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".





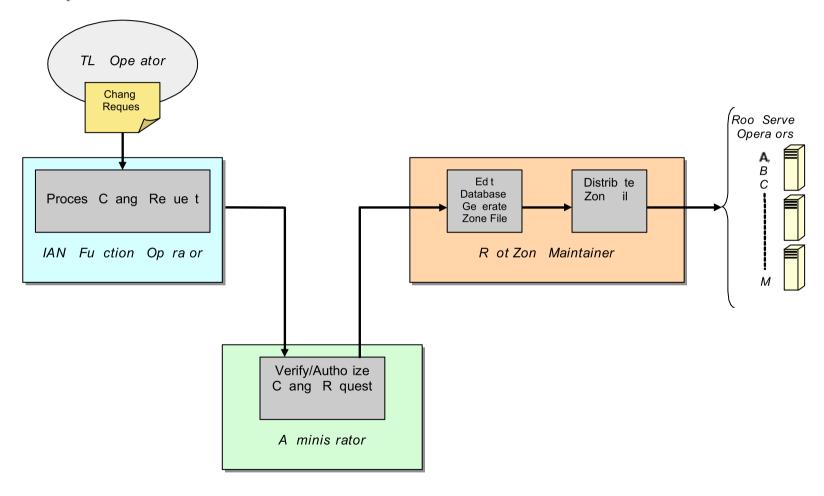
DoC NTIA proposals

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





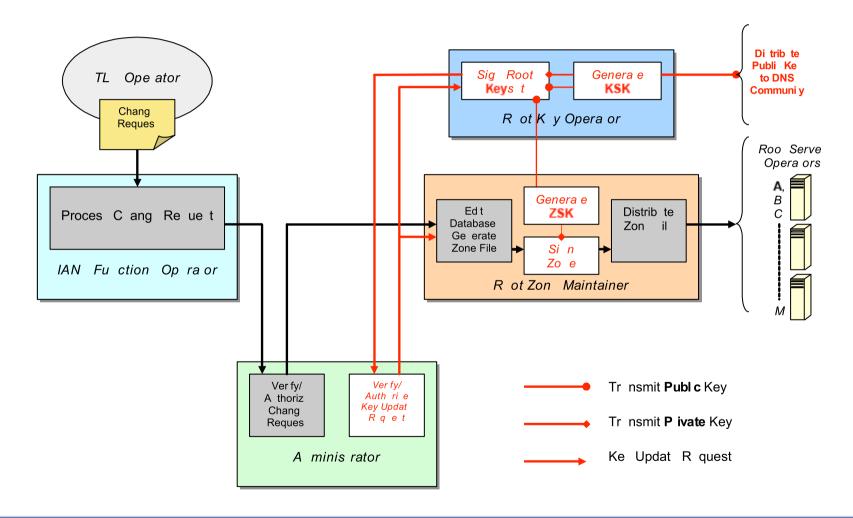
Authoritative Root Zone Management Process (Present)







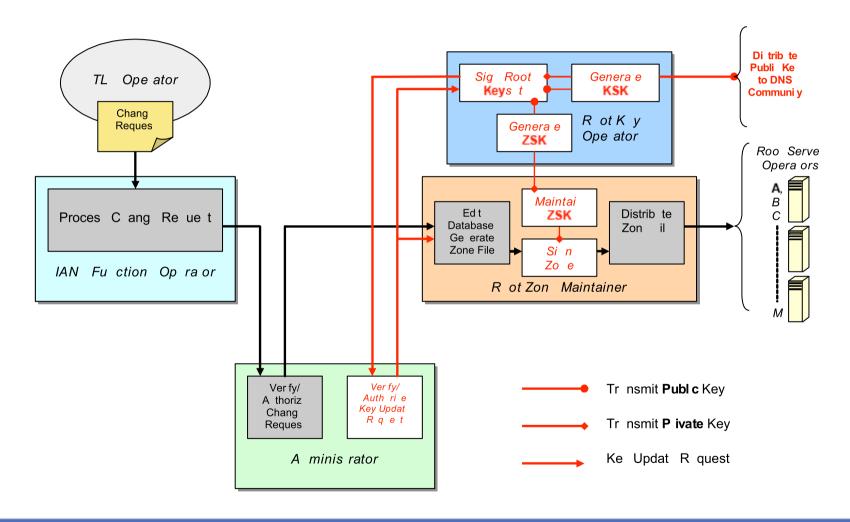
Proposed Process Flow No. 1





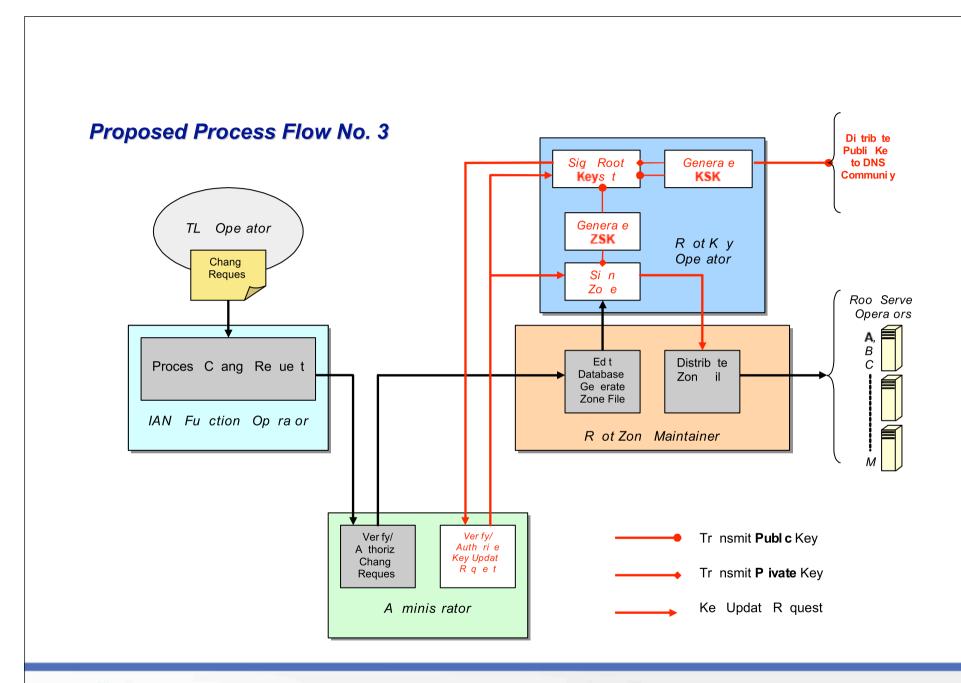


Proposed Process Flow No. 2











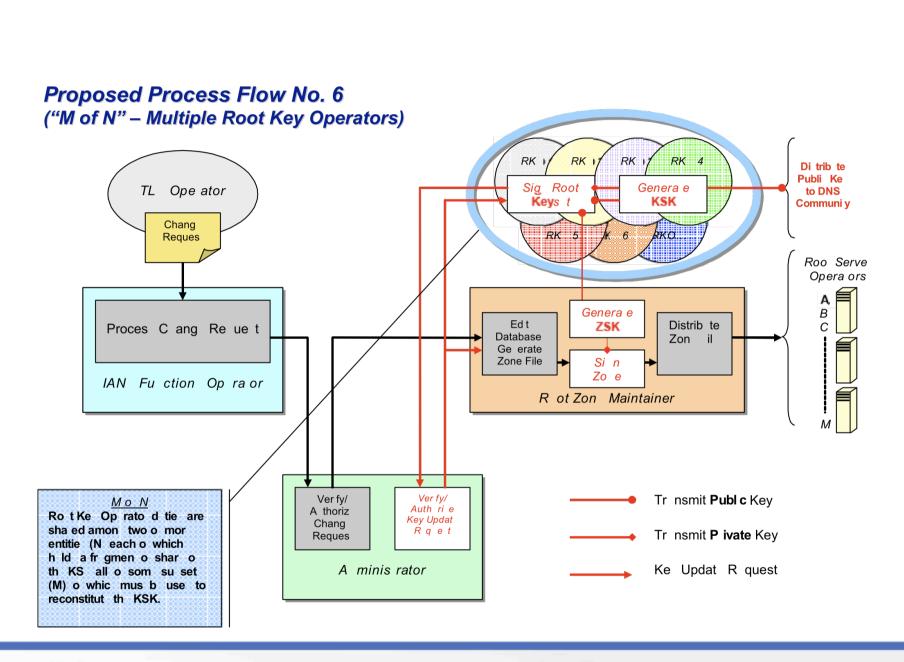


Proposed Process Flow No. 4 KS op ratio s i.e , generating the KSK and signing the root eyset would be co I cate with the zone ed tin / igning activitie an chang processin function within the AN. Functions Op rator, but TL Ope ator co tol fKS op ratio s may be s igned to other organi ation(s). Chang Reques Di trib te Publ c Key to DNS IAN Fu ctions Communi y Ope ator Generat Roo KKeys t Roo Serve Operators Genera e Edi Pr cess Distrib te ZSK Chang Dat base/ Zon il Reques Generat Zo e File Si n Zo e Roo Zo e Dist ibut r (forme ly M intainer) Ver fy/ Tr nsmit Publ c Key Ver fy/ Auth ri e A thoriz Key Updat Chang RqetTr nsmit P ivate Key Reques A minis rator Ke Updat R quest NETNOD

Proposed Process Flow No. 5 KS op ratio s i.e , generating the KSK and signing the root eyset would be co I cate with the zone ed tin / igning ac ivities within the Ro t Zone Maintainer, but control of KSK perations TL Ope ator may be assign d to other organization(s) Chang Reques Di trib te Publ c Key to DNS Communi y Generat Roo KKevs t Roo Serve Opera ors Genera e Ed t Distrib te В ZSK Database Proces Chang Zon il Ge erate R qu st Zone File Si n Zo e IAN Fu ctions Roo Zo e Main ai e Ope ator Ver fy/ Tr nsmit Publ c Key Ver fy/ Auth ri e A thoriz Key Updat Chang RqetTr nsmit P ivate Key Reques Ke Updat R quest A minis rator











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?



