Distributed Delegated Mappings

draft-watson-dinrg-delmap-01

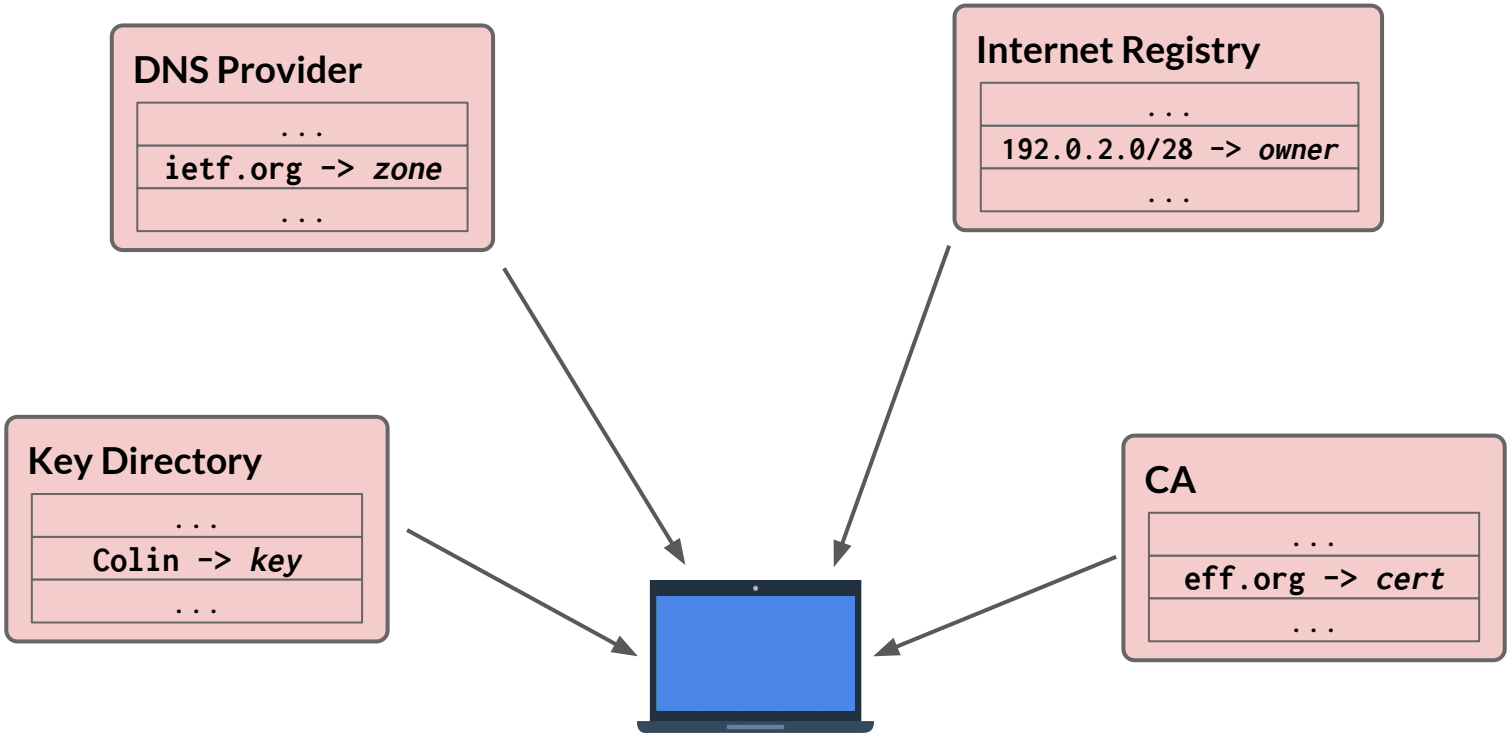
Jean-Luc Watson[1], Sydney Li[2], Colin Man[3]

DINRG - IETF 103

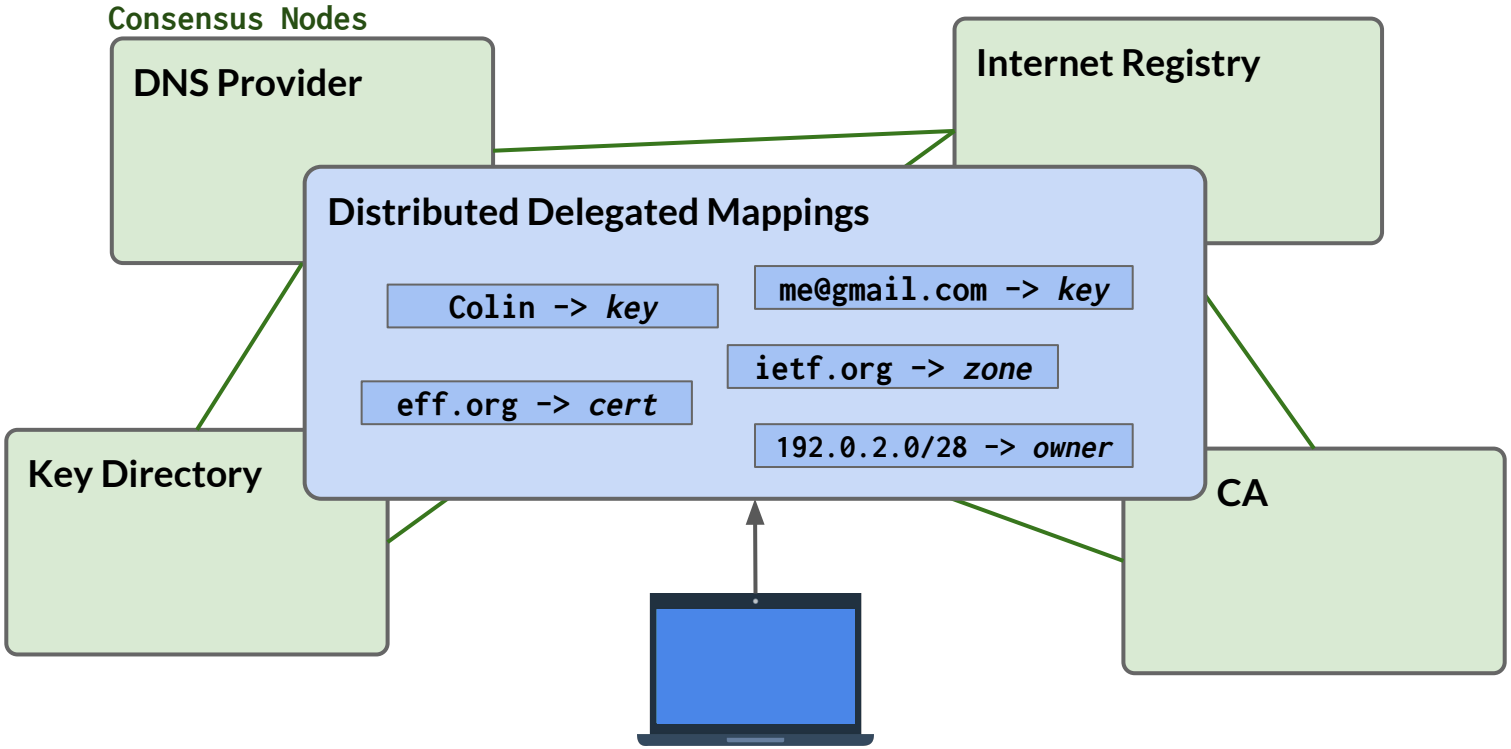
[1]UC Berkeley, [2]Electronic Frontier Foundation, [3]Stanford University

Recap

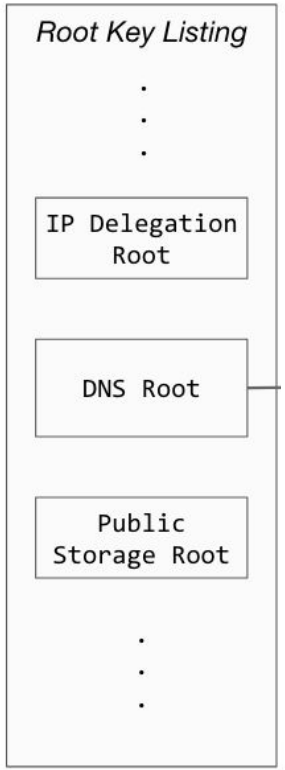
Mappings


DNS Provider
...
ietf.org -> zone
...
Internet Registry
...
192.0.2.0/28 -> owner
...
Key Directory
...
Colin -> key
...
CA
...
eff.org -> cert
...

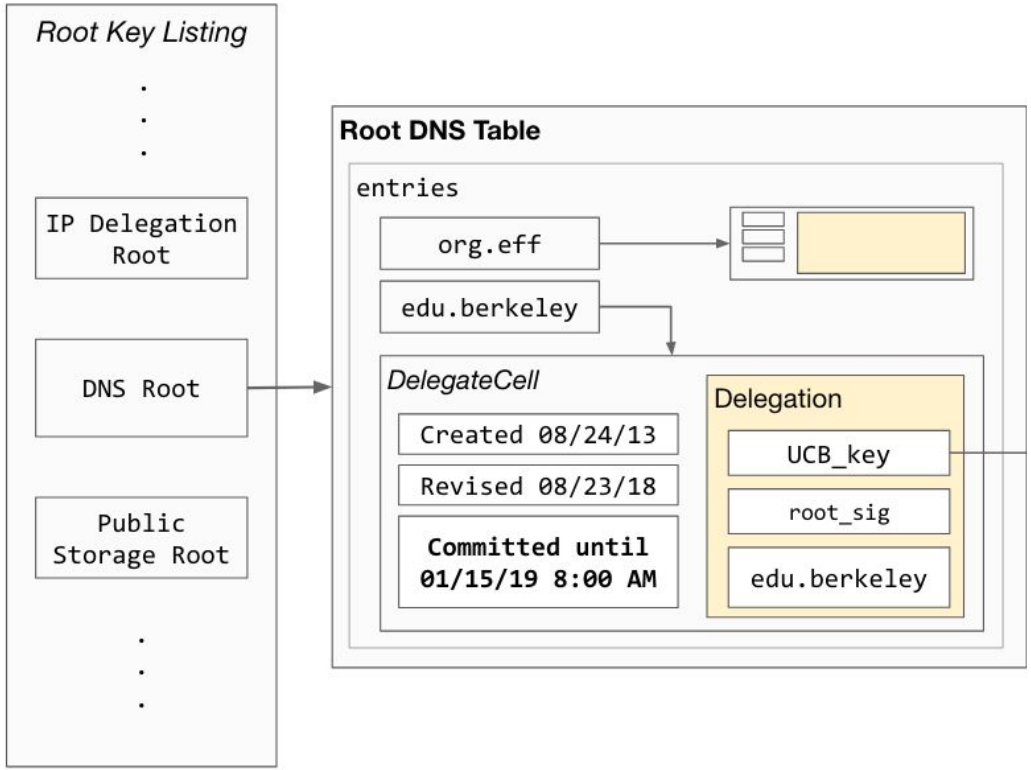
Mappings


Consensus Nodes
DNS Provider
Internet Registry
Distributed Delegated Mappings
Colin -> key
me@gmail.com -> key
ietf.org -> zone
eff.org -> cert
192.0.2.0/28 -> owner
Key Directory
CA

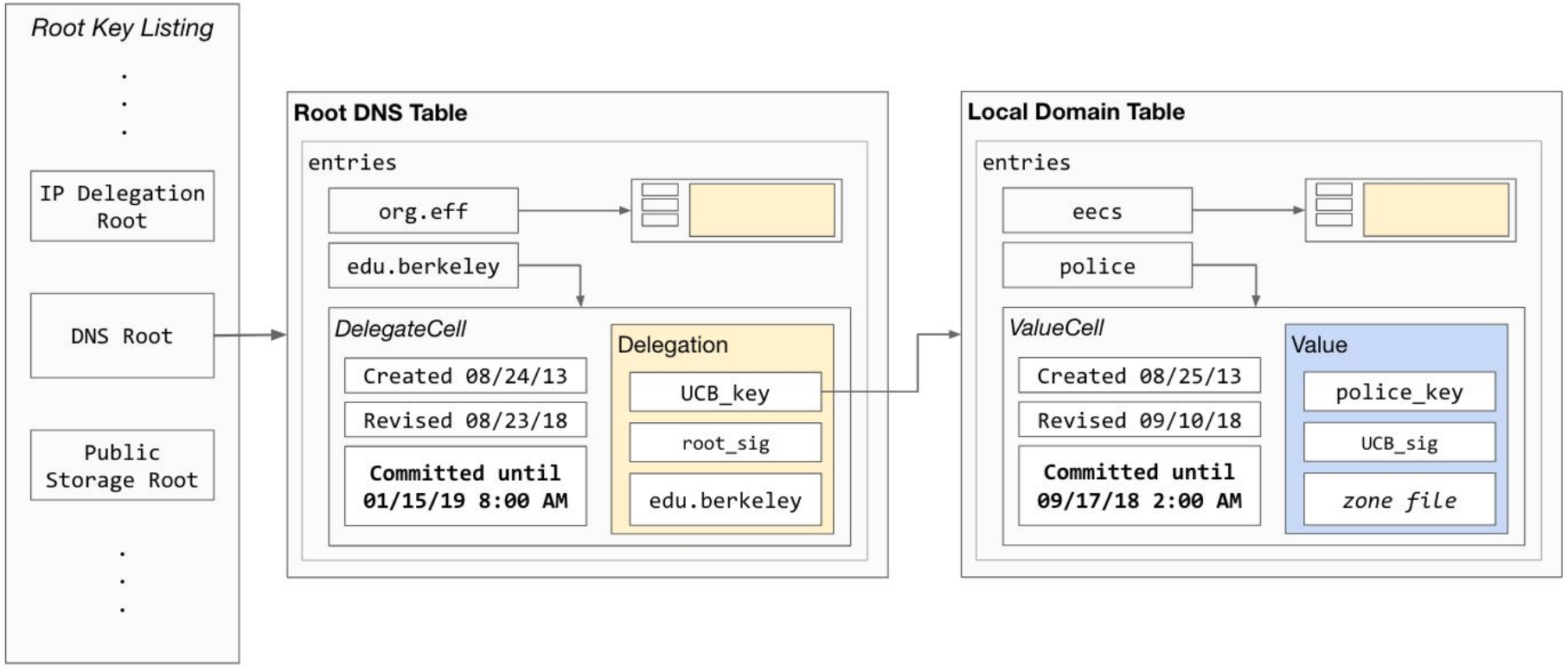
Structure


Root Key Listing
IP Delegation Root
DNS Root
Public Storage Root

Structure

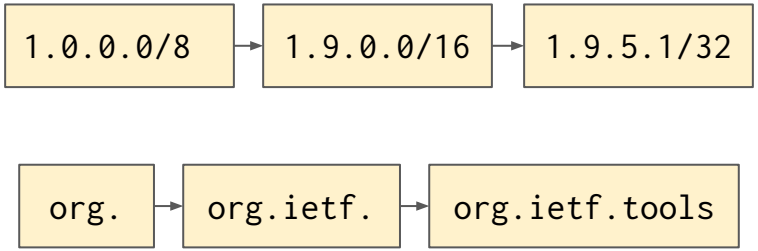

Root Key Listing
IP Delegation Root
DNS Root
Public Storage Root
Root DNS Table
entries
org.eff
edu.berkeley
DelegateCell
Created 08/24/13
Revised 08/23/18
Committed until 01/15/19 8:00 AM
Delegation
UCB_key
root_sig
edu.berkeley

Structure

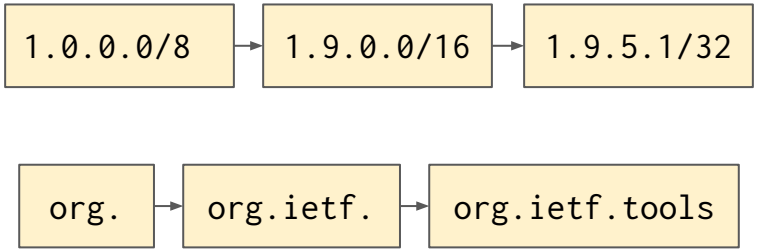

Root Key Listing
IP Delegation Root
DNS Root
Public Storage Root
Root DNS Table
entries
org.eff
edu.berkeley
DelegateCell
Created 08/24/13
Revised 08/23/18
Committed until 01/15/19 8:00 AM
Delegation
UCB_key
root_sig
edu.berkeley
Local Domain Table
entries
eecs
police
ValueCell
Created 08/25/13
Revised 09/10/18
Committed until 09/17/18 2:00 AM
Value
police_key
UCB_sig
zone file

Updates

1. Prefix-only delegation



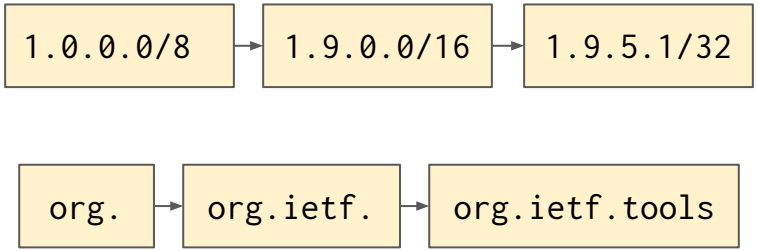
1. Prefix-only delegation



2. Updated verification rules

- Valid (commitment) timestamps
- Signed by party authorized to update specified fields
- Does not violate prefix property
  - No overlapping delegations
  - No duplicate values

1. Prefix-only delegation



2. Updated verification rules

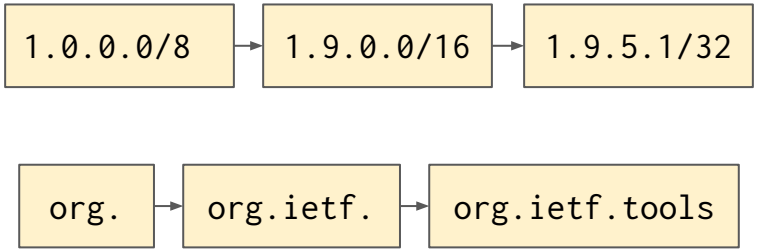
- Valid (commitment) timestamps
- Signed by party authorized to update specified fields
- Does not violate prefix property
  - No overlapping delegations
  - No duplicate values

3. Security Considerations

Discussion on how the system behaves in the face of attacks from:

- DoS/resource exhaustion
- Consensus node compromise
- Upstream compromise

1. Prefix-only delegation



2. Updated verification rules

- Valid (commitment) timestamps
- Signed by party authorized to update specified fields
- Does not violate prefix property
  - No overlapping delegations
  - No duplicate values

3. Security Considerations

Discussion on how the system behaves in the face of attacks from:

- DoS/resource exhaustion
- Consensus node compromise
- Upstream compromise

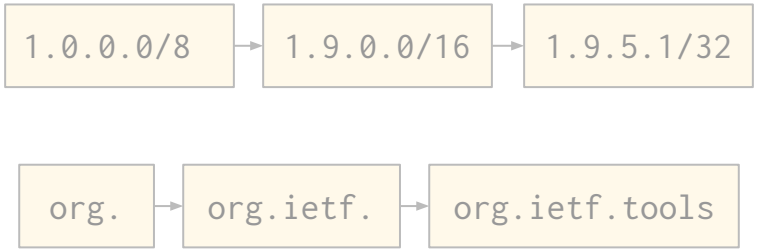
4. Table Allowances

New delegation field to recursively limit size of tables:

valuecells + delegatecell allowances <= table allowance

In certain cases, may be unlimited.

1. Prefix-only delegation



2. Updated verification rules

- Valid (commitment) timestamps
- Signed by party authorized to update specified fields
- Does not violate prefix property
  - No overlapping delegations
  - No duplicate values

3. Security Considerations

Discussion on how the system behaves in the face of attacks from:

- DoS/resource exhaustion
- Consensus node compromise
- Upstream compromise

4. Table Allowances

New delegation field to recursively limit size of tables:

valuecells + delegatecell allowances <= table allowance

In certain cases, may be unlimited.

Governance

Governance

Separation of Concerns

Mapping Safety

- Delegation rules
- Valid updates
- Verifying permissions
- Global consistency

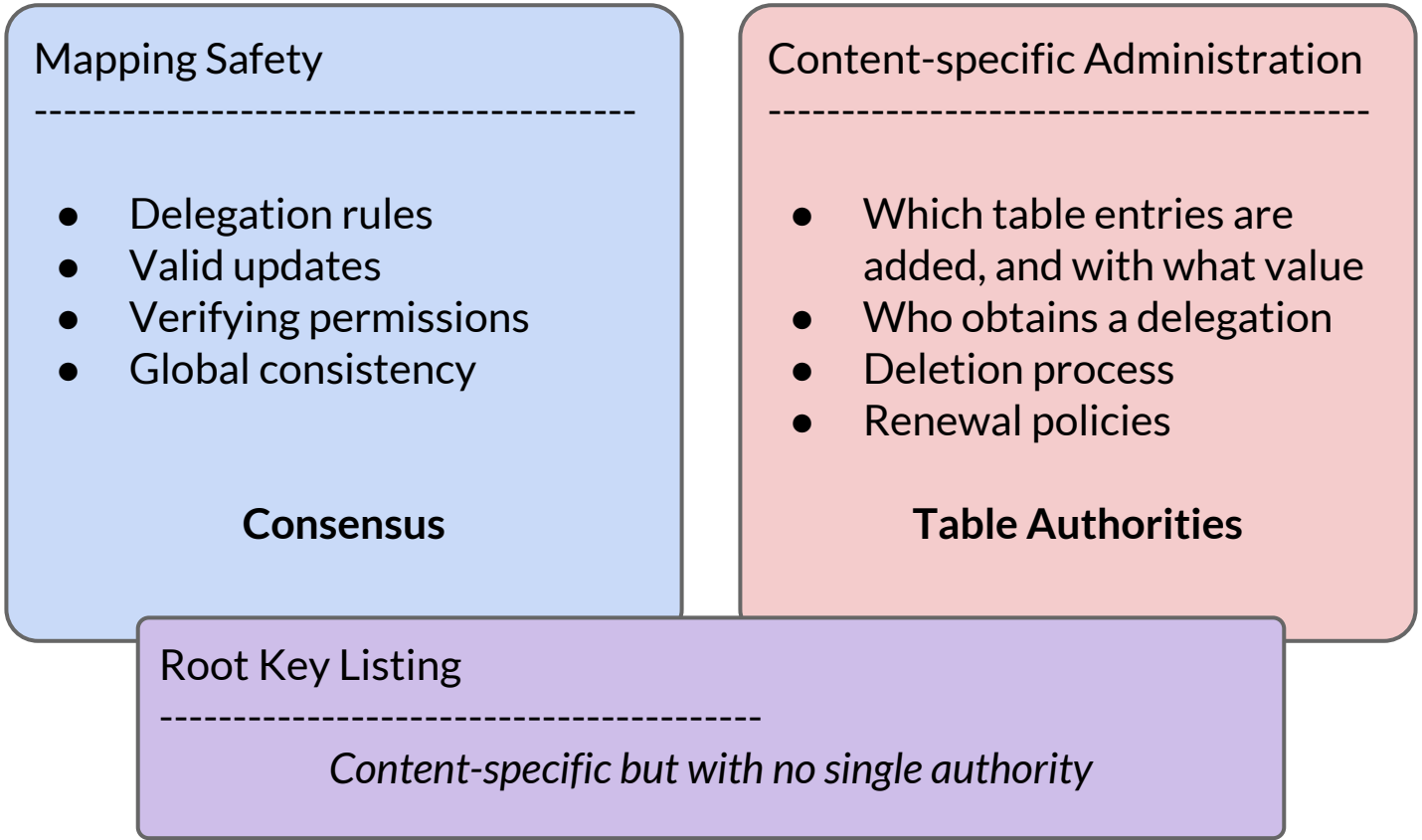
Consensus

Content-specific Administration

- Which table entries are added, and with what value
- Who obtains a delegation
- Deletion process
- Renewal policies

Table Authorities

Separation of Concerns



Separation of Concerns

Mapping Safety

- Delegation rules
- Valid updates
- Verifying permissions
- Global consistency

Consensus & **Voting**

Content-specific Administration

- Which table entries are added, and with what value
- Who obtains a delegation
- Deletion process
- Renewal policies

Table Authorities

Root Key Listing

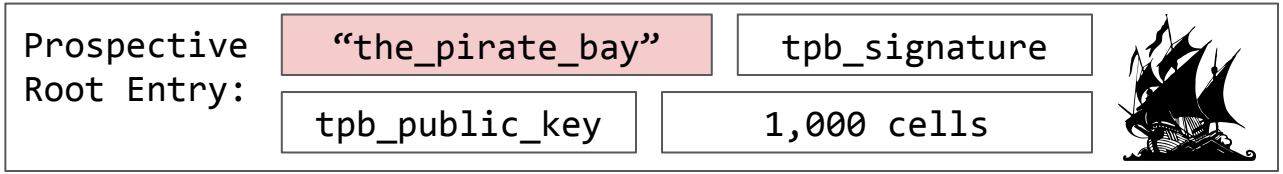
Content-specific but with no single authority

Voting

- Give consensus nodes agency to vote **for** or **against** significant, valid changes
- Explicit additional requirement for the underlying consensus scheme that is already common for protocol updates:
  - Quorums in slice infrastructures like SCP
  - Bitcoin-style percentage of agreeing blocks over a time window
  - Hard forks

Addressing governance through voting

Example:

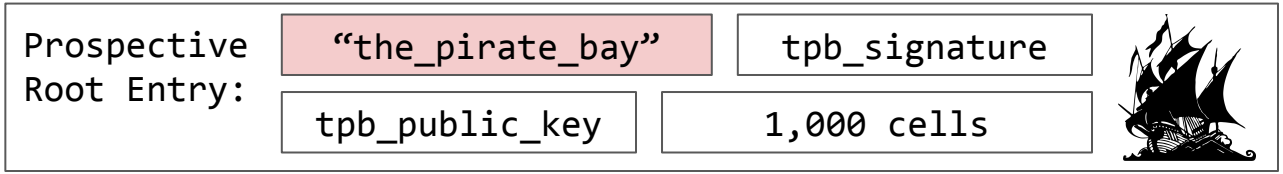


Two primary concerns from a consensus layer perspective:

① Some nodes may not want to support a root that is likely anti-copyright

②

① Root Application



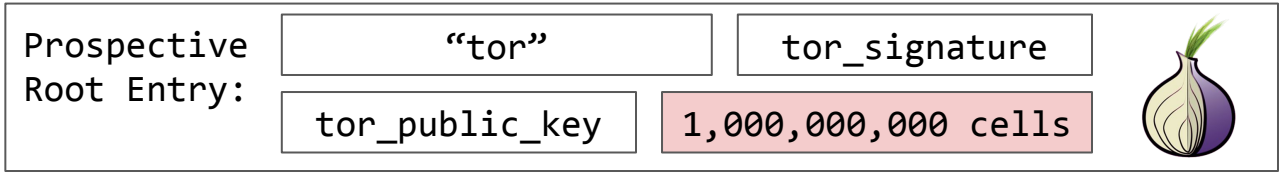
Nodes that disagree with *The Pirate Bay* can vote against the new root.

Potential outcomes:

- Vote on change succeeds → every node accepts that the root listing is updated even if they disagree with the new root’s application
- Vote fails → every node maintains the current listing
- Fundamental disagreement between significant node groups → realistically should not trust consensus relationships moving forward

Addressing governance through voting

Example:

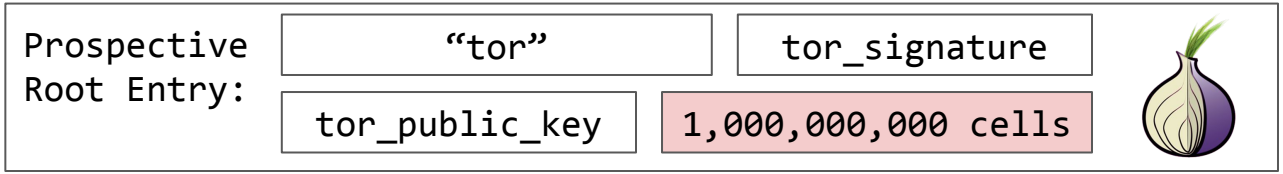


Two primary concerns from a consensus layer perspective:

① Some nodes may not want to support a root that is likely anti-copyright

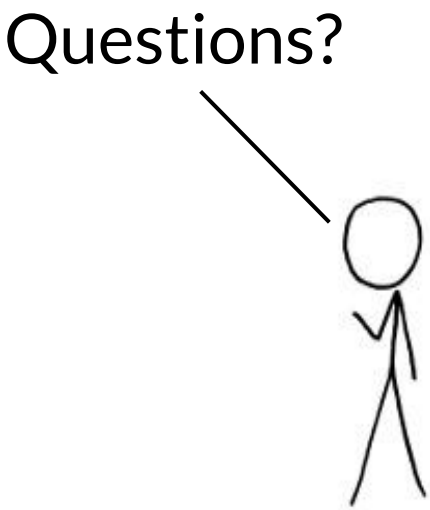
② Maintaining up to a billion mappings and their resulting requests would overburden some nodes’ infrastructure.

② Resource Consumption



Nodes evaluate resource usage by including explicit structural limits.

- Every node observes the same `allowance` value, enabling informed votes against new entries that may pose an unreasonable burden
- *Tor* must find large enough set of nodes willing to support 1 billion new cells OR change its request to a smaller, more reasonable value



https://tools.ietf.org/id/draft-watson-dinrg-delmap-01.txt