Signing the DNS Root

Signing the root ...

- Insight since earliest versions of DNSSEC.
  - About 1994.
- There has been talk for more than a decade.
- Various test beds:
  - Local lab environments: dnslab.net
  - EP.net
  - Versign
  - IANA
- General progress at glacial speed ... ☹

Last six months ...

- Proven: even glaciers move ...
- Two “solid” proposals on how to do it.
  - Verisign
  - IANA
- October 2008: Department of Commerce National Telecommunications and Information Administration (DoC NTIA) issues “Notice of Inquiry” (call for public comment).

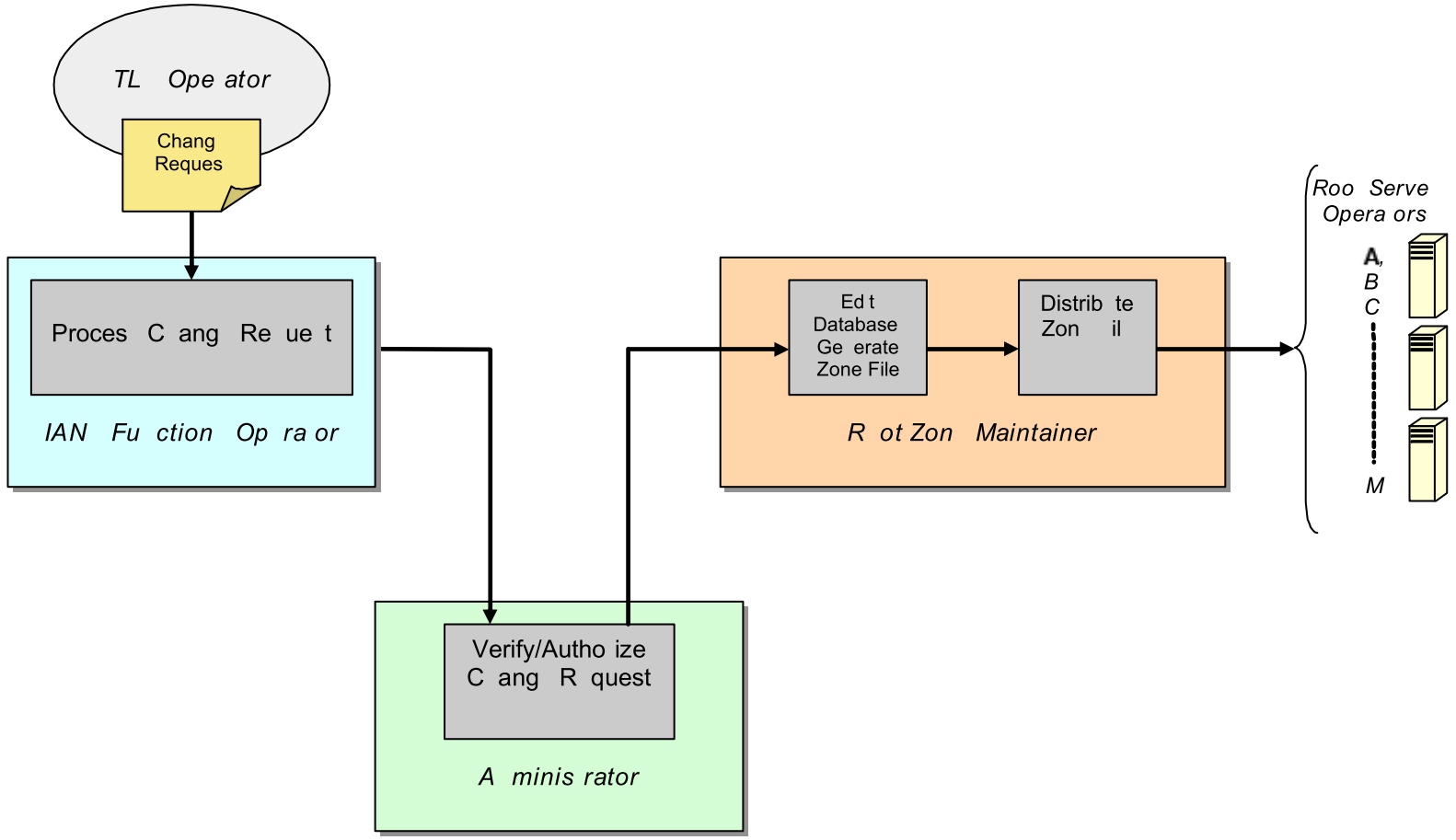
Issues?

- Two key pairs:
  - Key Signing Key (KSK) – renewed "seldom", trust anchor.
  - Zone Signing Key (ZSK) – renewed "often".
- Signing Process
  - Zone signing
  - Key signing
- Key generation
- Key storage
- Key access
- Who does what where?
- Interpretation of signatures.
  - What does it mean that a delegation is signed?
  - No change of "controls over the content".

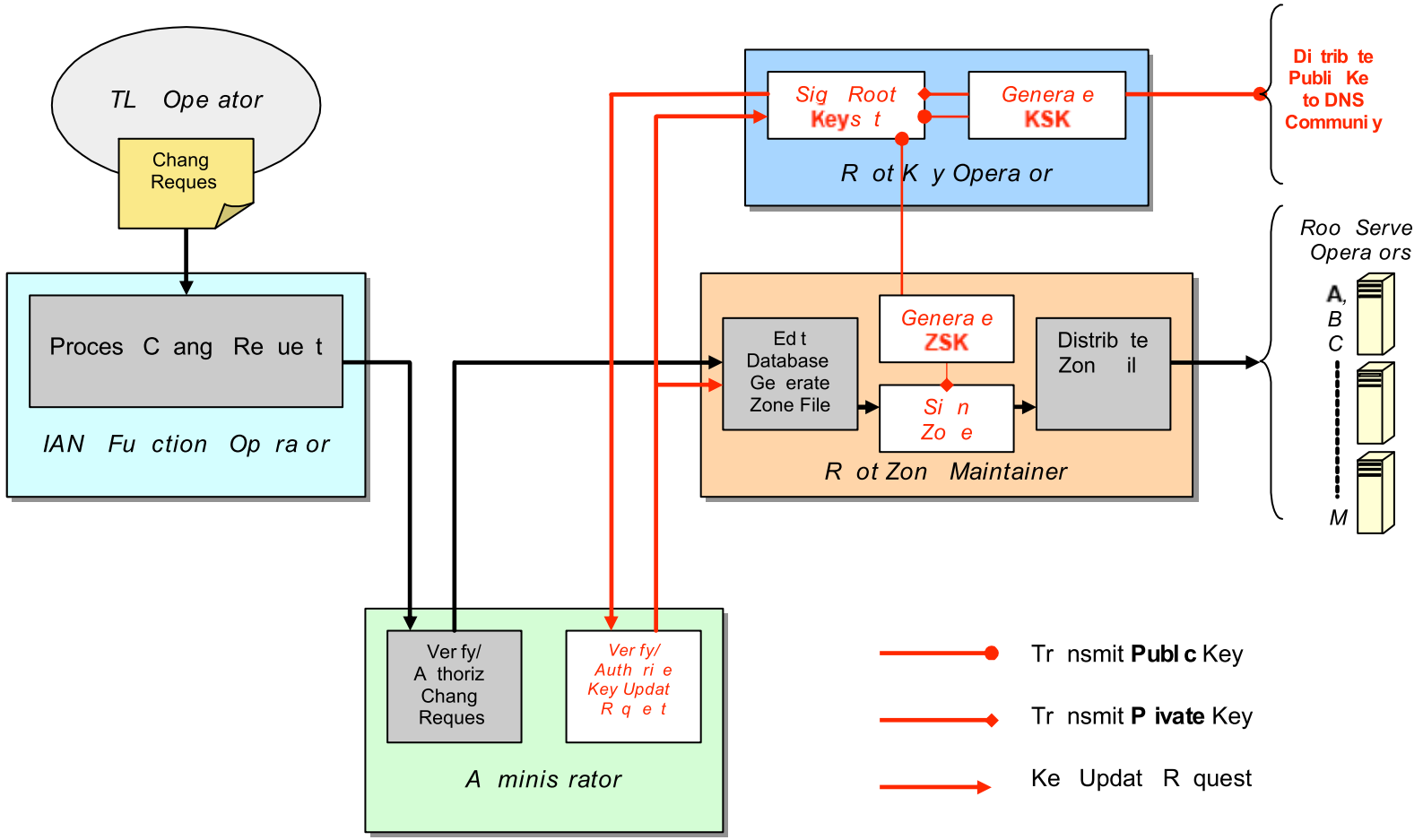
DoC NTIA proposals

- The following slides have depressingly small print.
- Sorry.
- They're not mine. ☺
- Stolen from
- http://www.ntia.doc.gov/DNS/DNSSEC.html

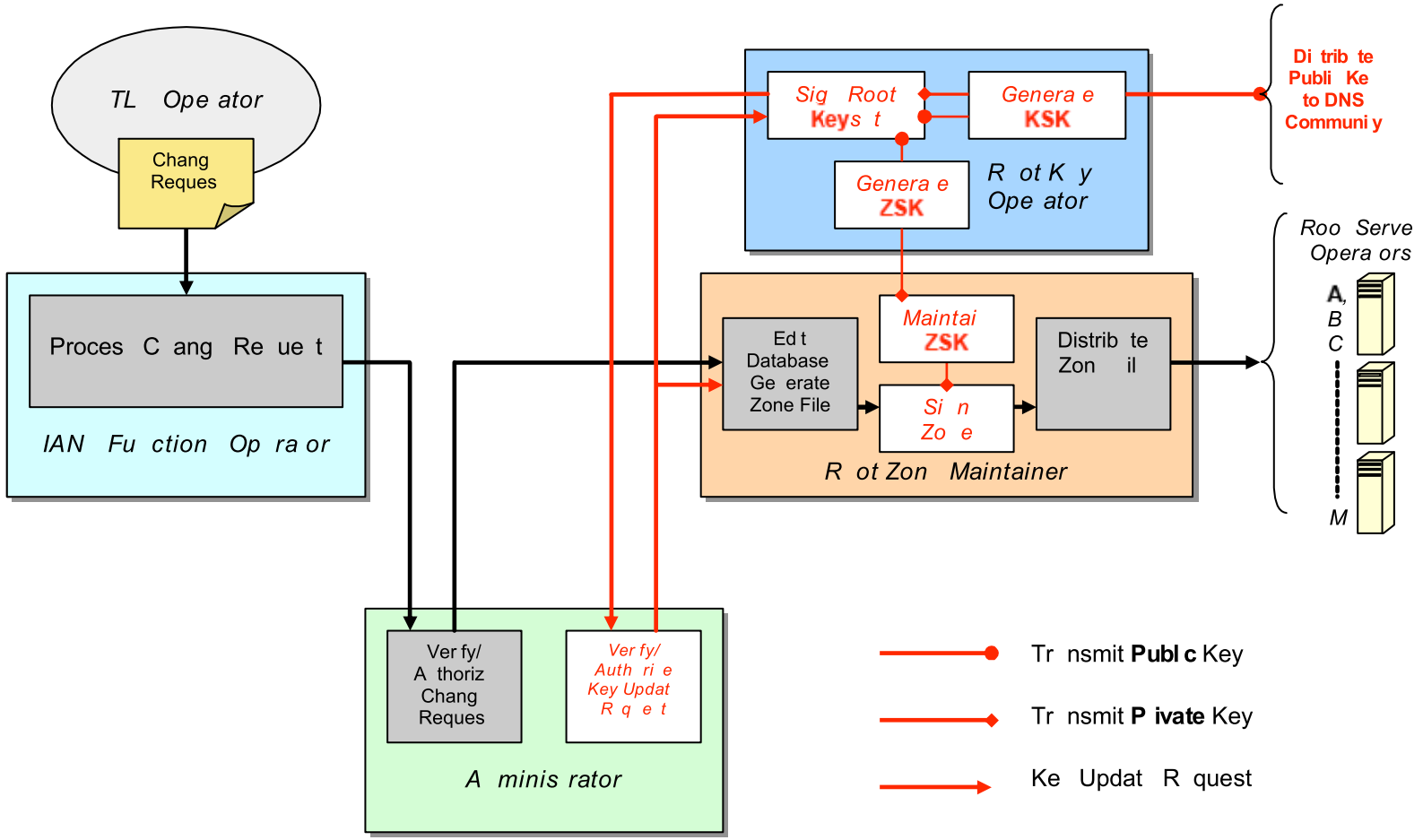
Authoritative Root Zone Management Process (Present)



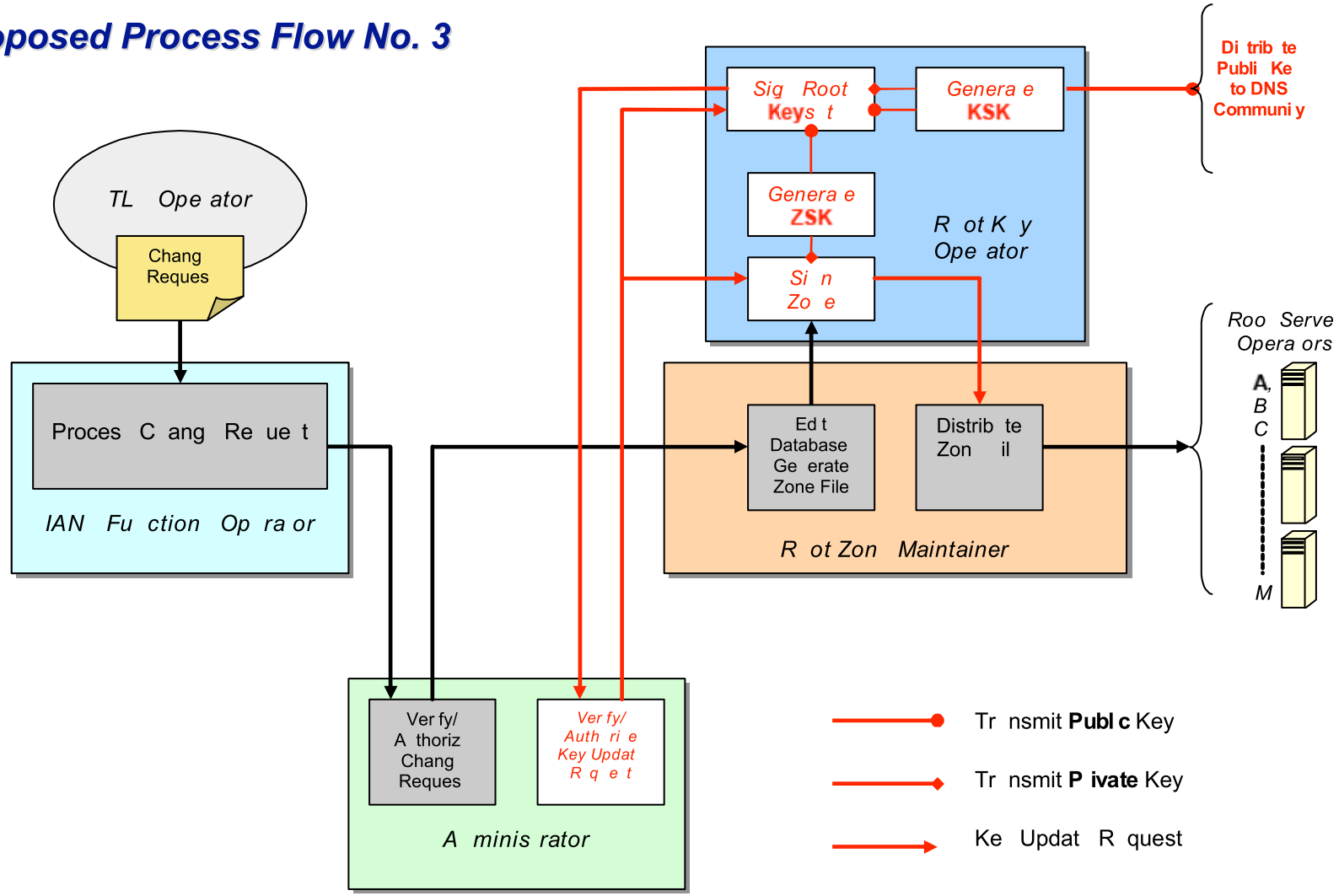
Proposed Process Flow No. 1



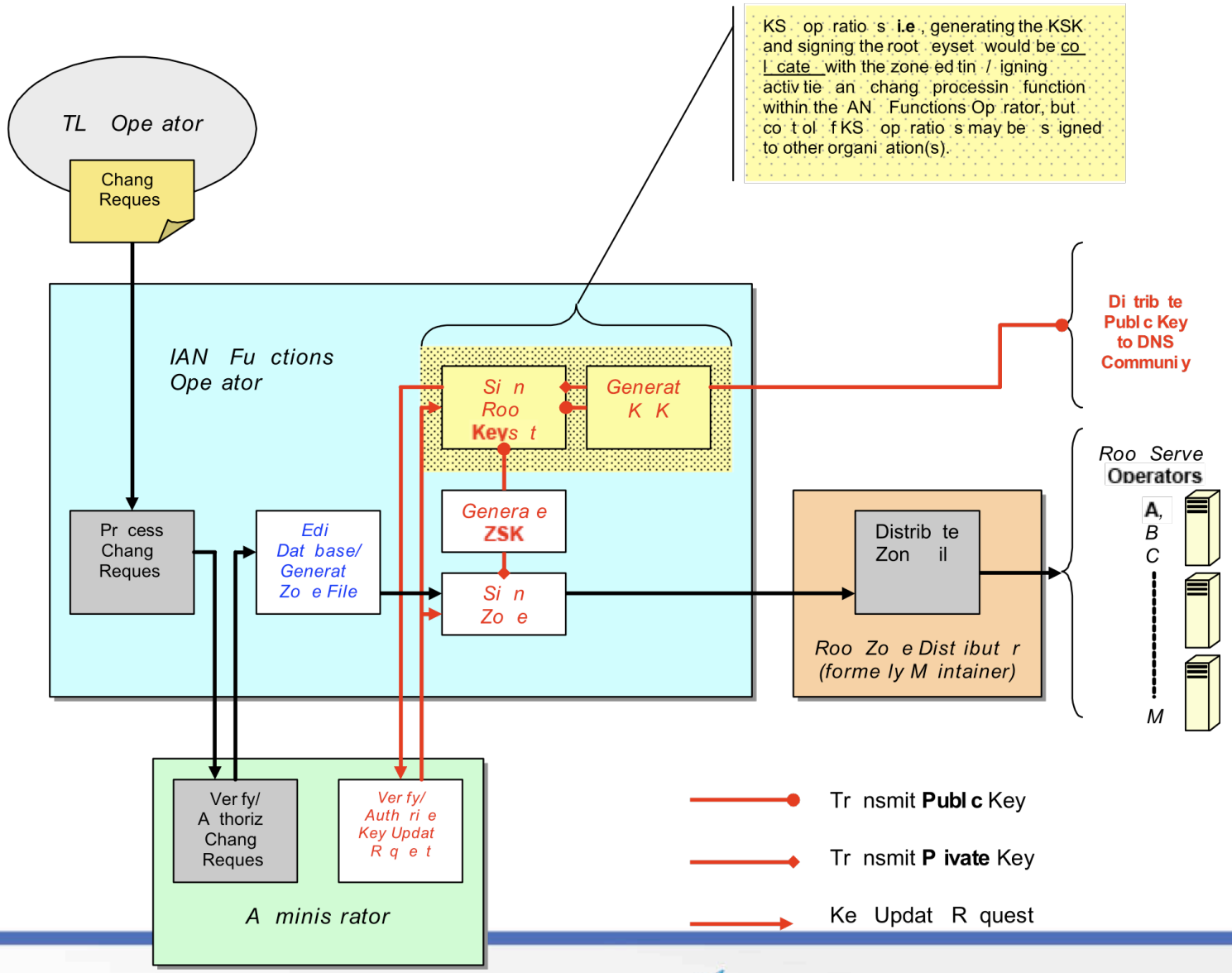
Proposed Process Flow No. 2



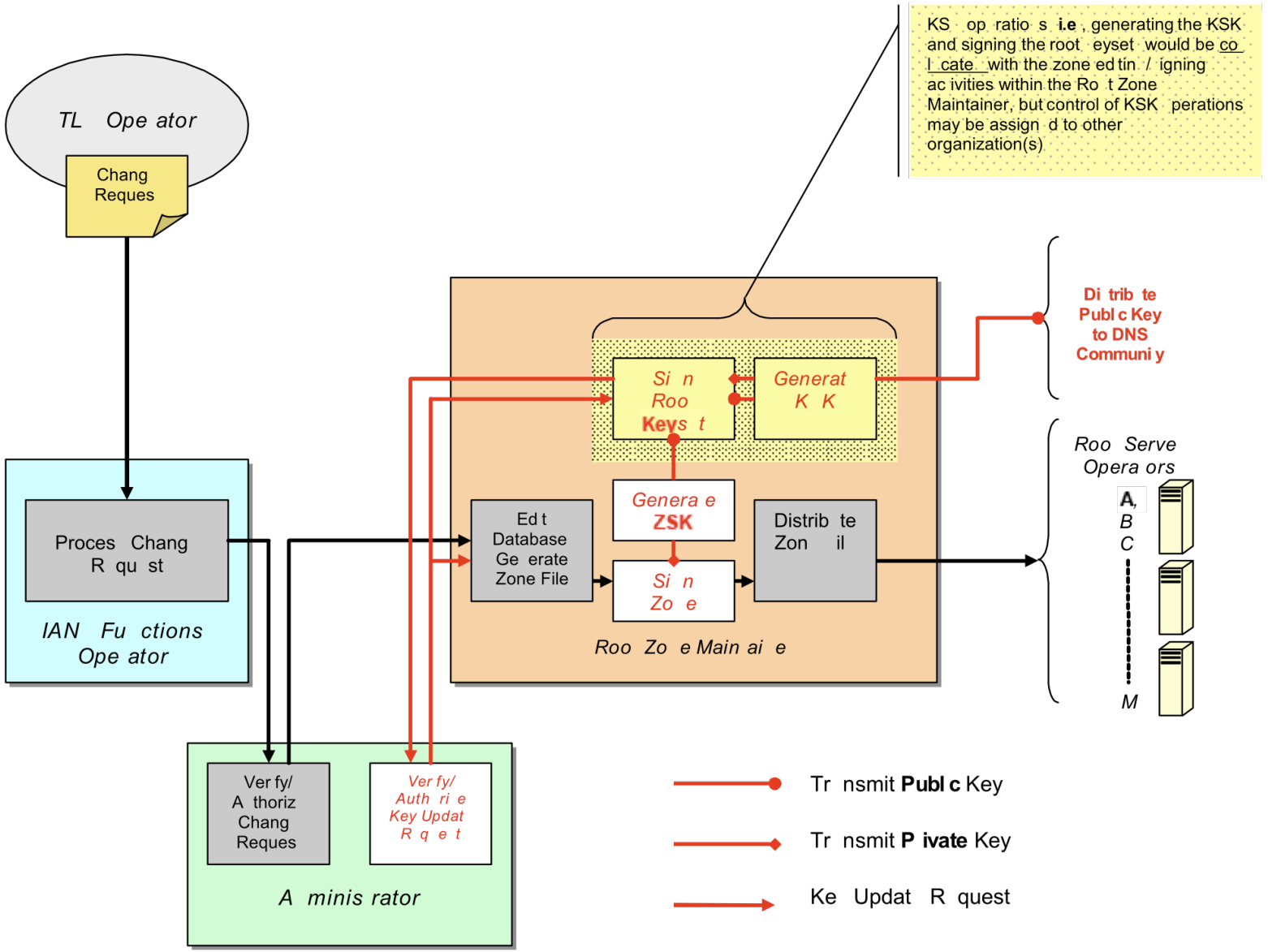
Proposed Process Flow No. 3



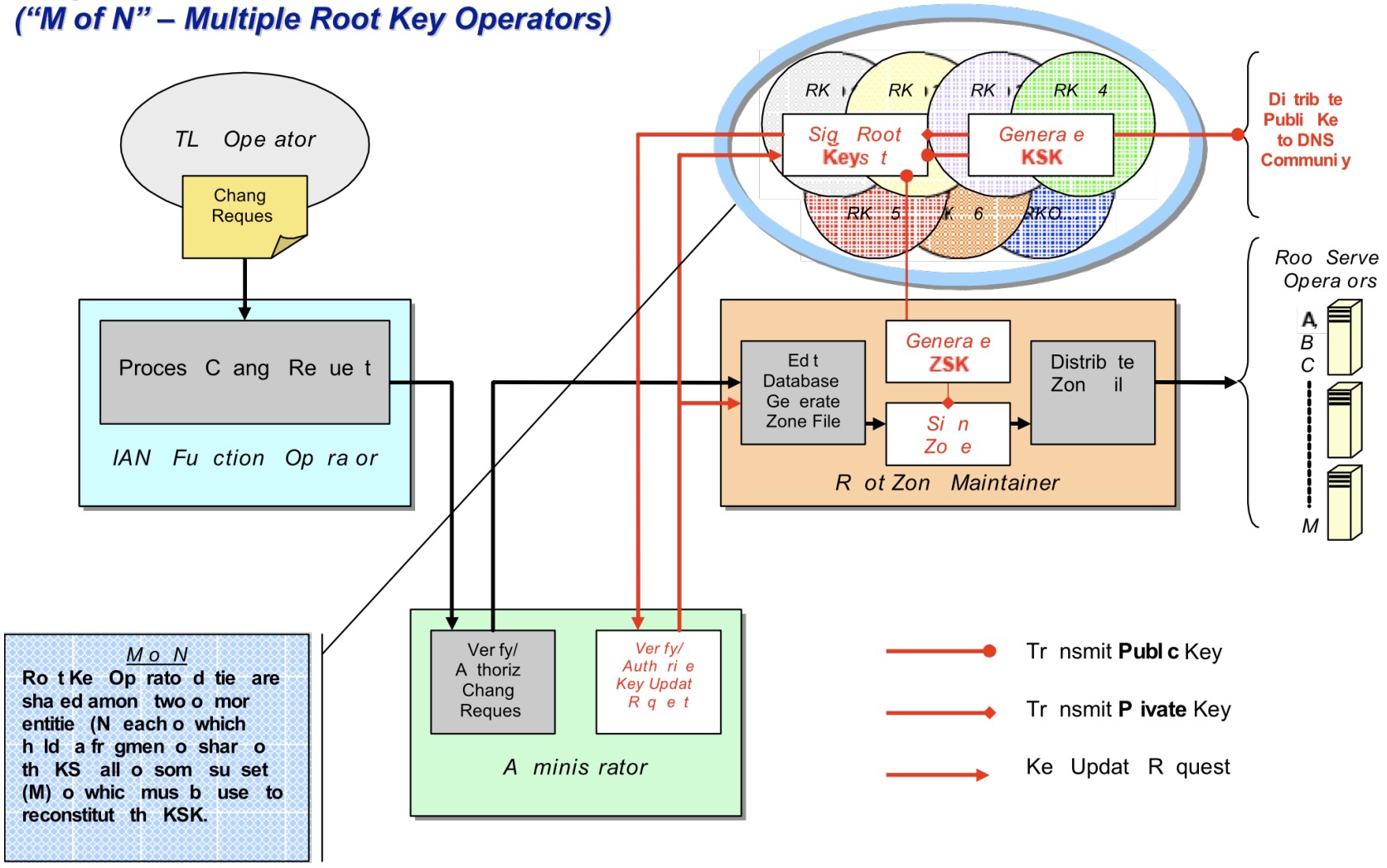
Proposed Process Flow No. 4



Proposed Process Flow No. 5



Proposed Process Flow No. 6
("M of N" – Multiple Root Key Operators)



Verisign Proposal (basically no. 6)

Pros:

- Procedures in place.
- Secure facilities.
- Minimal change to current roles.
  - "Quick" implementation?
  - Little political pushback?
- De-couples DB content from signature.
- "N of M" is neutral.

IANA's Proposal (basically no. 4)

Pros:

- Cleaner process.
- "All" under one roof.
- Gets Verisign out of the loop (more or less ...).
- Not-for-profit org.
- International endorsement?

EU ENISA Workshop

- European Network and Information Security Agency
  - EU Agency
- "Technical" Workshop in Brussels early in Feb 2009.
- Presentations by people "pro" and "con" DNSSEC.
  - Presentations and panel discussion.
- NTIA invited, but didn't show up. ☹
  - Would have been interesting ...
- Surprisingly many *against!*
  - Suprising amount of "no business case"!
- It's not about business, it's about infrastructure.
  - It's not about "selling domains", it's about "facilitating security".

Alternatives?

- DNS Lookaside Validation (DLV)
  - Involves 3rd party ...
  - ... who signs delegations upon request.
  - ... and which has to duplicate a lot of registry work.
  - "Dirty hack" to work around the root problem.
- Trust Anchor Repositories (TARs)
  - Don't scale ...
- Cryptographically they both provide similar functionality to a signed root, but for some reason with less political attention ...
- Break the clean (ahem! ☺) DNSSEC design.

Final Comments

- When is more important than who!
  - Get it done NOW!
  - We *can* change the process at a later stage.
- There *are* real problems in there ...
  - ... but only a few of them are technical ...
  - ... and the other ones are typically harder ... ☹
- US administration shows strong interest:
  - .GOV is already signed. Demands all subzones signed by end 2009.
  - .MIL, .US, and .EDU have more or less firm plans to sign.
  - This increases the pressure to sign the root.

Questions?