# Testing Resolver Implementations of RFC 5011 for the Root KSK Roll

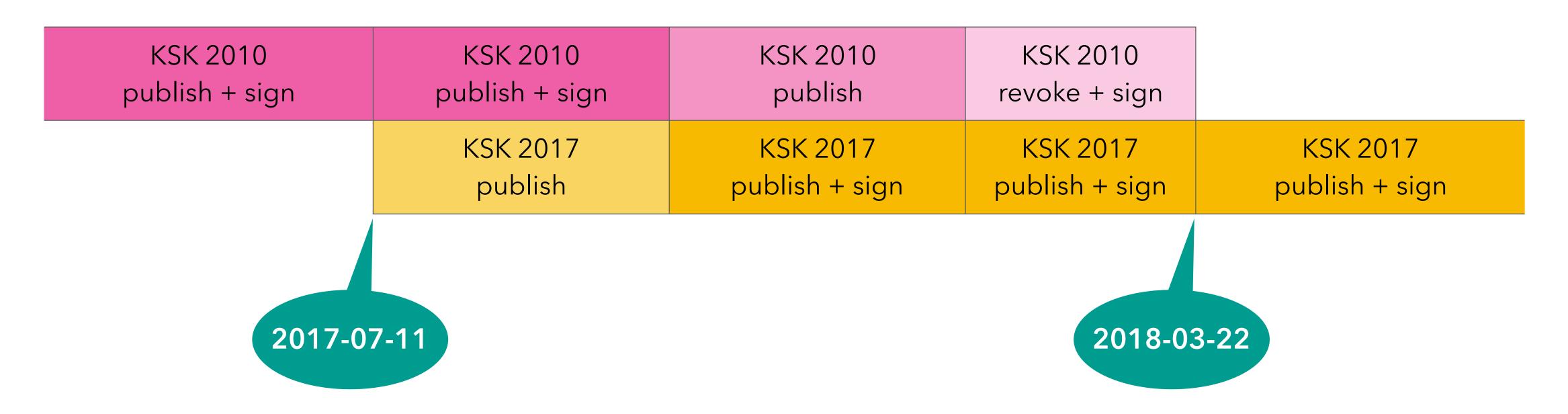
Martin Hoffmann

– OARC 28. San Juan. March 2018. –



### ICANN's (Original) KSK Roll Schedule

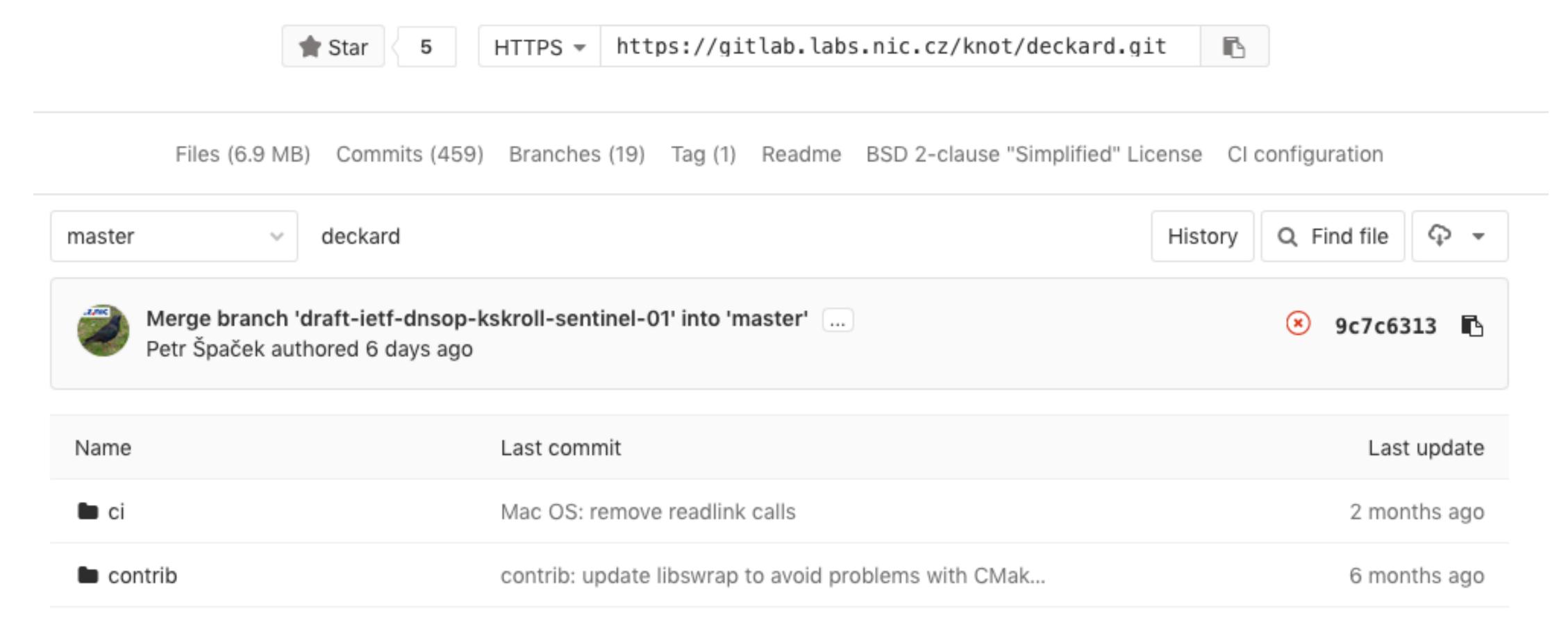
Phase C	Phase D	Phase E	Phase F	
First SKR	Publication	Rollover	Revocation	
2017 Q2	2017 Q3	2017 Q4	2018 Q1	2018 Q2
1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9



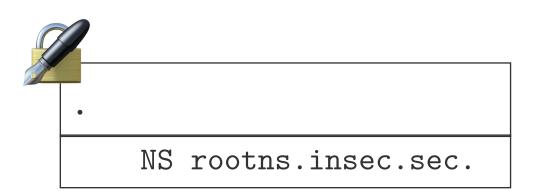


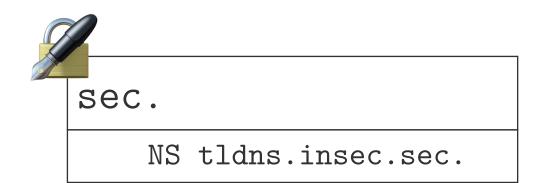
#### deckard @

Test harness for DNS software.



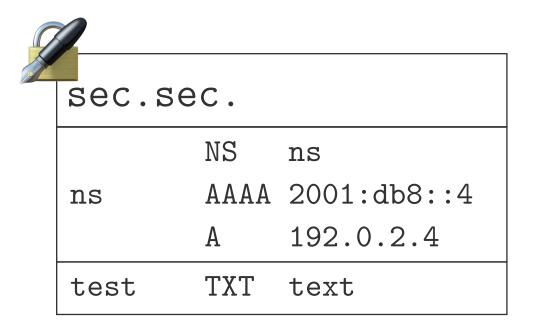
#### The Domain Name System (Complete View)

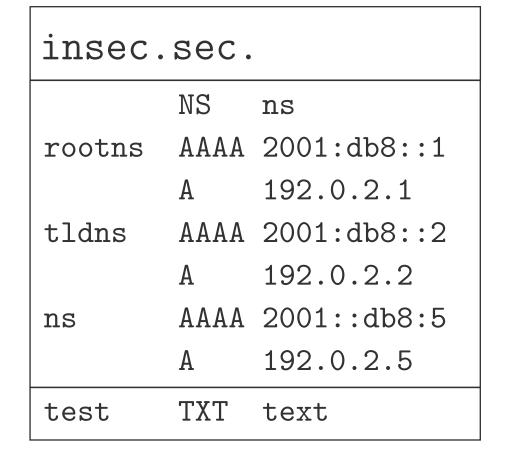


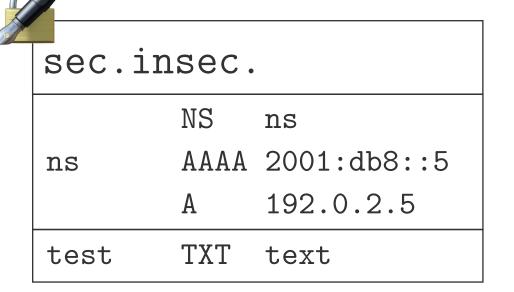


insec.

NS tldns.insec.insec.







sec.insec.		
	NS	ns
tldns	AAAA	2001:db8::3
	A	192.0.2.3
ns	AAAA	2001::db8:7
	A	192.0.2.7
test	TXT	text

#### **Test Scenarios**

- Happy path
- Un-publish before signing
- Roll-back after signing
- Revocation of old key
- Early re-introduction of old key
- Un-revoked old key
- Late re-introduction of old key
- Missing new key
- Non-writeable state directory

- Resolver restarts
- Resolver restarts with non-writable state directory
- Late installation with old key only
- Late installation with both keys
- Post-roll installation with old key only
- Post-roll installation with new key only
- Happy path with forwarding to a non-validating resolver
- Happy path while forwarding to a non-DNSSEC resolver

### Unbound

#### Versions

First production release	1.0.0	2008-05-20
RFC 5011 since	1.4.0	2009-11-26
Latest release	1.6.8	2018-01-19
Current Debian Stable	1.6.0	2016-12-15

# Unbound Findings

Late Installation

- Only trusts the new trust anchor after the 30 days' add hold-down.
- Even if the new trust anchor is provided on installation.
- Fixed in 1.6.5 (2017-08-21).

Re-introduction of Old Key

• accepts the old key after remove and add hold-downs.

# Unbound Operational

RFC 5011 needs to be explicitly enabled

• trust-anchor-file v. auto-trust-anchor-file

Non-writeable state directory

- initially: logs error and carries on until the next restart
- 1.5.4 (2015-07-09): logs error and stops.

### Bind 9

#### Versions

First production release	9.0.0	2000-09-16	
First still usable release*	9.6.2	2010-03-01	* supporting RSASHA256
RFC 5011 since	9.7.0	2010-02-16	
working since*	9.7.1	2010-06-17	* according to our tests
Latest release	9.12.0	2018-01-23	
Current Debian Stable	9.10.3	2015-09-16	

# Bind 9 Findings

Re-introduction of Old Key

- initially: accepts the old key even before the hold-downs have passed
- 9.10.2 (2015-02-25): never accepts revoked key again

Post-roll Installation with Old Key

- initially: resolver goes insecure instead of bogus
- 9.10.4 (2016-04-28): fixed

### Bind 9 Operational

RFC 5011 needs to be explicitly enabled

• trusted-keys v. managed-keys

Non-writeable state directory

initially: • repeatedly logs error and carries on

when restarted after roll: goes insecure

9.8.1 (2011-08-31): • logs error once, carries on

• if kept running until after roll: bogus

### Knot Resolver

#### Versions

First production release	1.0.0	2016-06-21
RFC 5011 since	1.0.0*	
Latest release	2.1.0	2018-02-16
Current Debian Stable	1.2.0	2017-01-25

<sup>\*</sup> in our tests first working in 1.2.0, faulty in 1.2.2, then working again in 1.2.5.

# Knot Resolver Findings

Re-introduction of old key

accepts the old key after remove and add hold-downs

Late installation with old key only

- 1.2.0: accepts the new key during the add hold-down but not after
- 1.2.5: accepts the new key for one day

Revocation of old key

• 1.5.0: accepts the old key for one day after removal from DNSKEY record

# Knot Resolver Operational

Trust anchors are always updated via RFC 5011 🥂

Non-writeable state directory

- initially: stops at start with permission denied
- 1.5.1: same message but keeps running and goes bogus one day late
- 2.0.0: stops at start again

# Knot Resolver Operational

#### Resolver restarts

• 1.2.0: add hold-down restarts with every restart if trust anchor is kept but config directory recreated, otherwise bogus three days after key roll.

• 2.0.0: fixed

### Thank you!

Martin Hoffmann martin@opennetlabs.com

