Tracking an Evolving Topic

- When we started work on the Key Timing draft some years ago we thought that we had the subject matter nailed
  - it was just a matter of sorting out all the details of the equations and to get the terminology and descriptions word-smithed
Tracking an Evolving Topic

- When we started work on the Key Timing draft some years ago we thought that we had the subject matter nailed
  - it was just a matter of sorting out all the details of the equations and to get the terminology and descriptions word-smithed
- We were naïve
Tracking an Evolving Topic

- When we started work on the Key Timing draft some years ago we thought that we had the subject matter nailed
  - it was just a matter of sorting out all the details of the equations and to get the terminology and descriptions word-smithed
- We were naïve
- As is quite obvious by now, the number of alternatives are growing in several directions and prior guidance from the WG ("only document, don’t recommend") is becoming an open-ended task
- There is a bit of Xeno’s Paradox ("the Tortoise and the Hare") over our attempts at codifying the underlying math for all methods of rolling DNSSEC keys
Tracking an Evolving Topic, cont’d

- But at the same time the intended audience (software implementors) are quite busily hacking away at real products
  - And frequently they refer to the Key Timing draft
- There is a problem of **timeliness** here, and that does not speak in favour of the Tortoise

- This is of course the reason why we raised the question to the WG about what the best way forward is at this point
  - The response was clearly in favour of “wrapping up” the present document, get it published and move on to the next step
But at the same time the intended audience (software implementors) are quite busily hacking away at real products
  ▶ And frequently they refer to the Key Timing draft

There is a problem of **timeliness** here, and that does not speak in favour of the current editors

This is of course the reason why we raised the question to the WG about what the best way forward is at this point
  ▶ The response was clearly in favour of “wrapping up” the present document, get it published and move on to the next step
    ▶ This is perfectly ok with us and we’re happy to do just that

However, this does leave one question...
Exactly What is The Next Step?

There are several things that would need to go into a possible -bis version of the Key Timing document:

- Things that we already think about:
  - Gradual State Transitions
  - Rollover Centric Logic
  - Treatment of CSK zones (zones that rely on a Common Signing Key, instead of the KSK/ZSK role separation)
  - Algorithm rollovers
Gradual State Transitions

For instance, current logic assumes that a transition from one active key to the next is immediate, but for large zones signing with the new key may be a gradual phase-in that will take some time until all signatures are replaced.
Rollover Centric Logic And Terminology

- The current draft is written from a “Key Centric” perspective. This is in line with how rollover key systems are usually described and have so far not been questioned (by either the editors or others).

- However, we are beginning to find that some things are not really “clear cut” in a system based on keys with atomic state transitions (gradual activation of a key is one example).

- It may be worthwhile to completely change the terminology and rollover logic by switching away from the key centric model.
  - i.e. keys have states and the rollover progresses as a function of the keys changing states to instead be "rollover centric"
  - i.e. the rollover has states, and keys change behaviour and tasks as a function of the rollover changing states
Common Signing Key Rollovers

- The CSK is a glaring example of what can happen when a Tortoise is too slow in progressing the work.
Common Signing Key Rollovers

- The CSK is a glaring example of what can happen when the editors are too slow in progressing the work
- New work is invented for them
Algorithm Rollovers

- This, on the other hand, was known from the outset to be an omission
- While we choose to declare it to be out of scope of the current document it is obvious that it needs “formal treatment” somewhere
Layout Changes

- The current version of the draft has had trouble to find enough reviewers
- Our interpretation of that is that it is due to the current document being quite long and technically complicated
- At the same time it is also clear that there are several distinct “parts” that are of relevance to different audiences
  - A part that contains definitions of terminology, descriptions of all key states (or rollover states) and timing diagrams without all the variables would be of more general interest
  - Another part that goes into the details of every single event for every single method of rollover and every possible choice of zone keys is, perhaps more of a connoisseur item
- By breaking them apart into separate documents the former would be in a better position to reach a larger audience, not only of reviewers, but more importantly in the larger community
Questions to the Working Group

Assuming that the current text, with minor additions (mostly caveats) as instructed by the WG, is more or less ready for WGLC...
Questions to the Working Group

Assuming that the current text, with minor additions (mostly caveats) as instructed by the WG, is more or less ready for WGLC…

1. Should the WG initiate work on a -bis document?
Questions to the Working Group

Assuming that the current text, with minor additions (mostly caveats) as instructed by the WG, is more or less ready for WGLC...

1. Should the WG initiate work on a -bis document?
2. If so, should that start immediately, or should we wait for a while, to gather more experience?