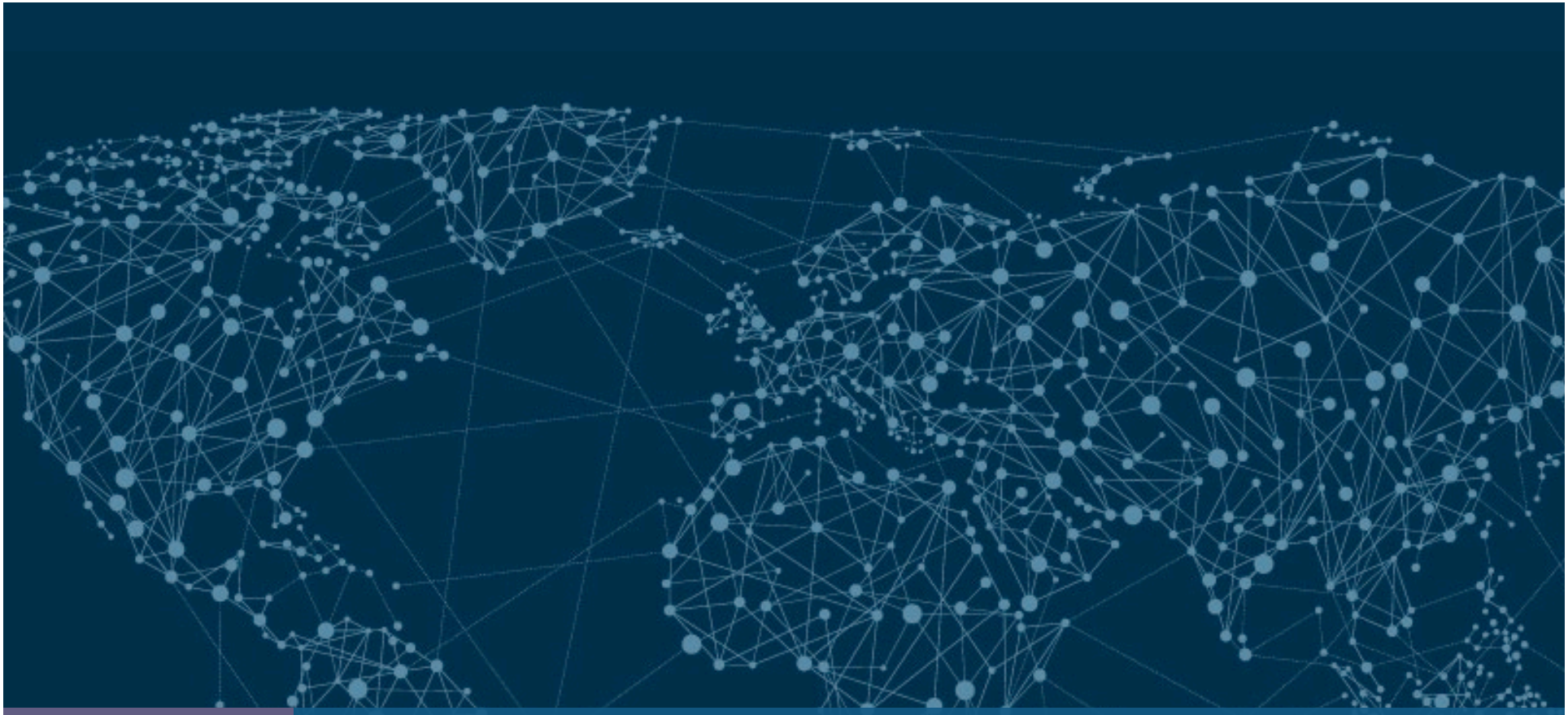


KSK Roll Prepping: RFC 5011

Presented at RIPE 71 DNS WG | November 19, 2015

Intro

- ICANN is preparing to roll the Root Zone KSK
  - ICANN performs the management of the root zone KSK as part of fulfilling the IANA Functions Contract, managed by the US Department of Commerce's National Telecommunications and Information Administration (NTIA); with cooperation from Verisign, the Root Zone Maintainer
- The Root Zone KSK is the DNSSEC trust anchor

Background

- From RIPE 70: *Root Zone KSK Rollover*
  - https://ripe70.ripe.net/archives/video/86/
- A team of seven volunteer experts, along with ICANN, NTIA, and Verisign, are investigating the issues
- Central to the discussions is the buzzword "RFC 5011"

The Volunteers

- The external volunteers are:
  - Joe Abley
  - Jaap Akkerhuis
  - John Dickinson
  - Geoff Huston
  - Ondrej Sury
  - Paul Wouter
  - Yoshiro Yoneya

State of the Plans

- The plan for the roll is not finalized
  - Proposed sets of actions are being analyzed
  - Consensus hasn't been reached quite yet

- But, what is becoming clear is
  - What is said in RFC 5011 will play a big role

Agenda

- What is "RFC 5011?"
- Managing RFC 5011
- Following the "spirit of the protocol"?
- What ICANN will likely do

RFC 5011

- *Automated Updates of DNS Security (DNSSEC)Trust Anchors*
  - Published September 2007
  - Published as STD 74 January 2013

- Full citation
  - StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <http://www.rfc-editor.org/info/rfc5011>.

From 5011's Abstract

This document describes a means for automated, authenticated, and authorized updating of DNSSEC "trust anchors".

…

Based on the trust established by the presence of a current anchor, other anchors may be added at the same place in the hierarchy, and, ultimately, supplant the existing anchor(s).

…

Summary of RFC 5011

- To add a trust anchor
  - Add a new DNSKEY record, sign with all KSK
  - After 30 days of seeing it, assume it's trusted
  - If the DNSKEY disappears, forget it was ever seen
- Once the KSK is trusted it stays trusted until revoked
  - If it goes missing, it is trusted but unusable until it re-appears

Philosophy Behind 5011

- An established trust anchor is used to introduce the next one
- If a candidate appears and there are no "complaints" (removals, denials) for the add hold-down, the trust anchor is good
  - Add hold-down is 30 days

RFC 5011 States

- RFC 5011 describes states of the keys
  - From introduction to removal of the trust anchor
  - The states are the "normative" definition of the process
- Examples
  - Thought to be common use cases

Tool support for RFC 5011

- Various DNS caching resolvers have implemented and tested RFC 5011
  - Consumer side
  - BIND, Unbound, Microsoft, Nominum, etc.
- Some trust anchor operators already follow RFC 5011
  - Producer side
  - No reports of disaster!

So, Why Talk About 5011?

- One area of concern is the manageability of RFC 5011

- The other area of concern is how (or whether) an (consumer) operator chooses to follow RFC 5011
  - Operator of a recursive server

Manageability of RFC 5011

- Designed to have “hands off” configuration of the resolver
  - A break in current model of operating a resolver
  - Some insight is needed to monitor the operations
- It is impossible to tell, remotely, whether a resolver will or has followed an RFC 5011 state change
- RFC 5011 is not designed to be remotely measured

IETF

- Within the IETF there are drafts addressing the lack of remote verification
  - Probably won't be in place for first KSK roll
  - https://datatracker.ietf.org/doc/draft-wessels-edns-key-tag/
  - https://tools.ietf.org/html/draft-wkumari-dnsop-trust-management-01
- Review them, please!

Without Manageability

- It's not possible to remotely know the state of a (consuming) validator's chosen trust anchors
- The trust anchor owners (producers) are limited to publicize the trust anchor changes
- The trust anchor owners can estimate acceptance of the new key, post-event

(Consumer) Operator's Choice

- RFC 5011 "in protocol"
  - Depends on DNS tools to implement RFC 5011
  - Relies on the intended automation

- RFC 5011 "in spirit"
  - Depends on an operator following the state machine of 5011 external to the DNS tools
  - Relies on an operator actively "playing along at home"

Why "5011 in Spirit"

- Centralized Configuration Management
  - Managing a fleet of servers, buzz: virtualization
  - Want to push out a centrally managed, common configuration to servers

- Edge servers not permitted to self-configure
  - 5011 in protocol is not an option

Will This Work?

- Certainly

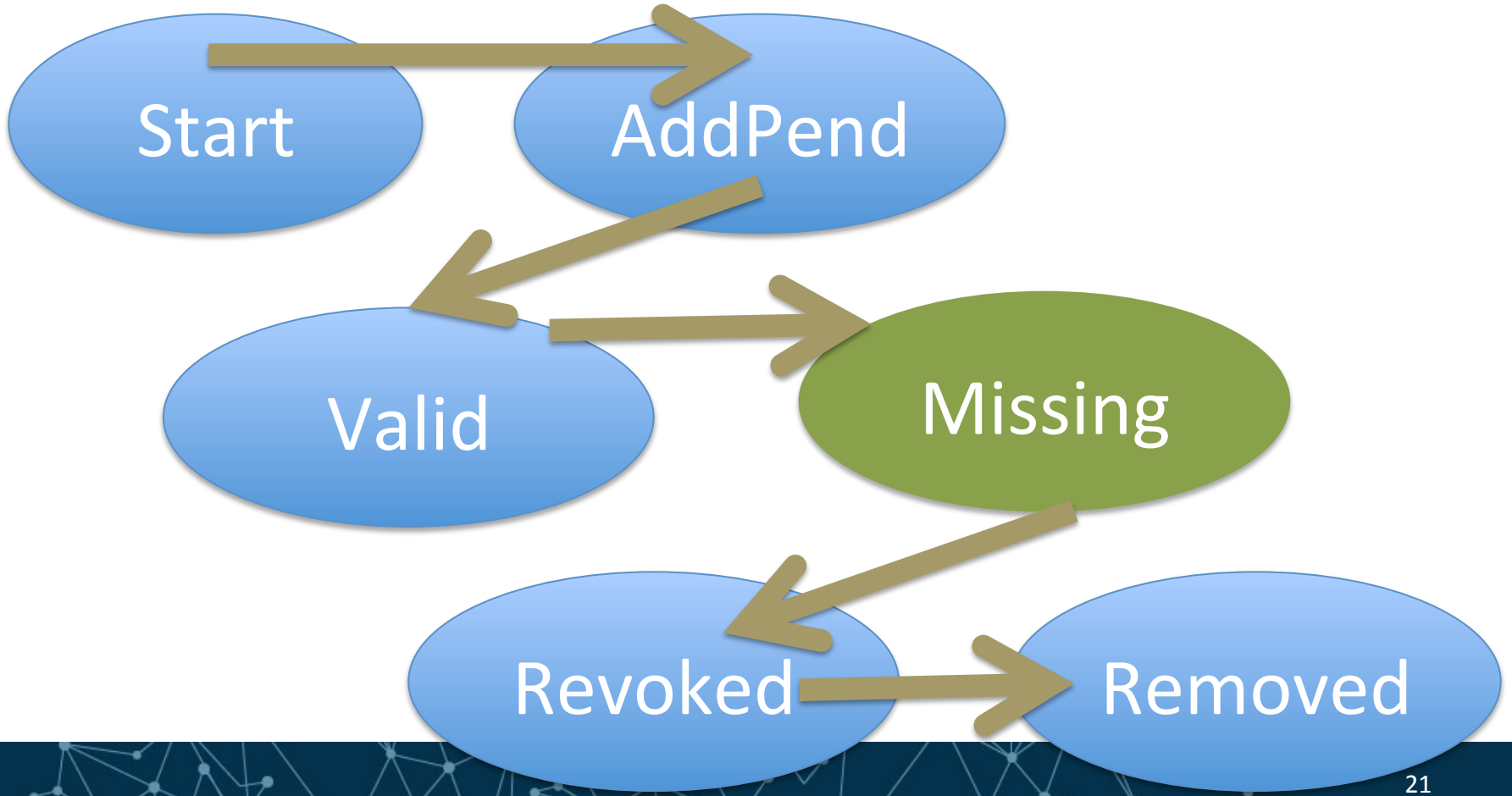
- The (consumer) operator needs to follow the RFC 5011 states as documented

Crucial Elements

- Timing of checks
  - 5011 specifies the frequency a client polls a server for trust anchor states
- Adherence to hold-down timers
  - Pay attention to the add and revoke timers
- Adherence to states
  - When a trust anchor is missing, it's not revoked

How Might ICANN Walk 5011?

- The plan is not final yet, perhaps this:



What's Special?

- Although not the so-called normal path, trust anchors may go "Missing" for a short time
  - To accommodate a scheduled ZSK roll action that would otherwise cause a large-ish response to a DNSKEY request for the root zone keys
  - An effort to limit fragmentation concerns

What else can help operators?

- https://www.iana.org/dnssec/files
- (IETF document in the works to describe)
  - https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor-12

- This has a "snapshot" of trust anchors (including those when missing) for use as a second source

Recommendation for Operators

- Build trust on many different sources
- RFC 5011 in protocol or in spirit is one way
- Find as many means to get the root key that do not share the same fate!
  - What you trust is up to you

What Will Happen?

- Plans are not final yet
- Adhere to RFC 5011's protocol
- Continue to publish new keys outside the DNS following the spirit of RFC 5011
- Publicize the event well in advance, minding preparation time
- Work in concert with impacted parties to avoid trouble tickets

What will help?

- Knowing who needs to be informed
  - Building a contact list of those who "pull the levers"
- Knowing how operators establish trust
  - What third parties are trusted, how many are needed?
- Knowing how to gauge readiness to roll

For more information

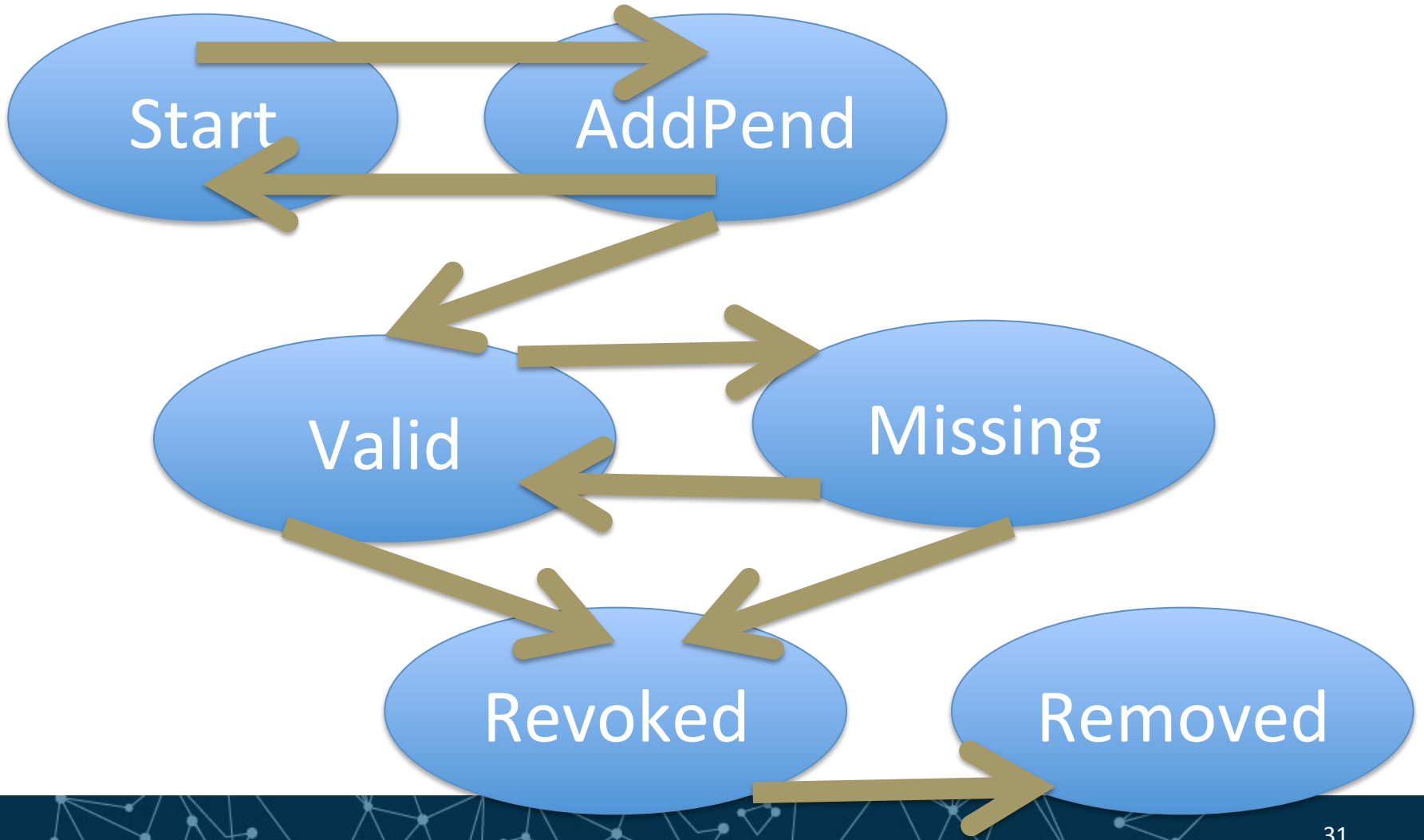
- Join the mailing list
  - https://mm.icann.org/mailman/listinfo/root-dnssec-announce
- Follow on Twitter
  - Hashtag: #KeyRollover
  - Follow @ICANNtech for the most up to date news

Supplemental Slides

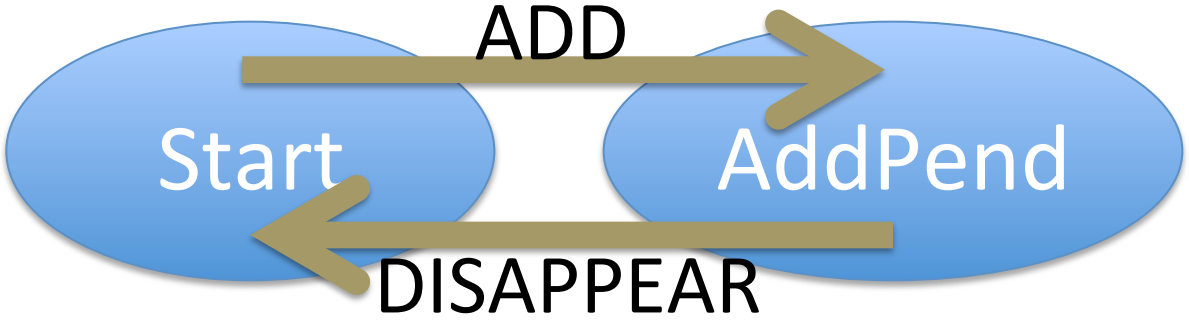
When Will All This Happen?

- Don't know yet.
- "It's complicated."
- But we are preparing for the change.

RFC 5011 State Machine

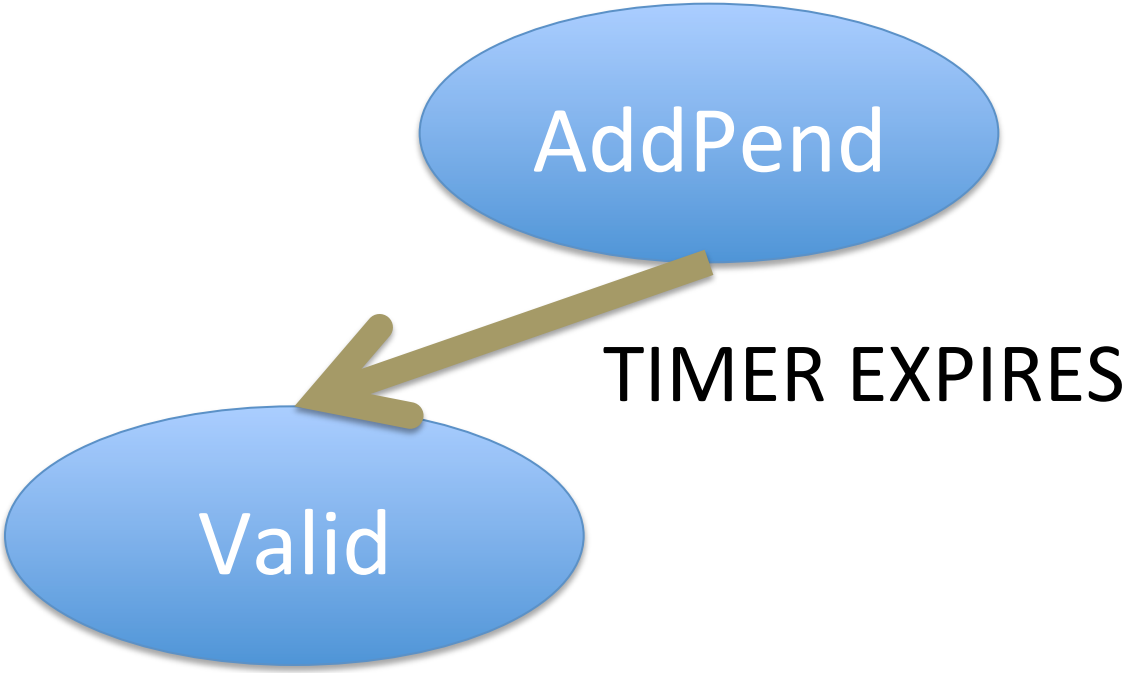


RFC 5011 State Machine (Intro)



- When a candidate appears a timer starts
- If candidate disappears before timer expires
  - Start over
- This timer is the add hold-down timer

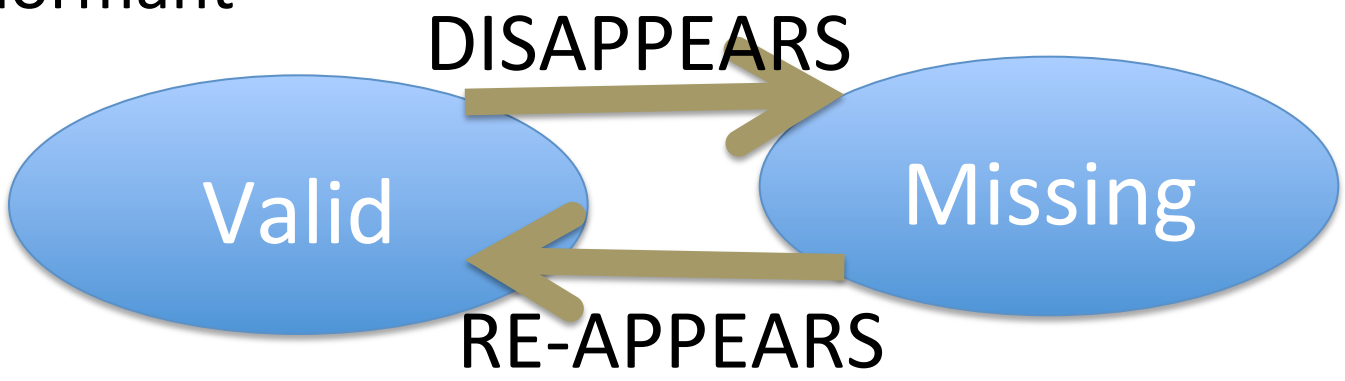
RFC 5011 State Machine (Trust)



- If the timer expires, the candidate becomes a trust anchor

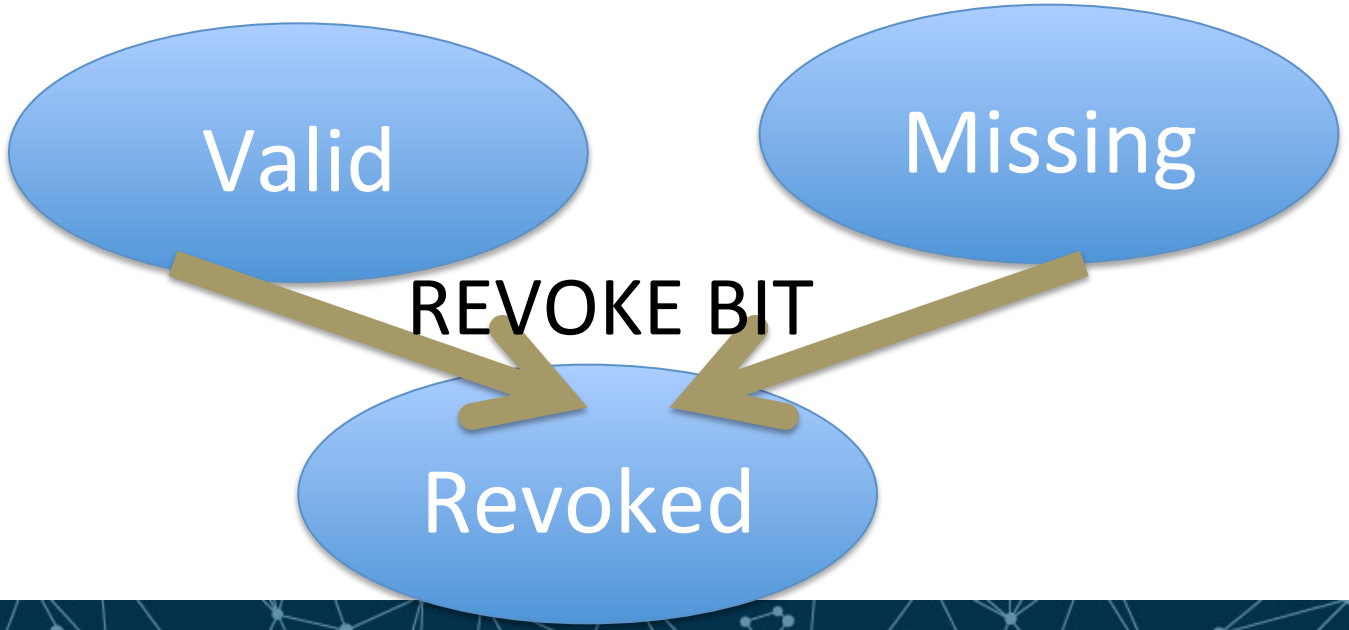
RFC 5011 State Machine (Missing)

- If a trust anchor goes missing from the DNSKEY set, it is simply just missing
  - Not revoked, not invalidated, just sleeping or dormant



RFC 5011 State Machine (Revoke)

- If a trust anchor appears (or reappears) with its revoke bit set (and is signed, etc.) the key moves to a revoked state
  - A timer is started, remove hold-down



RFC 5011 State Machine (Remove)

- When the final timer expires
  - The trust anchor is forgotten