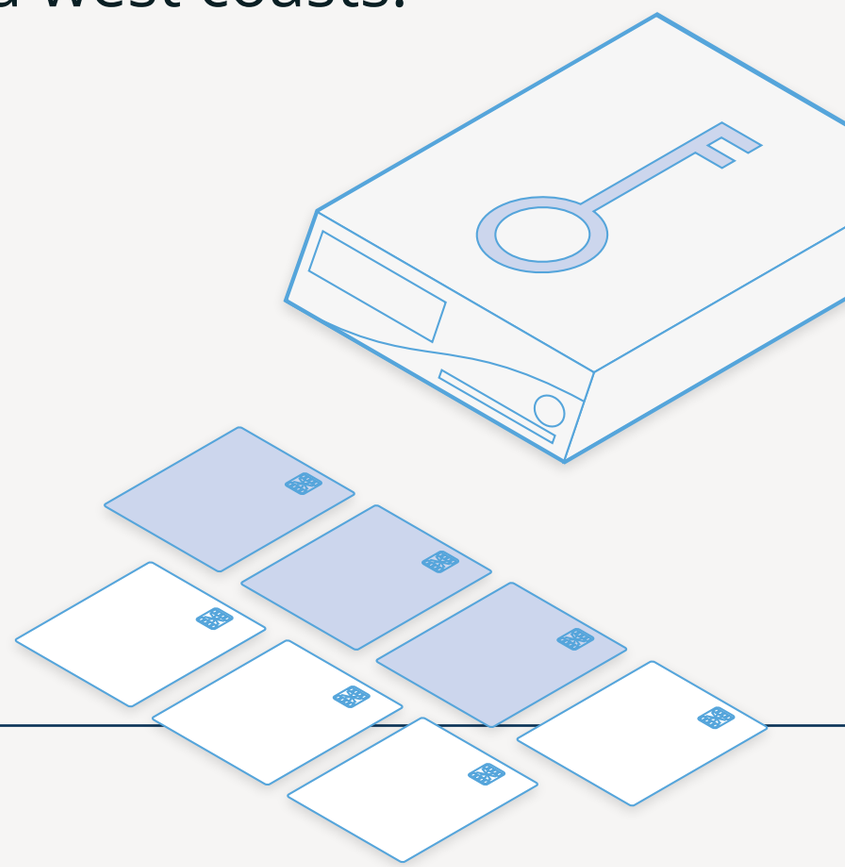
- Technical delegation data
- Technical metadata

Ensuring Root Zone File integrity

- DNSSEC adds cryptographic signatures to the zone file contents
- Allows DNSSEC-enabled software to verify the content is authentic from its original publisher
- The key that is used as the origin of this validation, is the root zone **key signing key (KSK)**

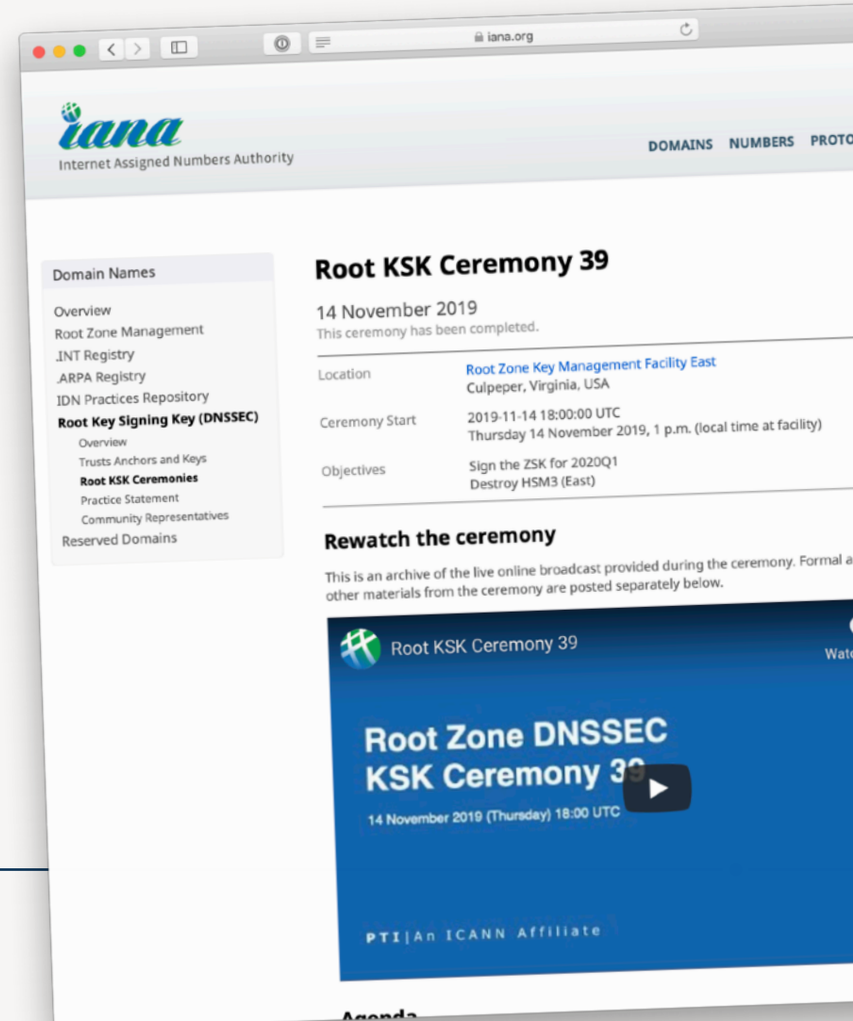
Managing the KSK

- Key is stored in specialized equipment called hardware security modules
- To use these devices, 3 of 7 trusted community representatives are present, along with other personnel in essential roles.
- The modules are stored in secure facilities with multiple levels of protection including safes, cages, and varying entry requirements.
- Stored in two independent facilities on US east and west coasts.



How do we use the KSK?

- KSK at rest is kept secure through:
  - Overlapping layers of security
  - Protecting the chain of custody
  - Minimizing collusion risk
  - Redundancy to ensure successful operation
  - Guarding against surreptitious entry
  - Open design
- Authorized use of the KSK is managed through planned events known as **key signing ceremonies**
- Ceremonies convene a quorum of participants needed to activate the KSK in its secure enclosure, with sufficient controls to satisfy observers it is being used in a legitimate way and there is no risk of inadvertent use.

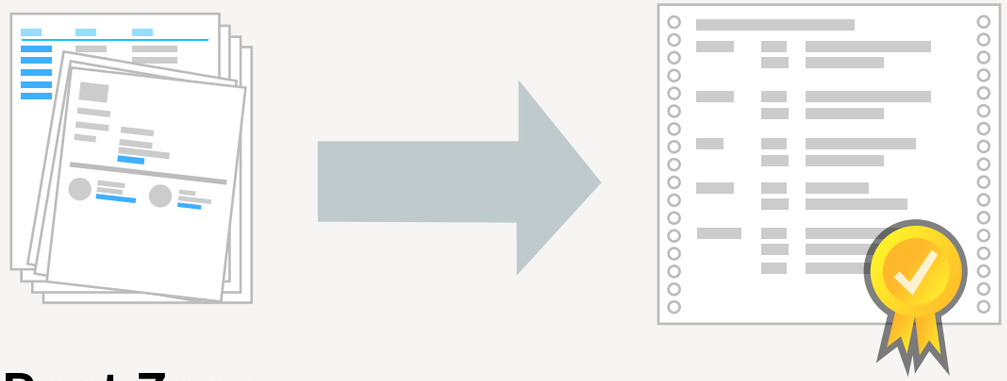


Key ceremonies

- 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 ceremony is conducted in a highly transparent manner, with the opportunity for interjection if anyone is concerned.
- The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the KSK has not been compromised.

Root Zone Distribution

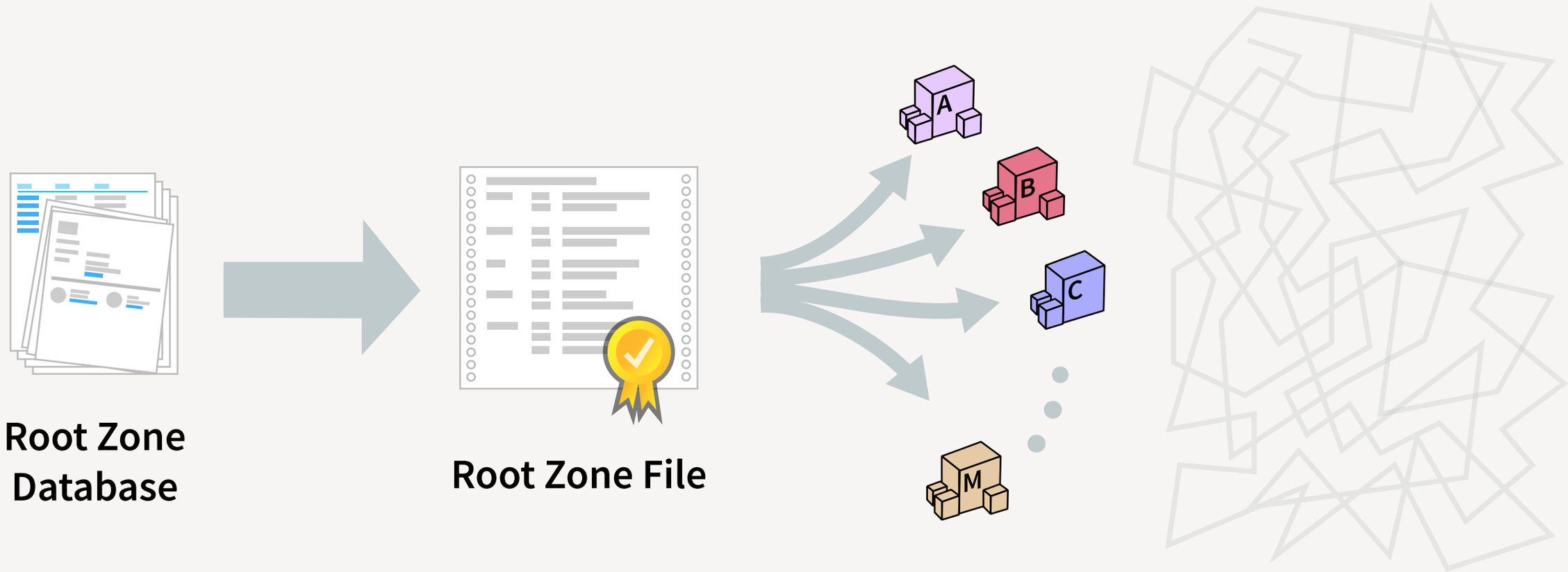
Production



Root Zone Distribution

Production

Distribution



Root Zone Database

Root Zone File

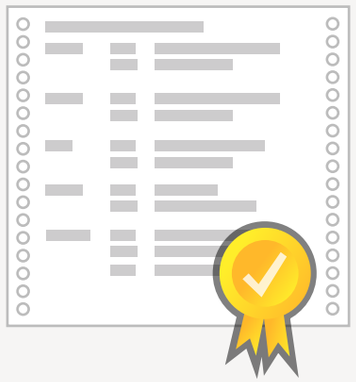
Root Servers

Root Zone Distribution

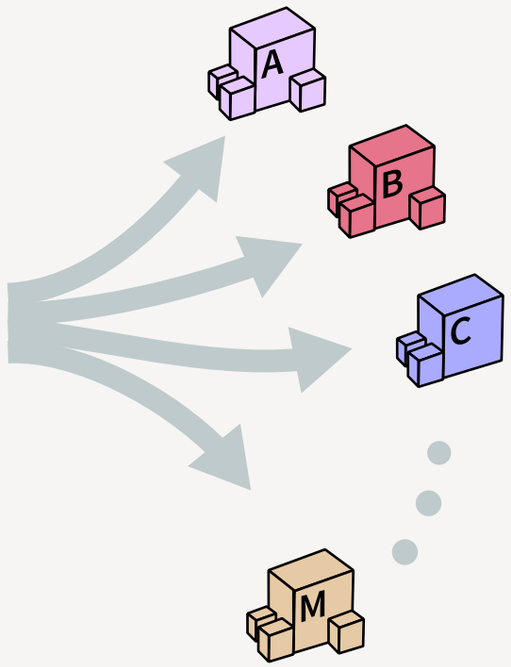
Production

Distribution

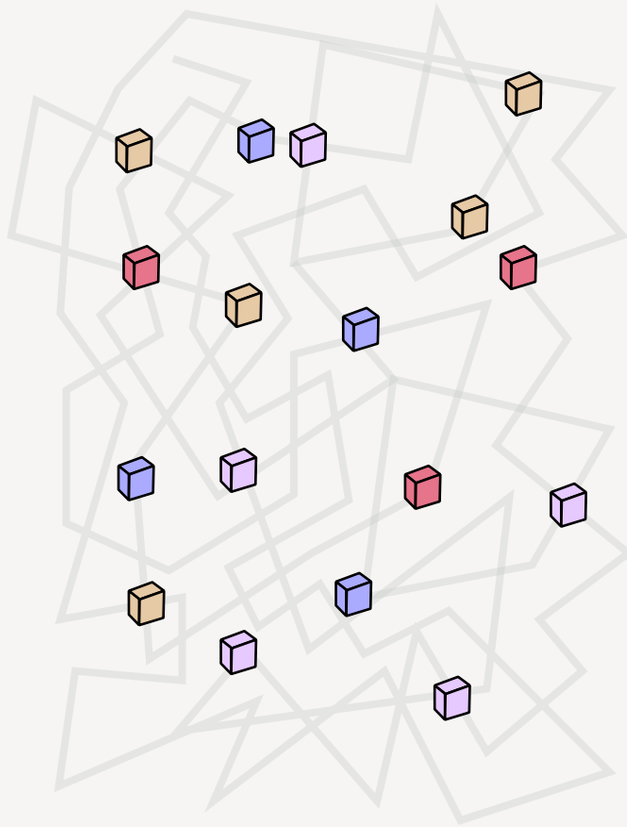
Root Zone Database



Root Zone File



Root Servers

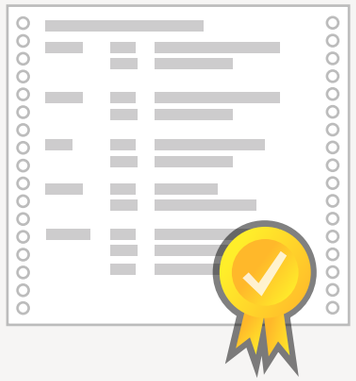


Root Zone Distribution

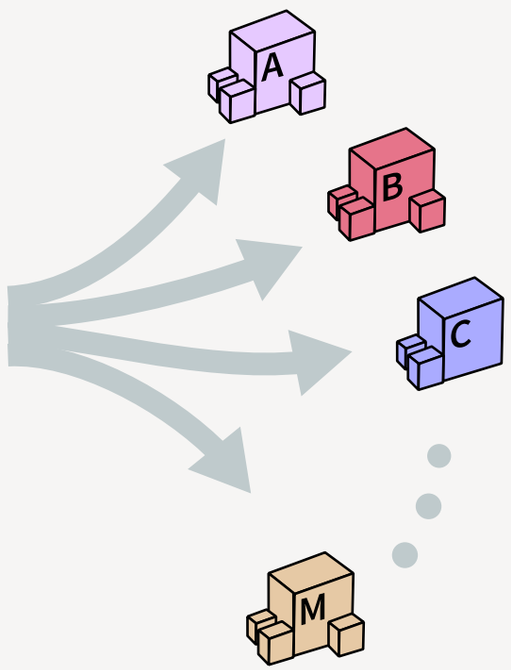
Production

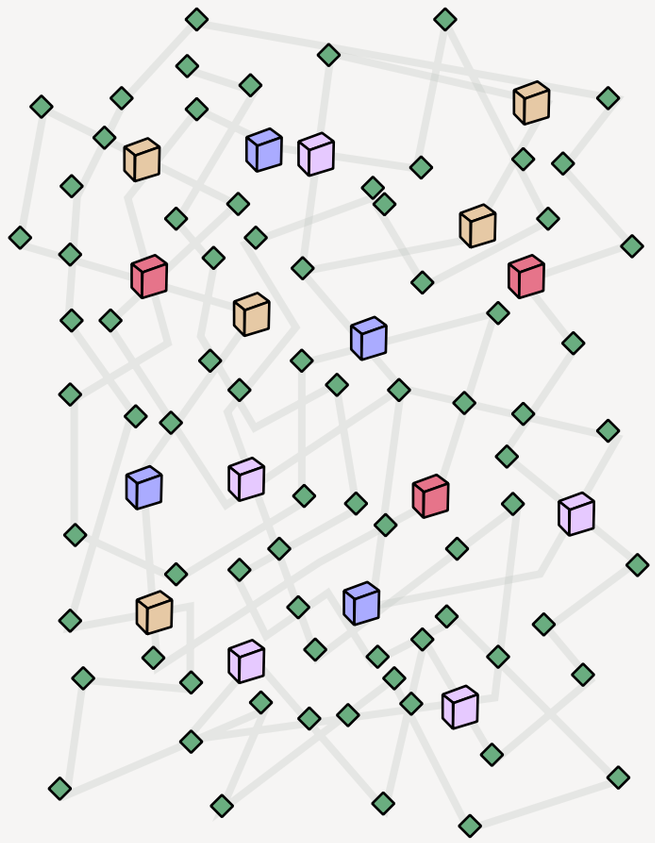
Distribution

Root Zone Database



Root Zone File





Root Servers

Thank you!

kim.davies@iana.org