DNSSEC ROLLING KEYS

Presented by
Olaf Kolkman (NLnet Labs)
and
Alain Aina(TRS)

Rabat, Morocco, 1 June 2008

DNSKEY in flavours

- Zone Signin Key (ZSK)
- Key Signing Key (KSK)
  - Functions as secure entry point into the zone
    - Trust-anchor configuration
    - Parental DS points to it
    - Interaction with 3rd party
- DNSKEYs are treated all the same in the protocol
- Operators can make a distinction
  - Look at the flag field: ODD (257 in practice) means SEP

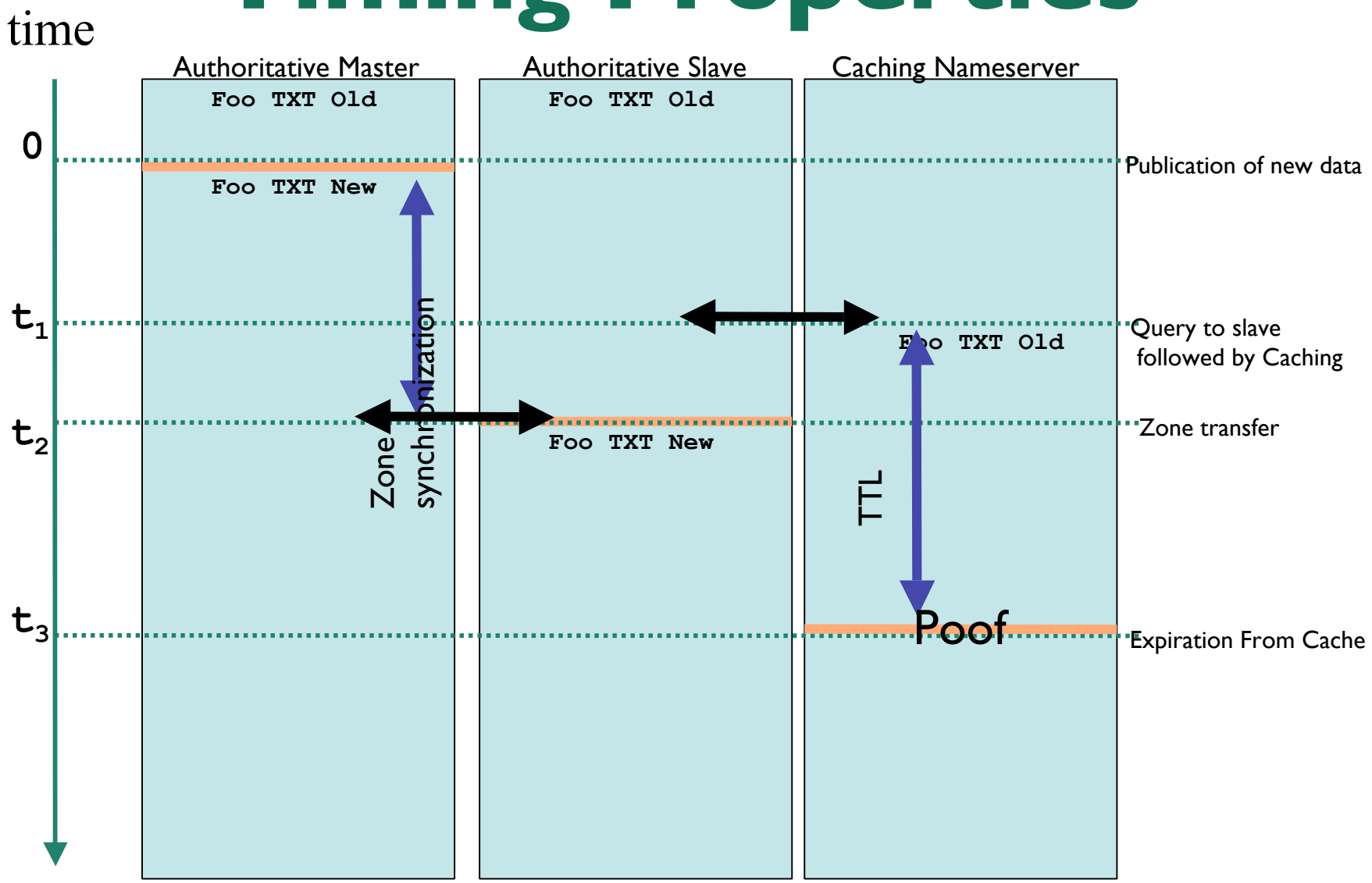
Benefits of using separate keys

- Rolling KSK needs interaction, rolling ZSKs can be done almost instantaneously
- Remember KSK replacement may result in
  - Trust-anchor updates
  - Change of DS record at parent
- Allows different responsibilities
  - ZSKs may be touched day to day by junior staff
  - KSKs may only be touched by senior staff

Rolling keys instantaneously?

- Remember that in the DNS caches are at play.
  - It takes a bit of time to have new information propagate
- When you happen to get new data you would like to be able to use DNSSIGs from the cache
- When you happen to get old data from the cache you would like to use new DNSSIGs
- Try to make sure both old and new keys are available
- Or, try to make sure both old and new sigs are available

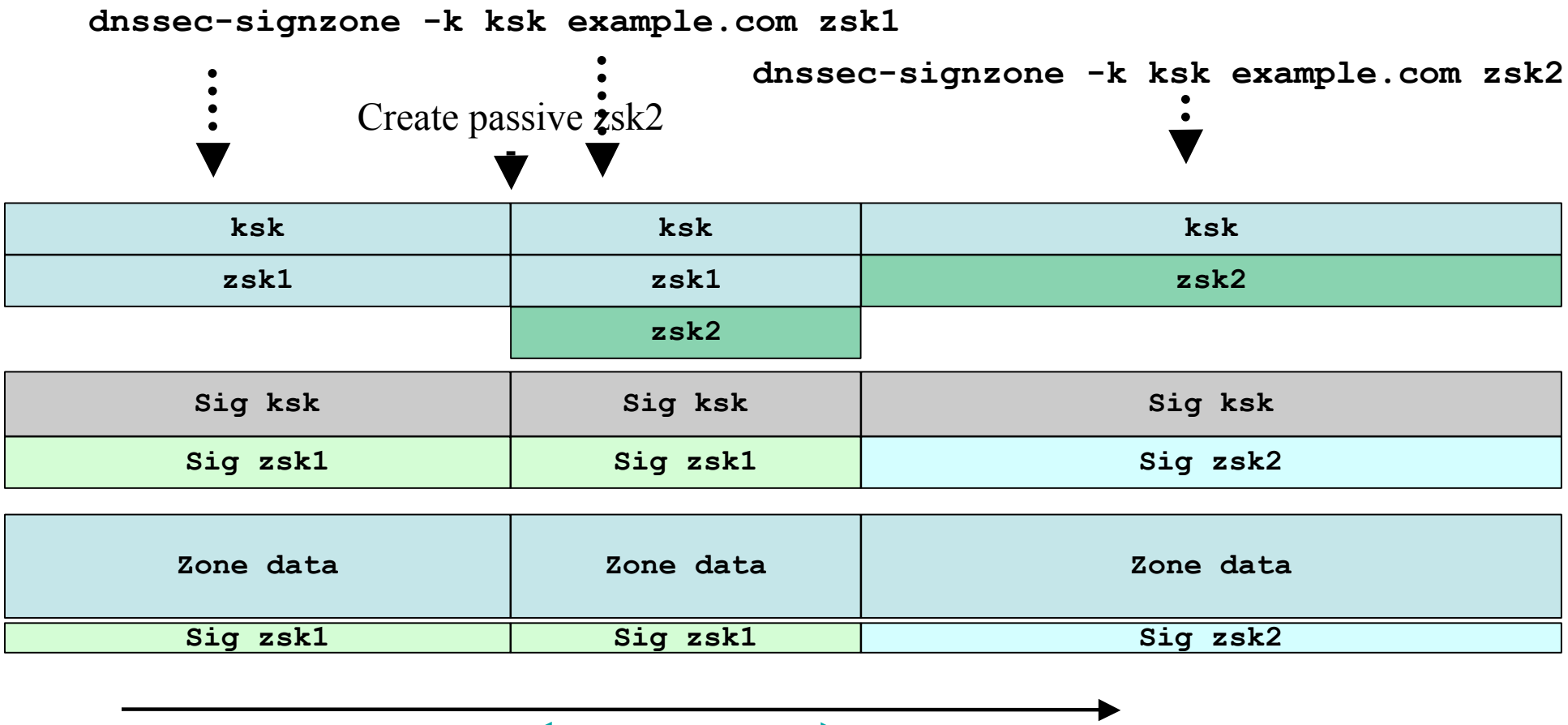
Timing Properties



PRE-publish ZSK rollover

- Introduce the new DNSKEY before you start using it to sign the data.
  - 'passive and active' key
  - The passive key is just published, the active key is used for signing
- You could also create two signatures after introducing the key, but that would cause your zone file to grow

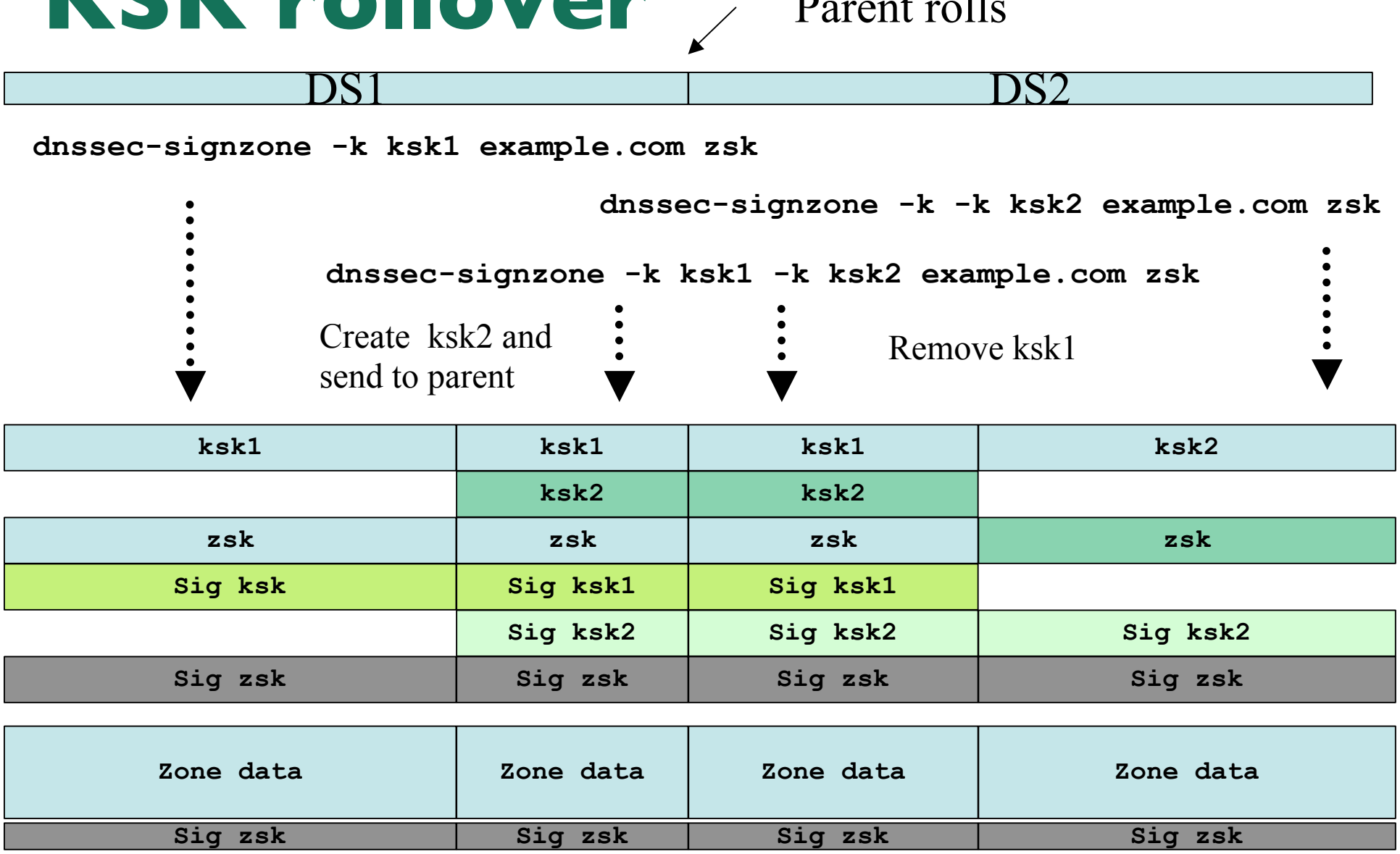
ZSK rollover



KSK rollover

- You are dependent on your parent.
  - You cannot control when the parent changes the DS rr
- Use the old KSK until the old DNS had time to propagate from caches

KSK rollover



Erratum

- RFC4641 contains error in tables
  - Some space is lacking in the tables

initial	new DNSKEY	new RRSIGs	DNSKEY removal
SOA0	SOA1	SOA2	SOA3
RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG11(SOA2)	RRSIG11(SOA3)
DNSKEY1	DNSKEY1	DNSKEY1	DNSKEY1
DNSKEY10	DNSKEY10	DNSKEY10	DNSKEY11
	DNSKEY11	DNSKEY11	
RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1(DNSKEY)	RRSIG1 (DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG11(DNSKEY)	RRSIG11(DNSKEY)

initial	new DNSKEY	DNSKEY removal
SOA0	SOA1	SOA2
RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG11(SOA2)
	RRSIG11(SOA1)	
DNSKEY1	DNSKEY1	DNSKEY1
DNSKEY10	DNSKEY10	DNSKEY11
	DNSKEY11	
RRSIG1(DNSKEY)	RRSIG1(DNSKEY)	RRSIG1(DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG11(DNSKEY)
	RRSIG11(DNSKEY)	

Double Signature Zone Signing Key Rollover