

key-timing

Stephen Morris
John Dickinson
Johan Ihren
Matthijs Mekking

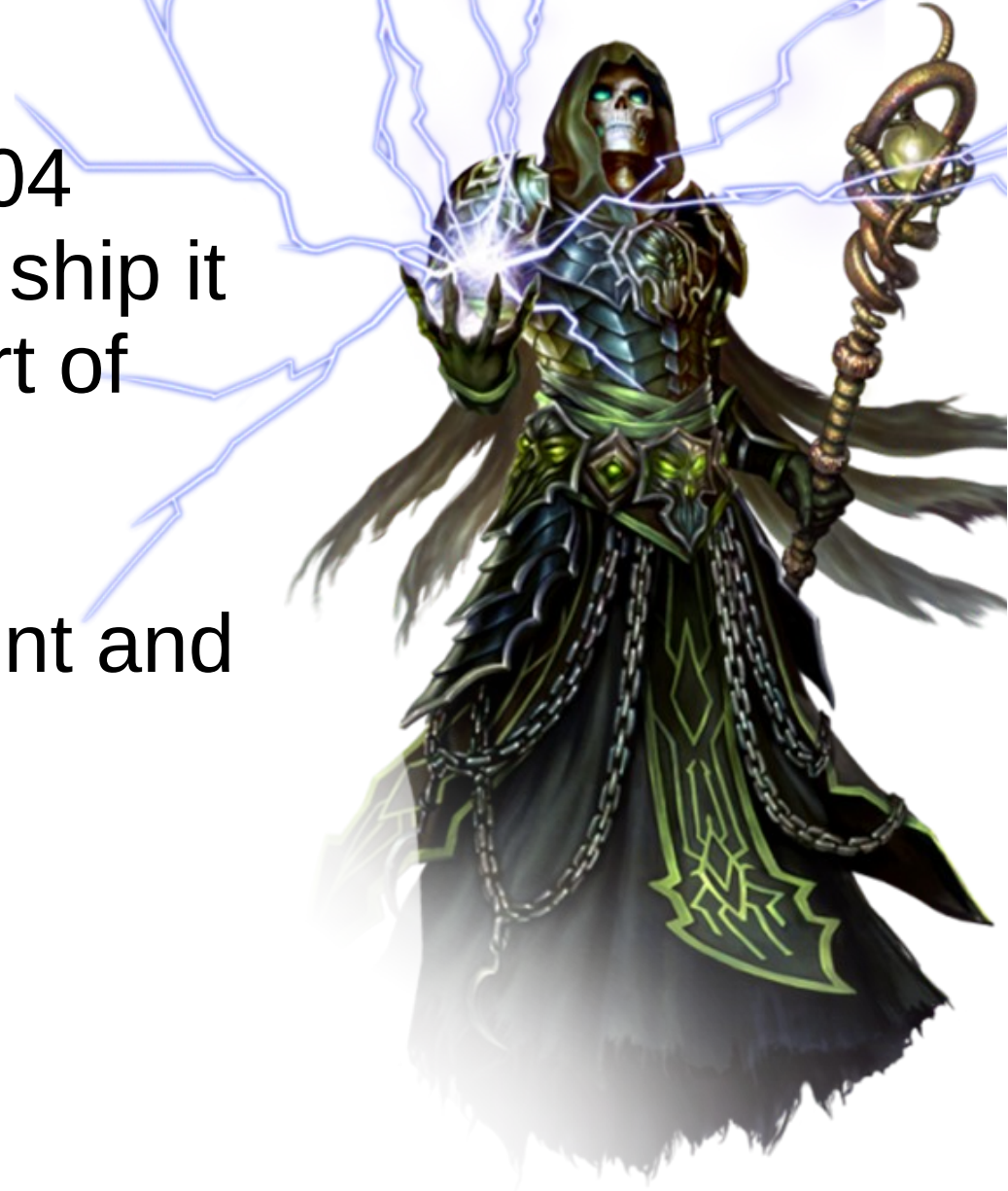
IETF90, dnsop

key-timing: the past

- Version -03 was two years ago
- There was an alternative document:
- *draft-mekking-dnsop-dnssec-key-timing-bis*
- Consensus was to ship the key-timing draft
- So there was a WGLC in August 2012
- And then nothing

key-timing: the present

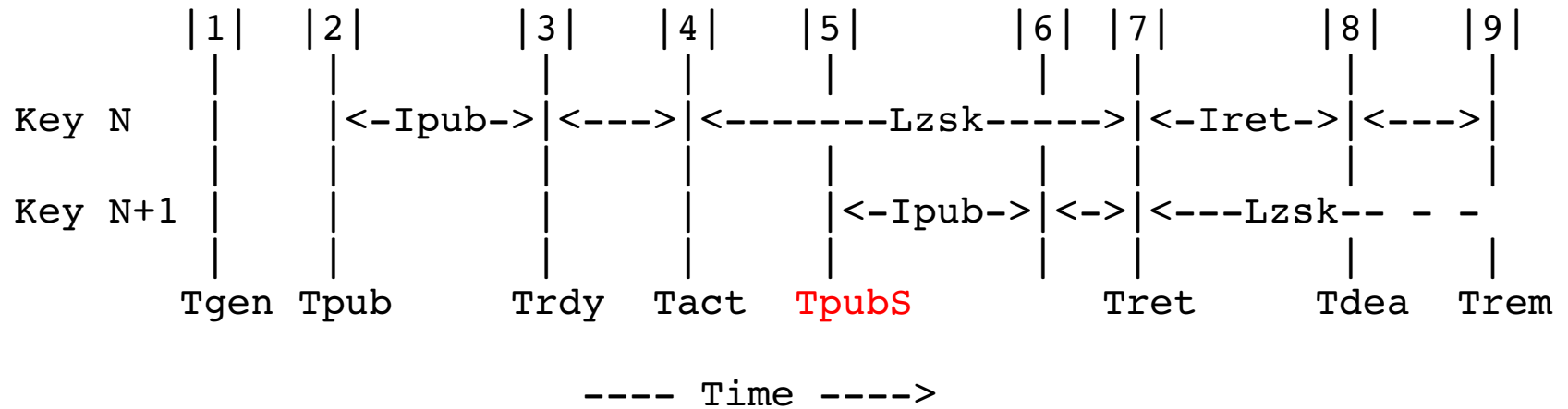
- We are now at version -04
- The consensus still is to ship it
- “We are practicing the art of necromancy” - Tim
- New co-editor
- We patched the document and think its much cleaner



key-timing: the present

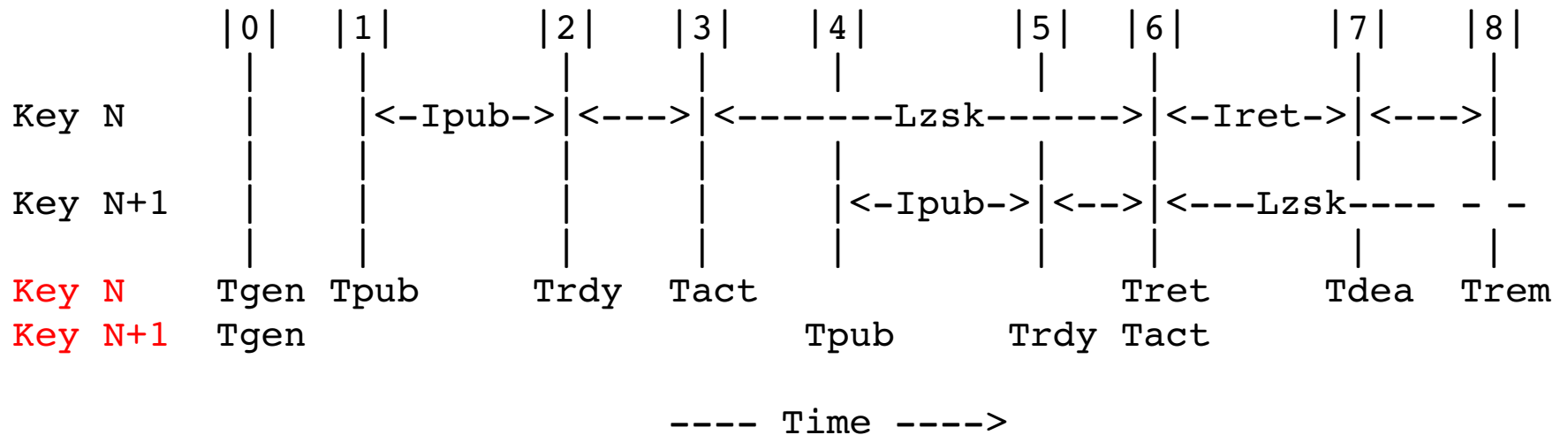
- Lots of editorial changes
- KSK Double-Signature is renamed Double-KSK
- Summary table removed
- ZSK Double-RRSIG has been removed
- Update diagrams and text to better reflect key states and key lifetimes.

key-timing: the present



$$\text{Trdy} = \text{Tpub} + \text{Ipub}$$

key-timing: the present



$$\text{Trdy}(N) = \text{Tpub}(N) + \text{Ipub}$$

key-timing: the future

- New WGLC
- There are ideas for improvement
- But let's discuss that after we ship this

