DNSSEC Key Rollovers
or
Rolling without Falling

Fredrik Palm, Handelsbanken

Johan Ihrén, Autonomica

Handelsbanken

DNSSEC – The end user perspective

Why DNSSEC ?

- Co-operation between four Swedish banks and **.se**.
- Share a common interest in securing Internet based services and information exchanges.

Why develop own tool ?

- Requirements
  - GUI as well as CLI.
  - Transparent handling of one or many domains.
  - Generic key storage (HSM, Smart Card, file system).
  - Split design, i.e. possibility to separate ZSK and KSK related tasks.
  - Delegate daily chores to operators, i.e. simple enough GUI with built in fail-safes.
  - Lucid presentation of key status.
- A quick survey gave that none of the existing tools met our requirements.

A fool with a tool is still a fool

- Key management is a lot more complex than it appears to be.
  - Do not rush things. Let things mature over time.
  - Respect but do not fear the complexities.
  - Keep tabs on what the world is doing.

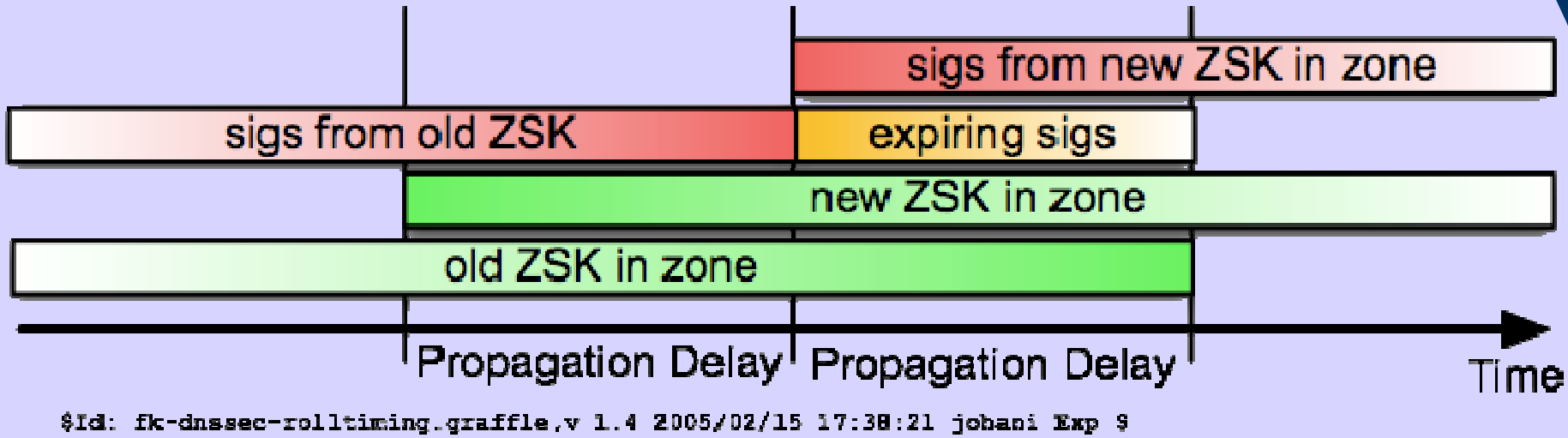
Going into production

- Do your homework. Read up on federal requirements etc.
- Policies and procedures in place
- Training
- Testing
- Gradual implementation

So what is a Key Rollover?

- The ordered replacement of one crypto key with another
  - not particular to DNSSEC, this is a generic issue for systems utilizing crypto keys
  - DNSSEC only makes it slightly more challenging because of the numbers of keys involved
- The no-so-ordered replacement of a key is often called “emergency rollover”

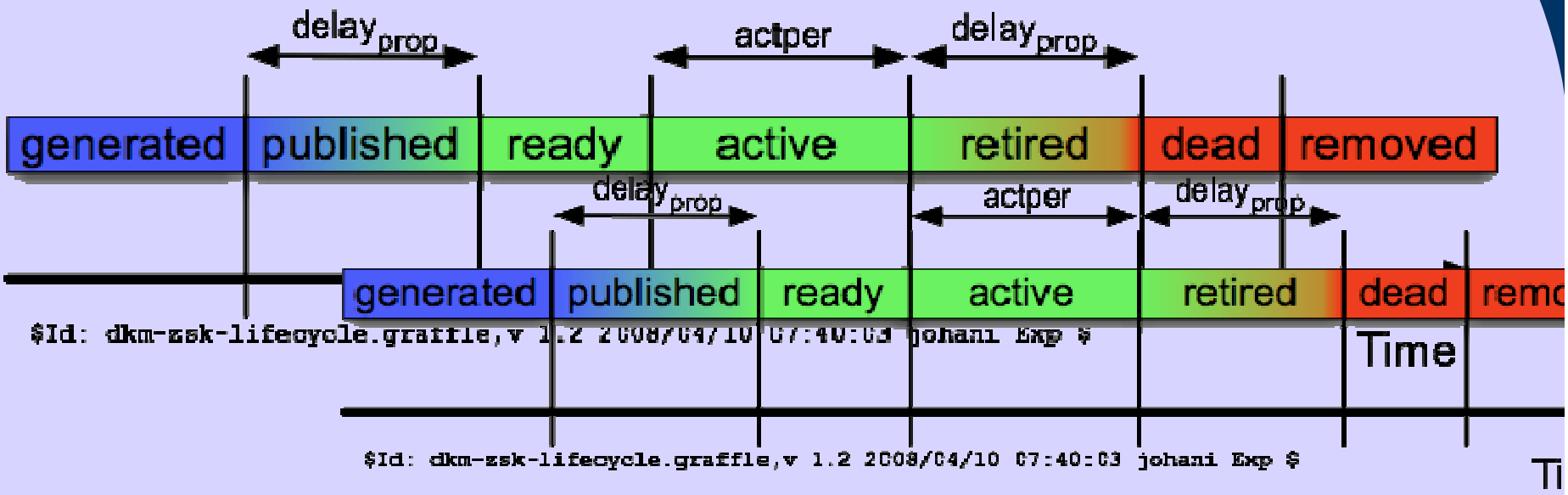
The ZSK Rollover



- But is this all there is to the story?

ZSK State Transitions

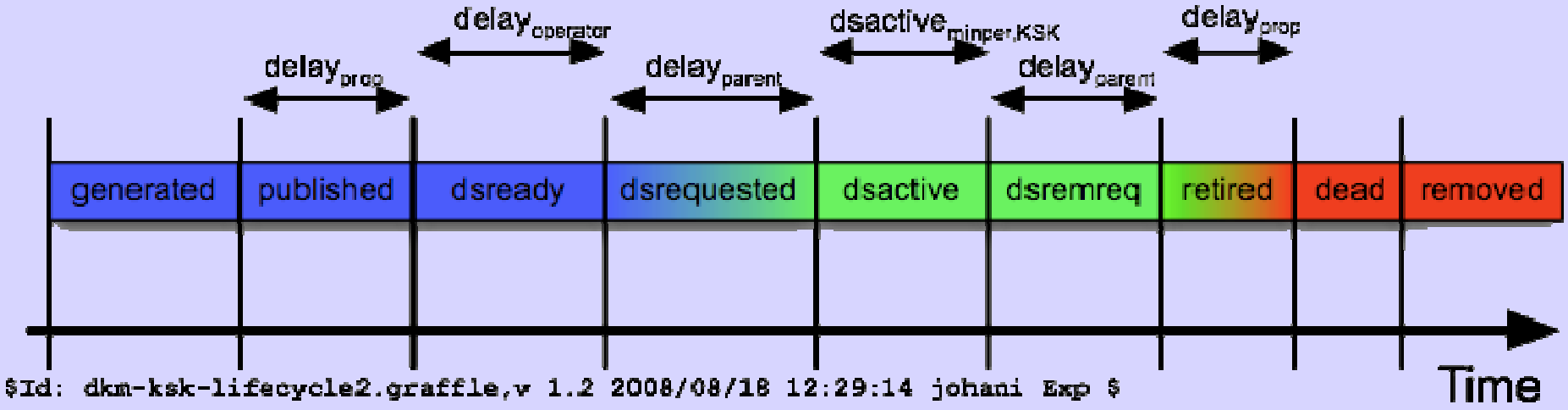
- Well, not really. There are more states:



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

KSK State Transitions

- The KSK is similar:



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

How to deal with this?

- DKM (the system we're presently implementing) does functional separation a la:

DKM = Policy + Logic + Software

  - this is not unique to DKM in any way
- There may be some hardware too
  - although it is an explicit goal to be able to run entirely in software, to make the result more generally useful to others
- It's quite possible that there's more than a little bit of KASP influence in here

“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

“Rollover Logic”

- 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

Comparing Implementations

- Because of the complexity of DNSSEC key rollovers it seems that we will see a plethora of different solutions in the near future
  - that's good
- However, to avoid macedonia ("comparing apples to pears until only mashed fruit remains") it would be good to see
  - at least some agreed upon terminology
  - preferably also state machines
- Such work is presently underway

Remember

- DNSSEC key rollovers may seem complicated today
  - the complexity **will** be hidden by software
  - there are many different systems being developed right now, trying different approaches, and some of them **will** “get it right”
  - in a year or two there will be lots of good options to choose between

Thanks

frpa01@handelsbanken.se

johani@autonomica.se