DNSSEC Key Timing Considerations Follow-Up

draft-mekking-dnsop-dnssec-key-timing-bis

Matthijs Mekking, NLnet Labs

Current State

- Targeted at software developers
- Incomplete
  - Single Type Signing Scheme (STSS)
  - Algorithm Rollover
- Ready for last call, minor surgery allowed
- Major surgery would lead to -bis

Follow-up

- Document is written from scratch
  - Personal analysis
  - Groundwork for the OpenDNSSEC Enforcer NG design
  - Large part taken from the current draft
- Contributing with the editors
- Evolved version of the key-timing document

Major Surgery

- Rollover Considerations
- Key Types
- Key Goals
- Unraveled Key States
- Rollover Centric Logic
- New Rollover Scenarios

Rollover Considerations

- Speed
  - ZSK Double-Signature Rollover
  - KSK Double-RRset Rollover
- Size
  - ZSK Pre-Publication Rollover
- Interactions
  - KSK Double-Signature Rollover

Key Types

- Roles
  - “A key acts as a ZSK and/or KSK.”
  - The two does not rule each other out
- Makes it easier to implement STSS (CSK)

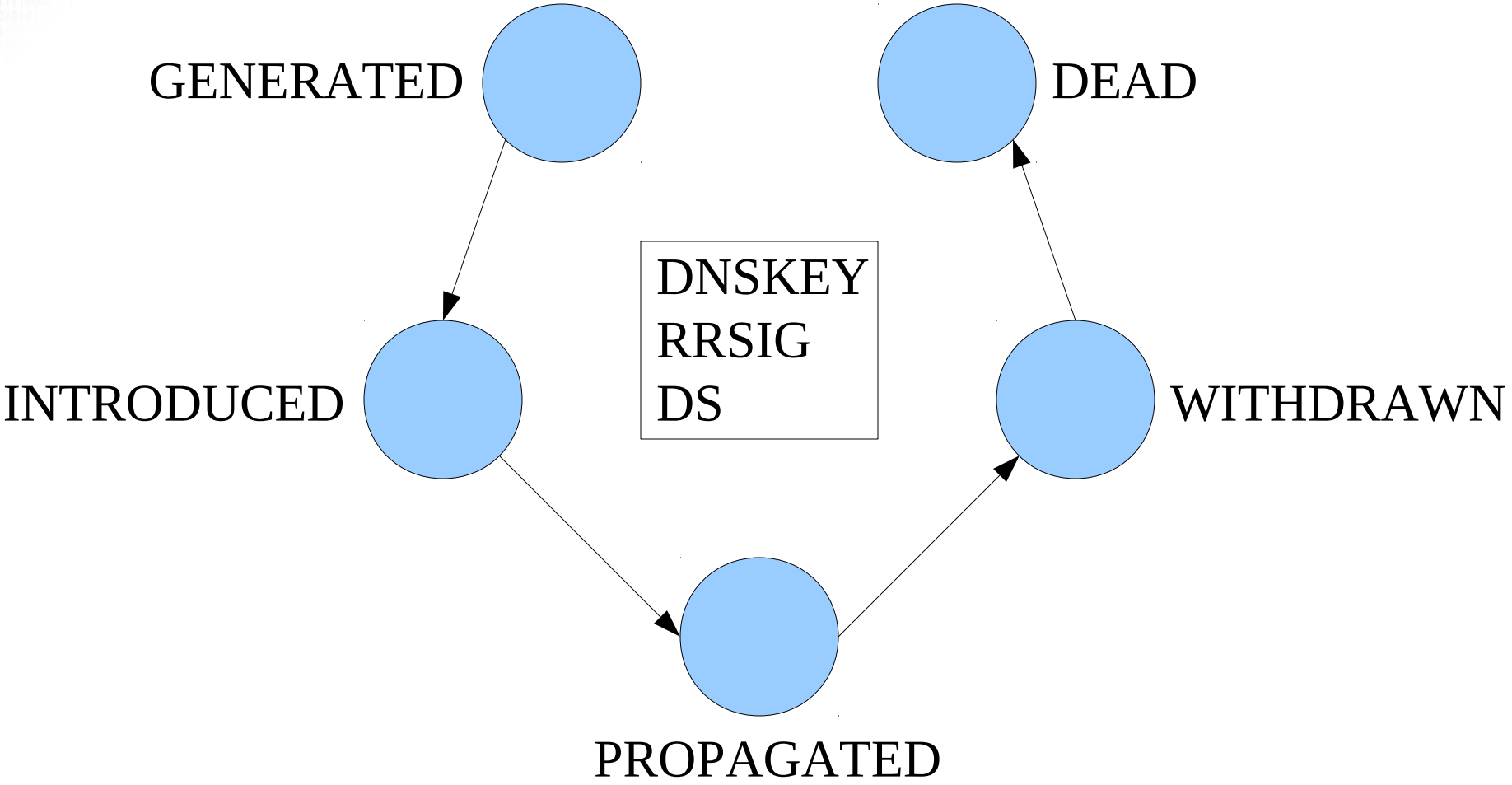
Key Goals

- “A key rollover is defined by setting a goal on a number of keys”
  - Activate key
  - Remove key

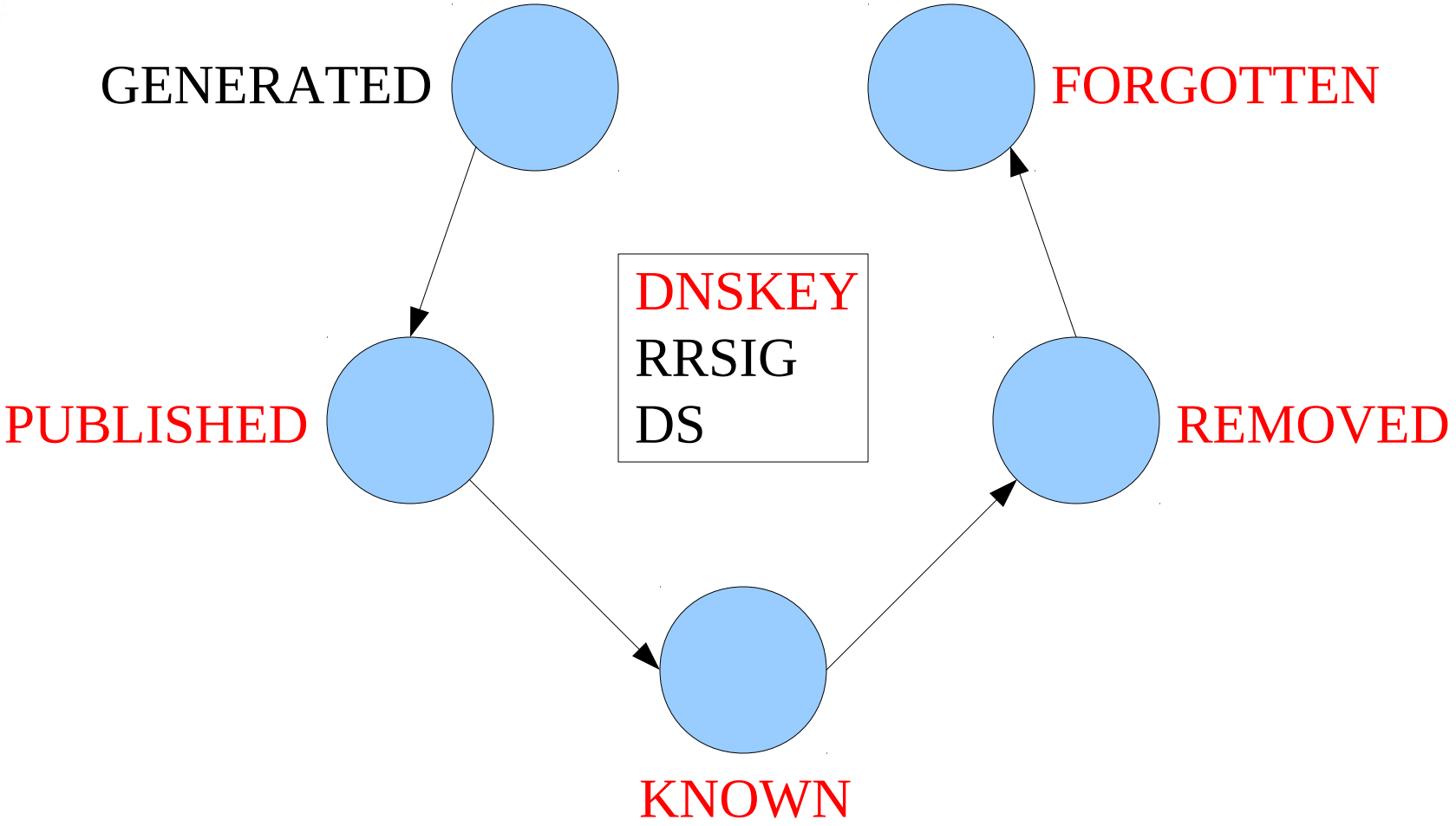
Unraveled Key States

- Key states in current document are overloaded
- Questions:
  - What is the DNS related, associated information of a key?
  - Where is this information available?
- Unravel key states:
  - Identify the pieces of information the state refers to: DNSKEY, RRSIG, DS

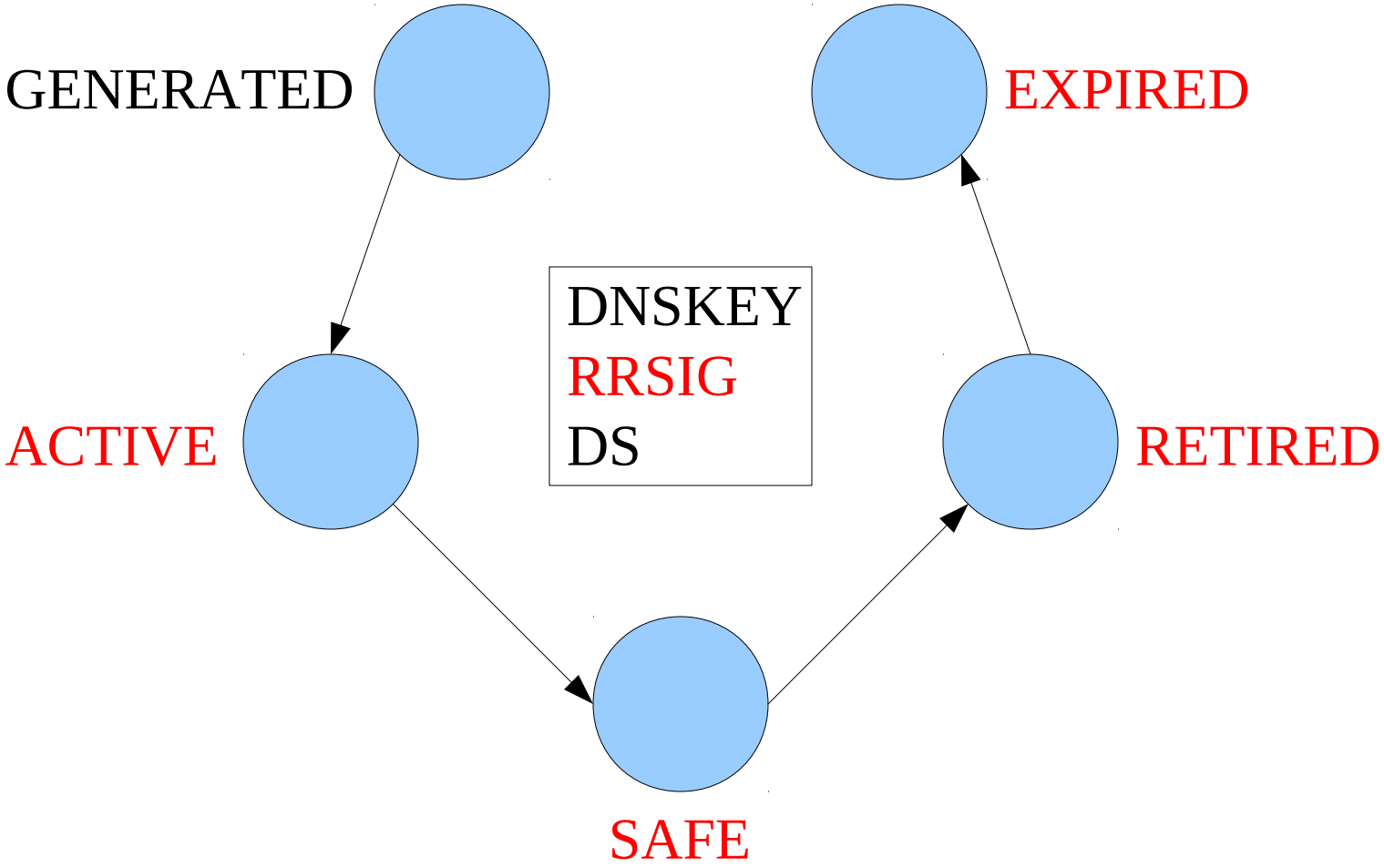
Unraveled Key States



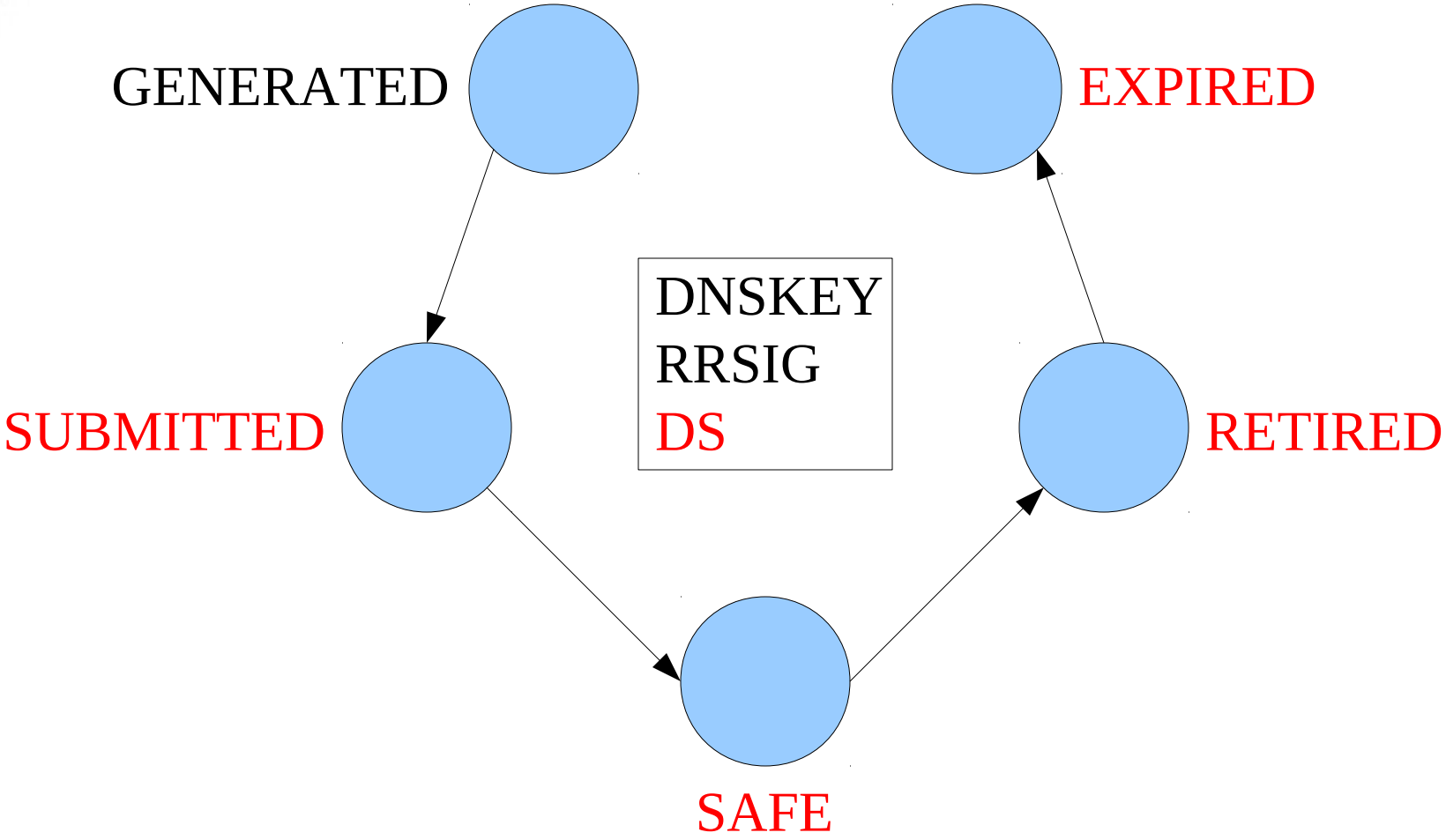
Unraveled Key States



Unraveled Key States



Unraveled Key States



Rollover Centric Logic

- Start with a prerequisite
  - "We have an active key Kc that needs to be replaced by key Ks"
- Set key goals
  - Remove Kc, Activate Ks
- Rollover is complete if goals are met

New Rollovers

- Single Type Signing Scheme (STSS)
  - Combining ZSK Rollovers with KSK Rollovers
- Algorithm Rollover
  - Work in progress (dnsext)
- Policy Rollover (needs more text)
  - Enabling, Disabling DNSSEC
  - From a split to STSS and back again

What's the next step?

- Would this document be a good basis for -bis document?
- Version -01 soonish

draft-mekking-dnsop-dnssec-key-timing-bis