DNSSEC
Key Rollovers and Timing Issues:

`draft-morris-dnsop-dnssec-key-timing-00`

John Dickinson, John Dickinson Consulting

Johan Ihrén, Autonomica AB,

Stephen Morris, Nominet

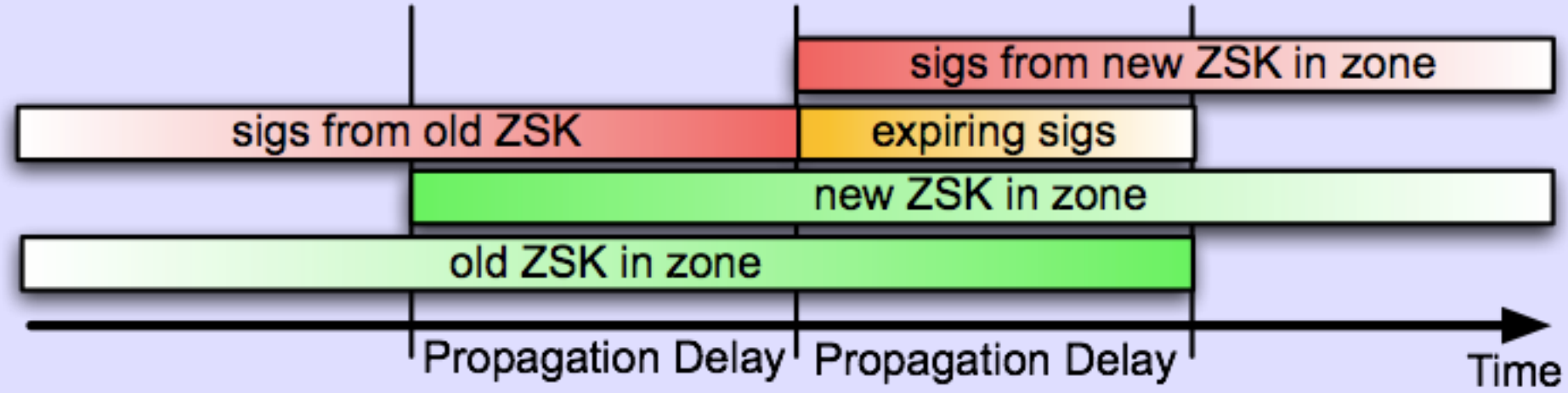
Aim of the draft

- Our aim is to describe the underlying logic of DNSSEC key rollovers in a rigorous way
  - including the associated equations and relations that determine and affect parameter and policy choices
- We acknowledge that rollovers have been described elsewhere

Key Rollovers Are

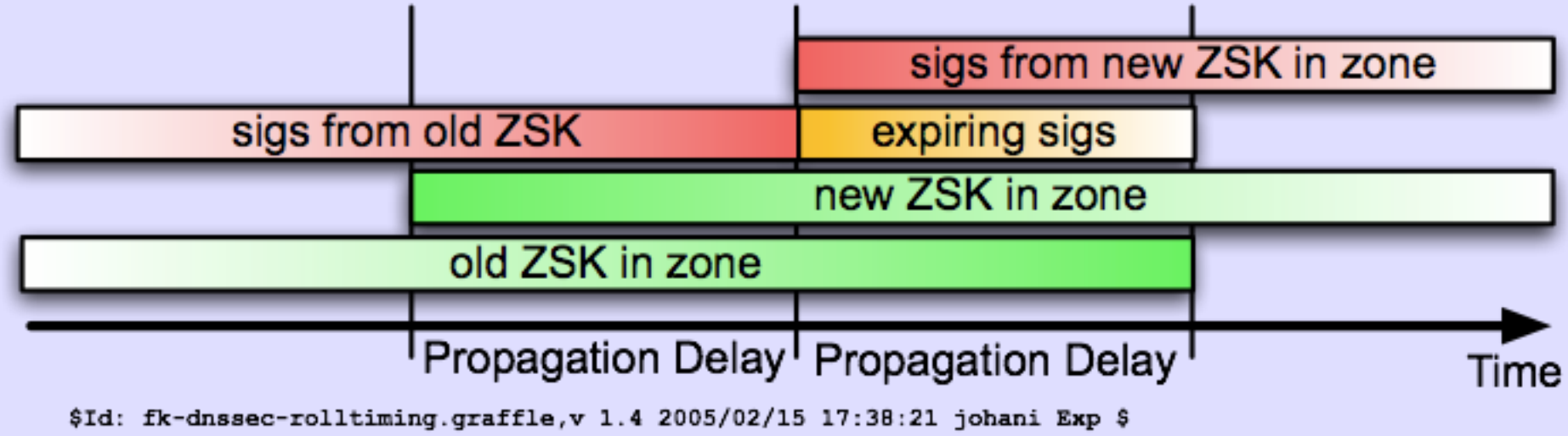
- Rollovers are conceptually easy
  - there are several RFCs that cover parts of the complexity, e.g. RFC4641
- Rollovers are technically challenging, mainly due to the various timing constraints that affect "safe behaviour"
  - the timing issues have not previously been completely described (as far as we've found)

The ZSK Rollover



$Id: fk-dnssec-rolltiming.graffle,v 1.4 2005/02/15 17:38:21 johani Exp $

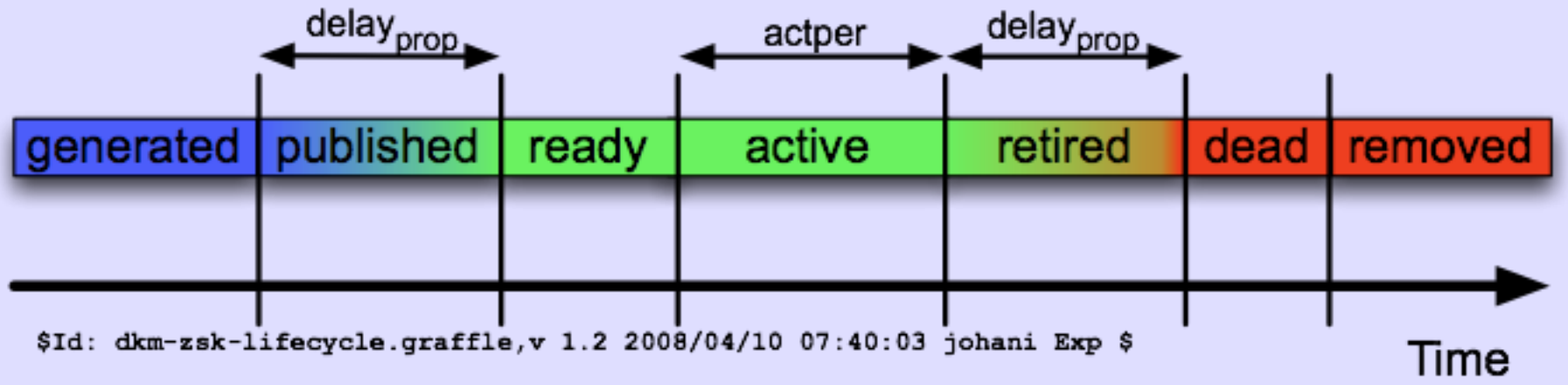
The ZSK Rollover



- But is this all there is to the story?

ZSK State Transitions

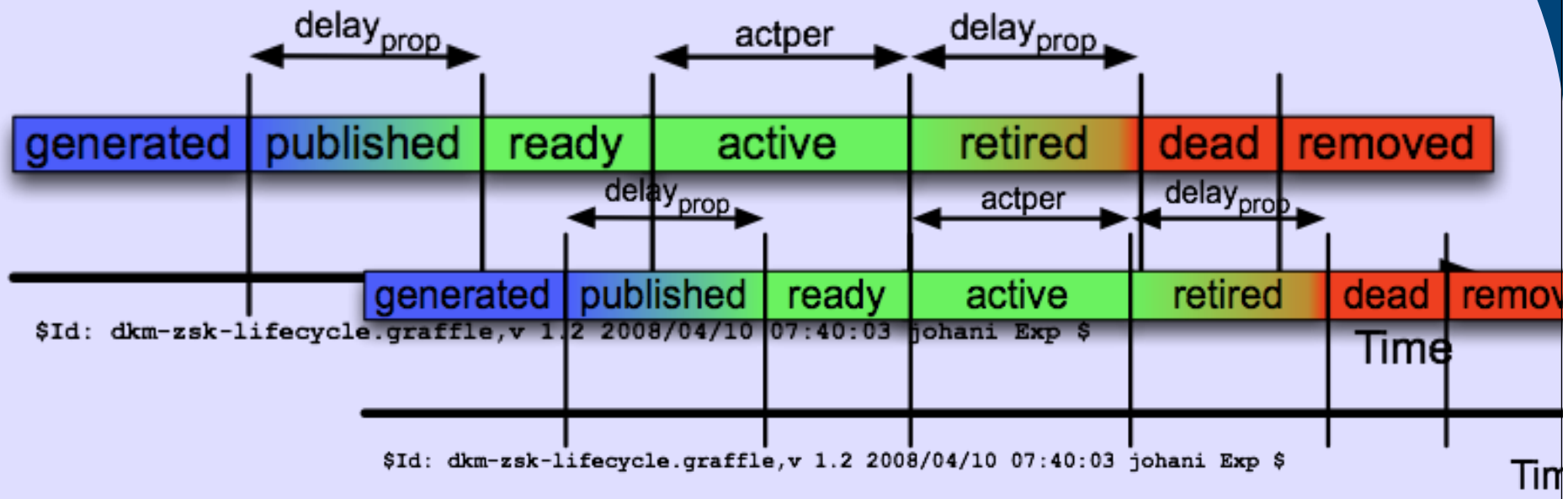
- Well, not really. There are more states:



  - note that this is not to scale, some of these may be measured in minutes, some in weeks

ZSK State Transitions

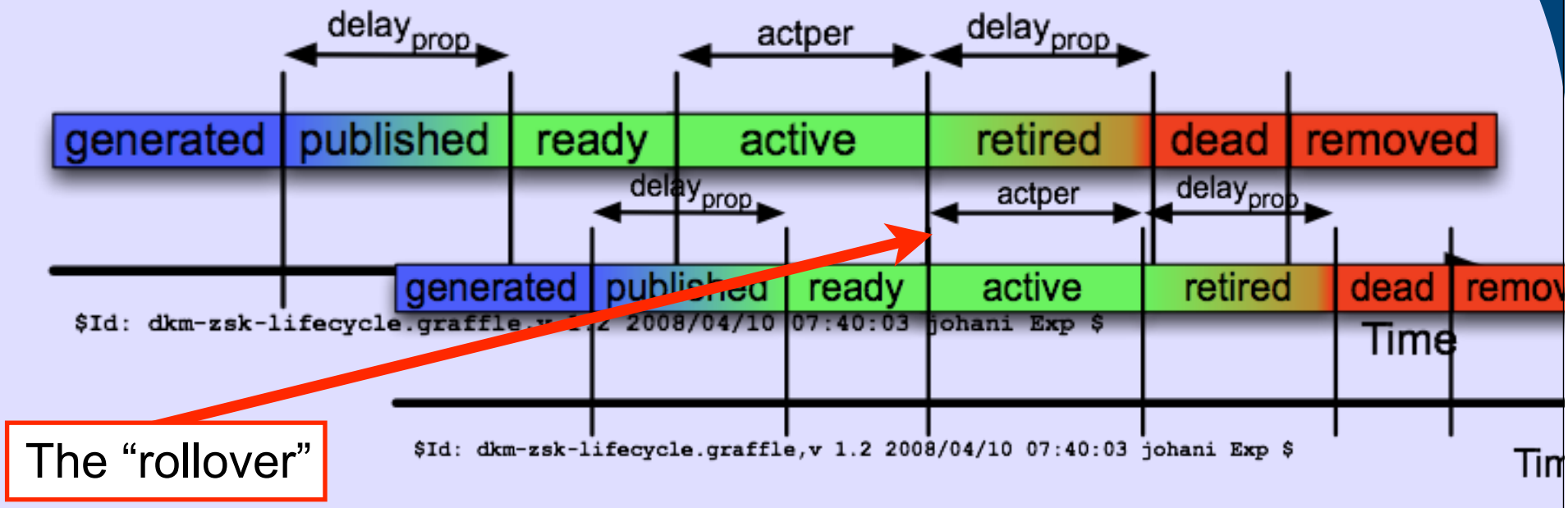
- Well, not really. There are more states:



  - note that this is not to scale, some of these may be measured in minutes, some in weeks

ZSK State Transitions

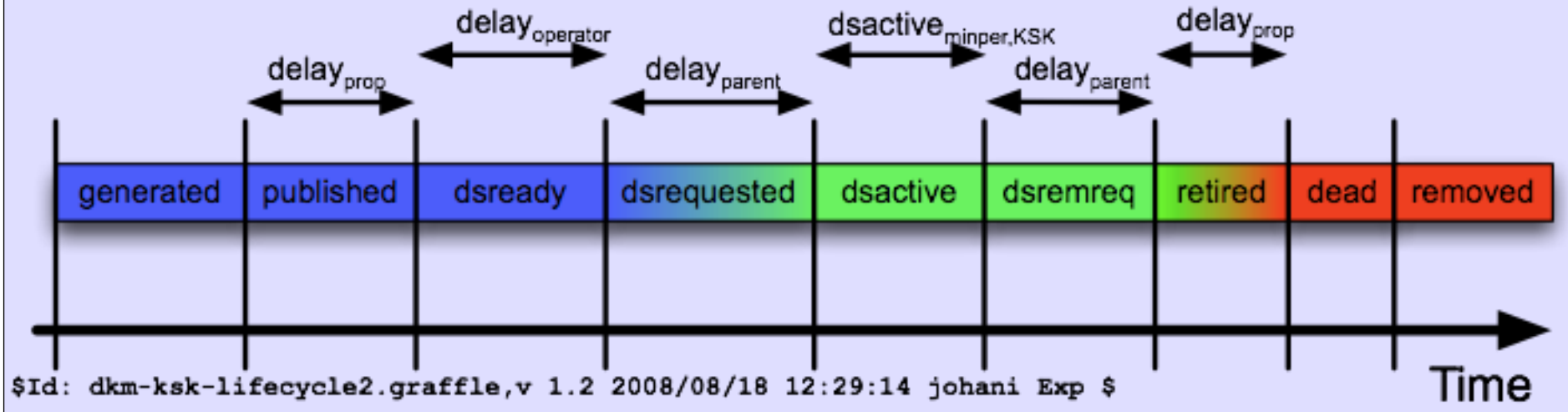
- Well, not really. There are more states:



  - note that this is not to scale, some of these may be measured in minutes, some in weeks

KSK State Transitions

- The KSK is similar:



  - there are a few extra states in the middle to deal with the parent interaction

“Rollover Policy”

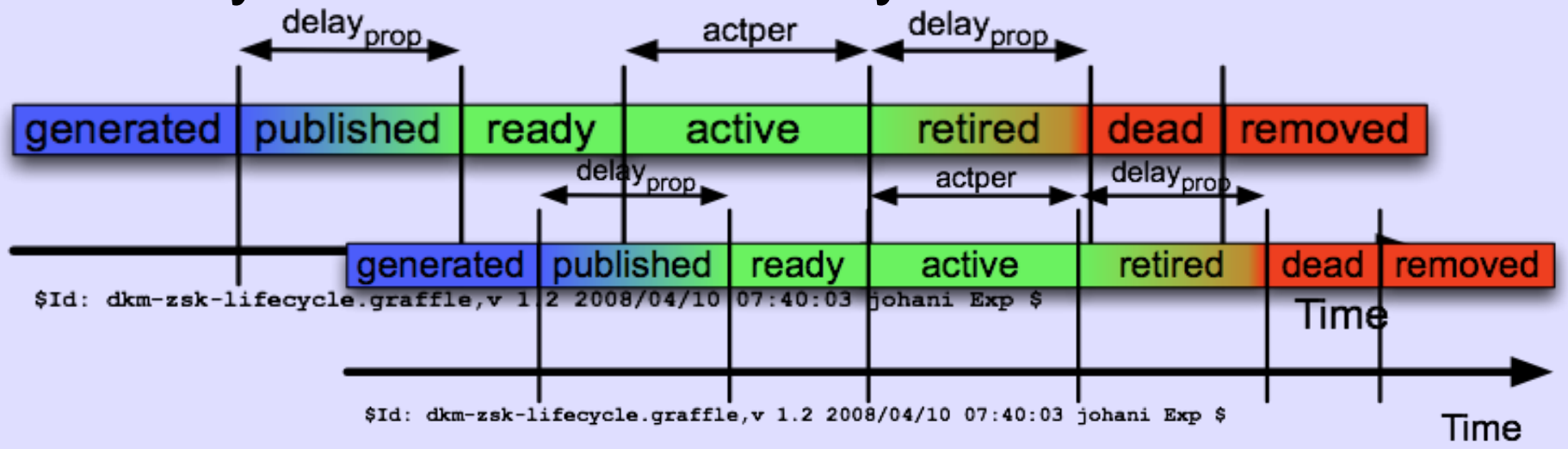
- Policy is needed to encode what is wanted (by the zone owner):
  - “a zone signing key should be active for four weeks”
  - “the propagation delay is 8 days”
  - “there should always be at least one emergency key”
  - etc

“Safe Behaviour”?

- The role of rollover logic is not to ensure that a rollover operation is complete by a particular time
  - far from it
- The logic is there to ensure that no state transition is done until it is “safe” to do so
  - i.e. “policy” is what you **want**, but “logic” is what you **get**. I.e. to be “safe” the policy violation is to be preferred

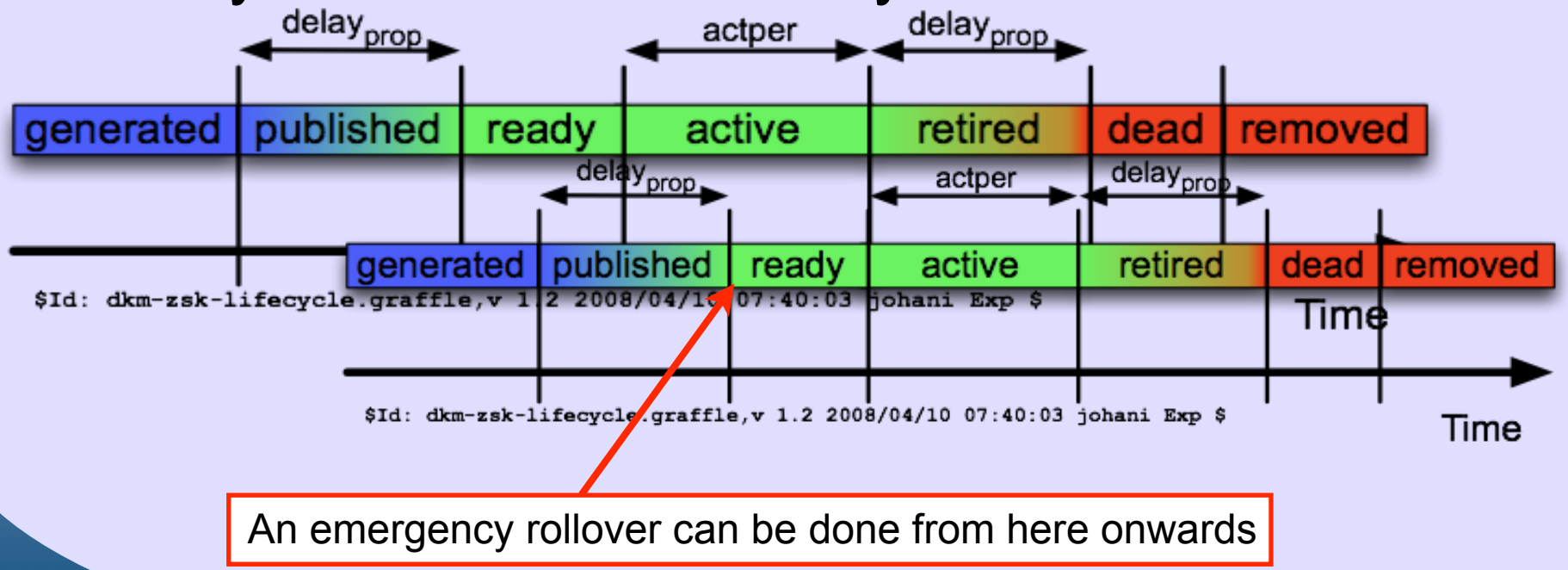
Emergency Rollovers

- We treat emergency rollovers simply as an immediate state transition from the active key to the next active key



Emergency Rollovers

- We treat emergency rollovers simply as an immediate state transition from the active key to the next active key



Emergency Rollovers, cont'd

- This has several consequences for the logic:
  - if the next key isn't "ready" there will be no immediate emergency rollover (because it isn't safe)
  - it is possible to "count backwards" to determine when to publish subsequent keys to ensure that emergency rollover is possible to do immediately
- Note, however, that immediately after an emergency rollover the next key after the new key may not be "ready"
  - so a **policy** for how many immediate emergencies in row to support is needed

Key and Signing Policies

- The present draft only deals with key timing issues and policies
- Signing timing issues and policies are not included
  - because the present draft is complicated enough as it is

Signing Policies?

- Some examples of policy issues for signing:
  - lazy re-signing (only sign as RRSIGs approach their expiration)
    - if so, what signature intervals are reasonable?
  - scheduled resigning (sign on a regular basis, regardless of signature lifetime)
  - signing in a static update (e.g. sign the zone file and reload) or dynamic update environment
  - recommendations for signature "jitter"
  - etc, etc

Next Steps

- We are asking the working group to consider this document as a WG document
- We intend to proceed with the companion document to cover signing issues

Other Questions?

jad@jadickinson.co.uk

johani@autonomica.se

stephen.morris@nominet.org.uk