

```
1000010010001011000000101100001000001111100  
1101011001010110100101100110010111100  
100111010111111000111101100011111100  
11111010000111101010010010011111100  
1001010010111000011101000100000100000  
100001111010011110100010111000  
01000101011001011010001000100100  
00011110100110110001111100  
0001010110100011001110001111100  
001011100100101001101100  
010010101100011100000100  
100100101000111110010100  
0111000101111001100  
1101010111101100  
100010100101000100  
0100011100100000  
0111010111100  
111001100000  
0101111000  
001101000  
00101  
00100  
00011
```

DNSSEC ROLLING KEYS

Presented by
Olaf Kolkman (NLnet Labs)
and
Alain Aina(TRS)
Rabat, Morocco, 1 June 2008

<http://www.nlnetlabs.nl/>

Rabat, Morocco, June 1 2008

**NLnet
Labs**

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

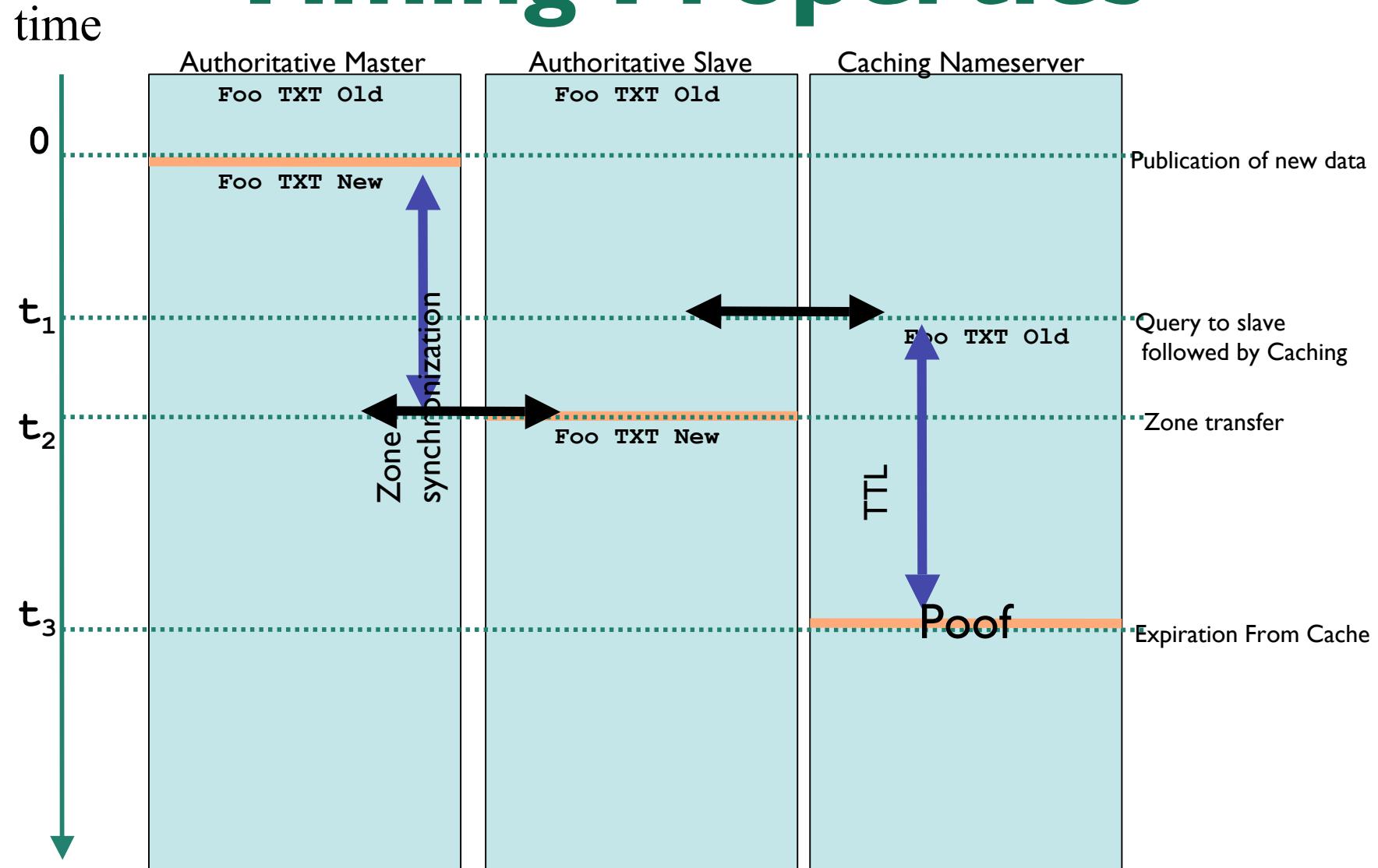
Benefits of using separate keys

- 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

`dnssec-signzone -k ksk example.com zsk1`



`dnssec-signzone -k ksk example.com zsk2`

ksk	ksk	ksk
zsk1	zsk1	zsk2
Sig ksk	Sig ksk	Sig ksk
Sig zsk1	Sig zsk1	Sig zsk2
Zone data	Zone data	Zone data
Sig zsk1	Sig zsk1	Sig zsk2

time



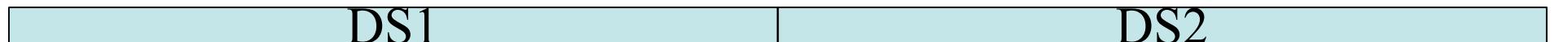
At least TTL DNSKEY RRs
Rabat, Morocco, June 1 2008

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

Parent rolls



`dnssec-signzone -k ksk1 example.com zsk`



`dnssec-signzone -k -k ksk2 example.com zsk`

`dnssec-signzone -k ksk1 -k ksk2 example.com zsk`

Create ksk2 and
send to parent



Remove ksk1



ksk1	ksk1	ksk1	ksk2
	ksk2	ksk2	
zsk	zsk	zsk	zsk
Sig ksk	Sig ksk1	Sig ksk1	
	Sig ksk2	Sig ksk2	Sig ksk2
Sig zsk	Sig zsk	Sig zsk	Sig zsk

Zone data	Zone data	Zone data	Zone data
Sig zsk	Sig zsk	Sig zsk	Sig zsk

time



At least TTL DS RRs

Rabat, Morocco, June 1 2008

Erratum

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

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

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

Double Signature Zone Signing Key Rollover

