Tamperproof Root Zone Management System

Steve Crocker

9 October 2017

Motivation

- Some governments worry their ccTLD entry might be removed from the root zone abruptly and without their cooperation.
  - Yes, they know it's unlikely, and, yes, they know it would not cause immediate disruption, and, yes, they know it would cause the U.S. irreparable political harm. They worry nonetheless.
- Is it possible to design and field a system that precludes this possibility? **Yes.**

Basic Concepts (1)

1. Sealed system that cannot be tampered with.
   - Easiest if the RZM process is in one place, but feasible even if the functions are split across ICANN and Verisign.
2. Root zone is divided into portions associated with each TLD.
   - SOA, Root Servers and Glue records require additional discussion.

Basic Concepts (2)

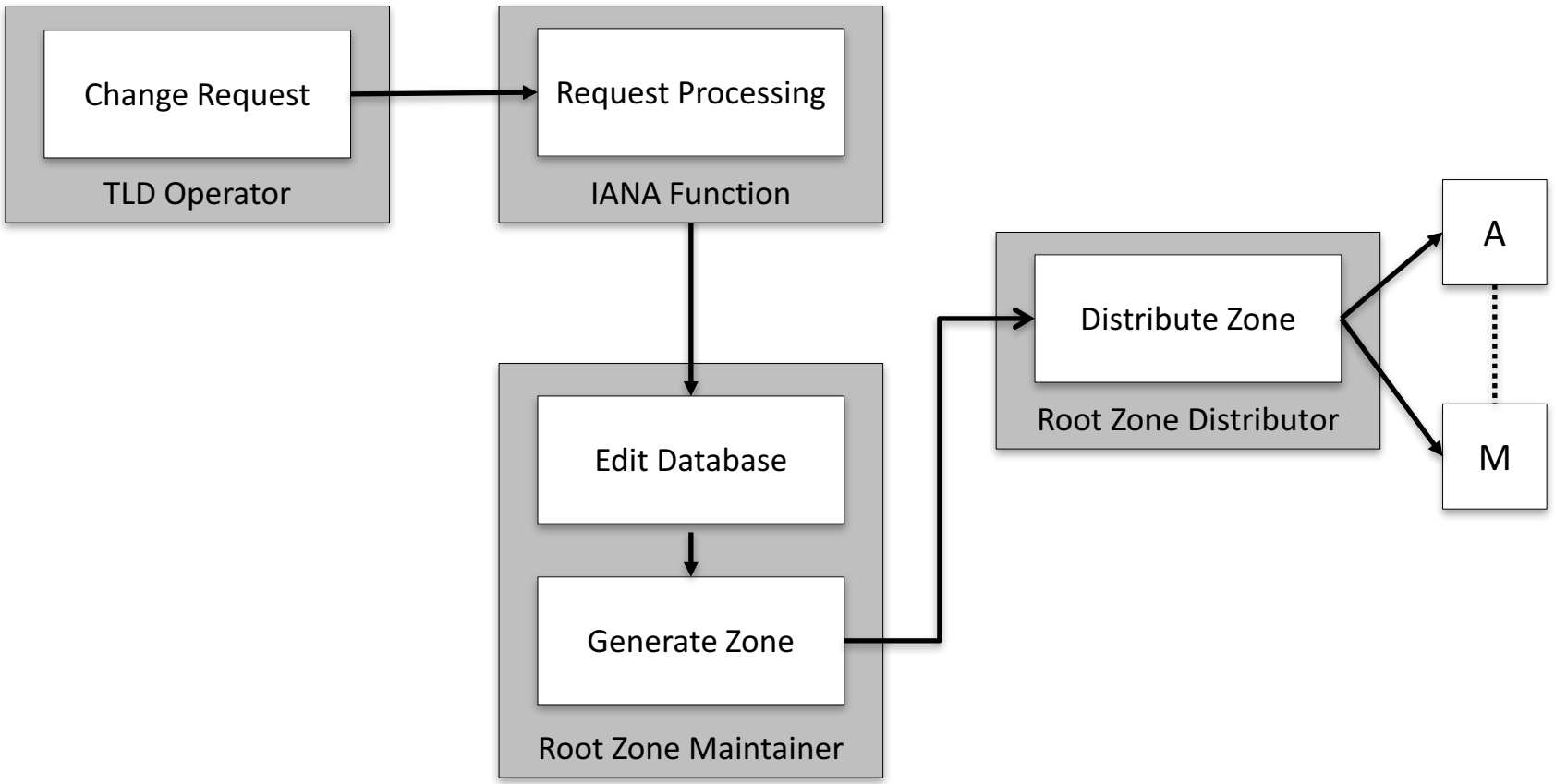
3. No change to a TLD's portion of the root without TLD operator's concurrence.
   - This does not address other potential complaints from ccTLD operators and their governments, e.g:
     - The TLD operator's wishes should be sufficient.
     - The TLD operator's request should be fulfilled immediately.
   - However, the creation of this system may cause attention to these other complaints.

Basic Concepts (3)

4. A separate mechanism is needed to associate a TLD operator with its portion of the root zone.
   - Cannot be done with purely mechanical controls.
   - Multi-party political control needed.
5. Not all TLD operators will be ready to fit into tamperproof system right away. A transition or hybrid mechanism is required.

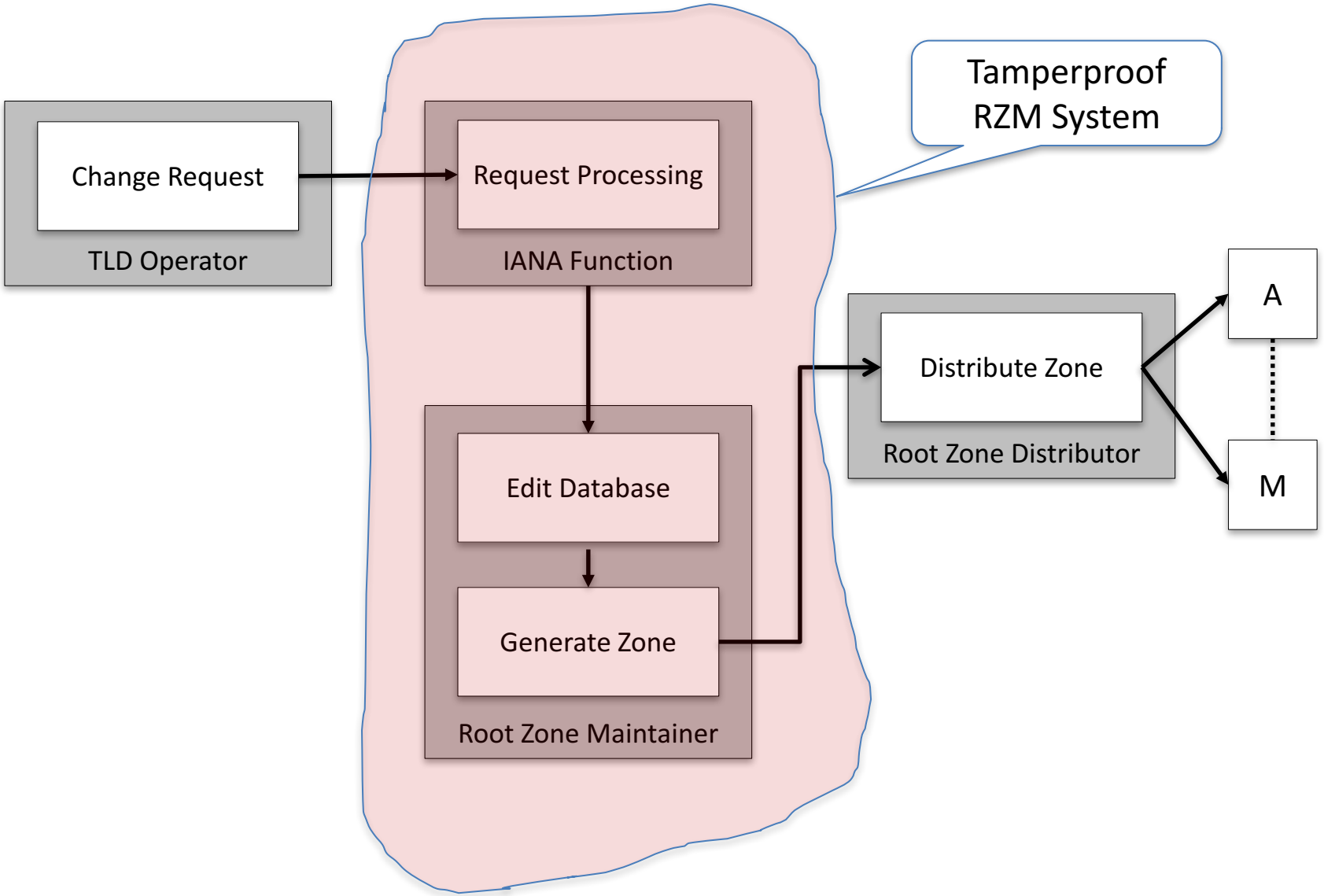
Current Root Zone Update Process

(Simplified: Key Generation and Signing Not Included)



Future(?) Root Zone Update Process

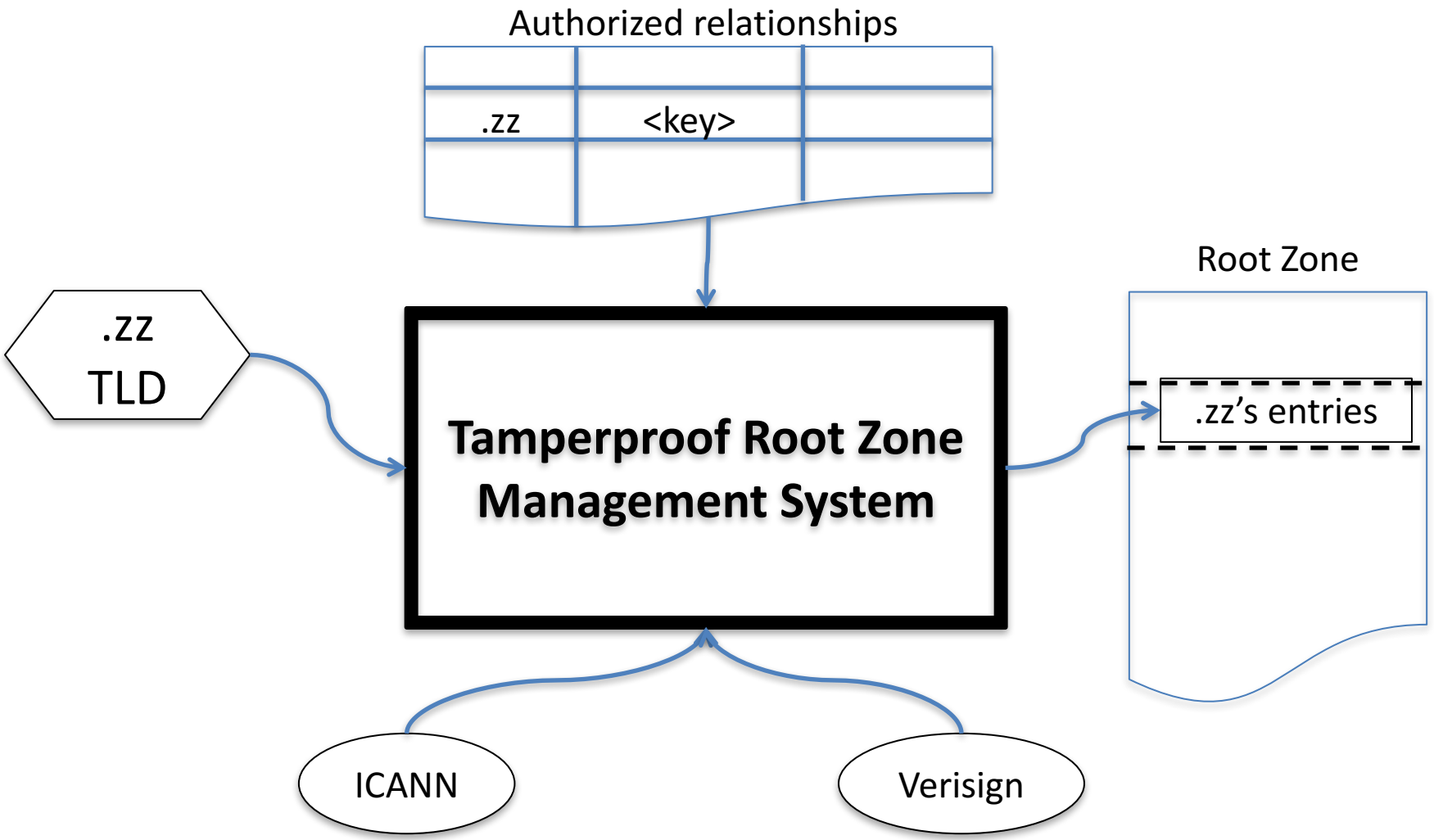
(Simplified: Key Generation and Signing Not Included)



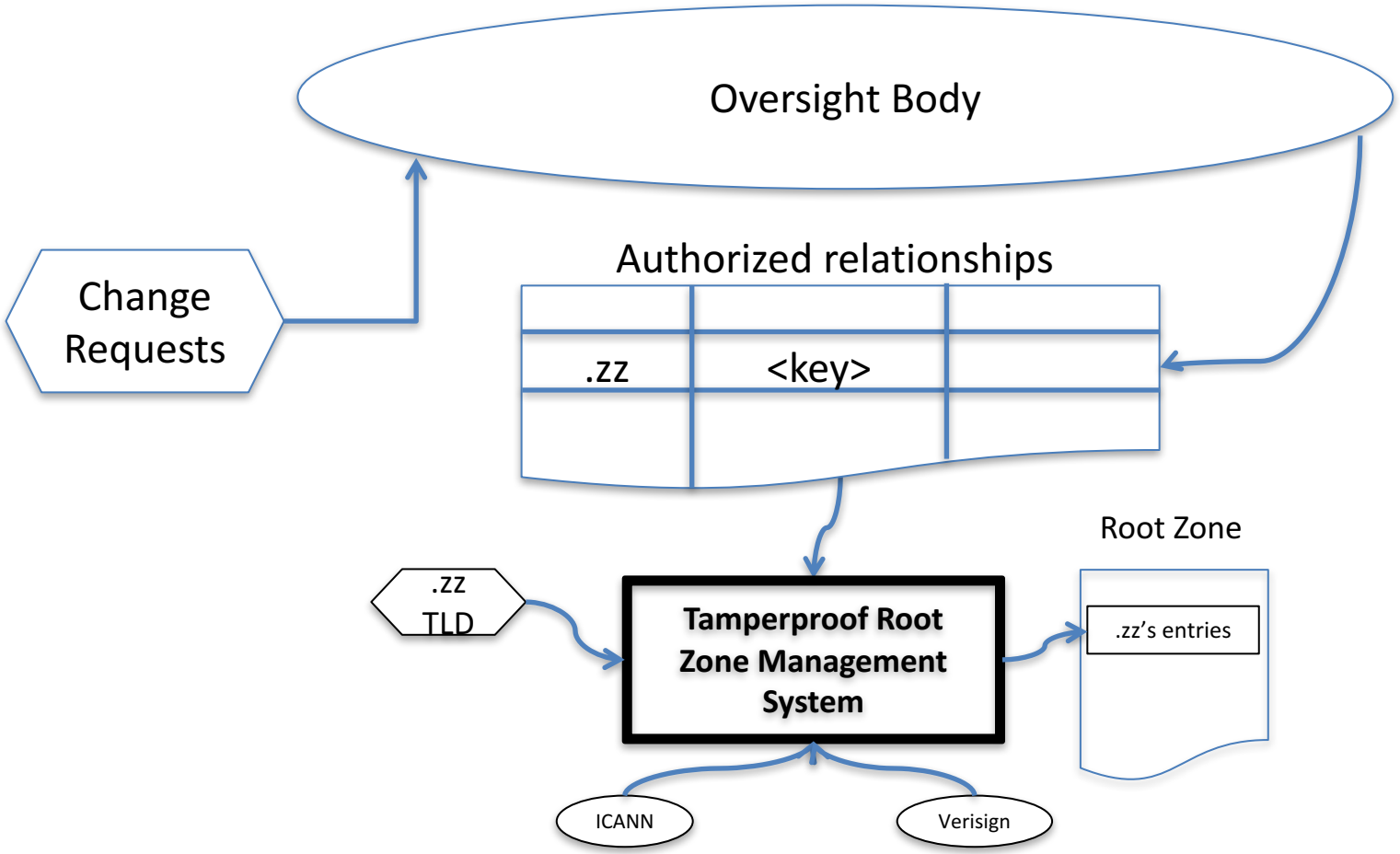
Two types of Transactions

- “Ordinary” updates
  - Changes in NS records
  - Changes in DNSKEY (or DS?) records
  - Associated glue records
- Major changes
  - Initial assignment and changes of control
  - Changes in contact info

Ordinary Changes



Major Changes



Oversight Body & Authorized Relationships

- Oversight Body composed of representatives from the world – similar to root key TCRs
- Authorized Relationships visible everywhere
- Process for change should be slow and deliberate

Next Steps

- Flesh out conceptual design
  - Include key management
  - Two tracks, single vs split organization
  - Choices in protocols for update requests
- Concept paper for circulation
- Operational practices document
- Decide whether to proceed with any or all of the three parallel paths.
- Breadboard design
- Etc.

Three Parallel Paths

- Protocol between TLD operators and IANA
- Protocol within Root Zone Maintainers
- Procedures for the initial assignment, reassignment, etc. using community oversight