



DNSSEC Key Timing Considerations

`draft-ietf-dnsop-dnssec-key-timing-01.txt`

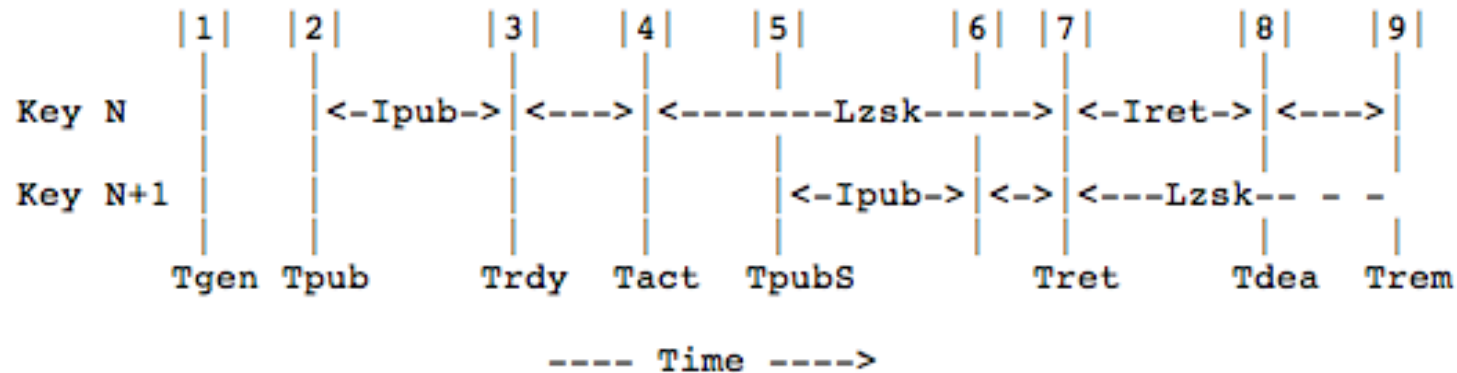
.se

Rollover mechanisms

ZSK Method	KSK Method	Description
Pre-Publication	(not applicable)	Publish the DNSKEY before the RRSIG.
Double-Signature	Double-Signature	Publish the DNSKEY and RRSIG at same time. (For a KSK, this happens before the DS is published.)
Double-RRSIG	(not applicable)	Publish RRSIG before the DNSKEY.
(not applicable)	Double-DS	Publish DS before the DNSKEY.
(not applicable)	Double-RRset	Publish DNSKEY and DS in parallel.

.se

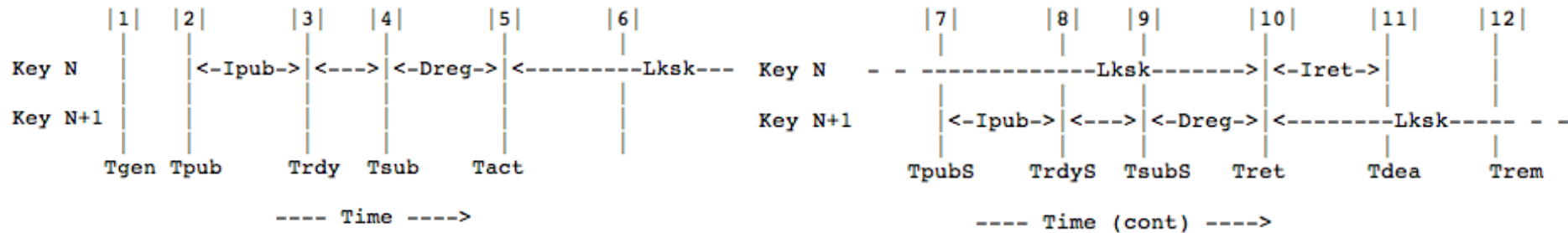
Pre-Publication ZSK rollover



- First key: $I_{pub} = D_{prp} + \min(TTL_{soa}, SOA_{min})$
- Future keys: $I_{pub} = D_{prp} + TTL_{key}$
- $T_{pubS} \leq T_{act} + L_{zsk} - I_{pub}$
- $I_{ret} = \min(D_{sgn} + D_{prp} + TTL_{sig}, L_{sig} + D_{skw})$

.se

Double-Signature KSK rollover



- $I_{pub} = D_{prp} + TTL_{key}$
- $T_{pubS} \leq T_{act} + L_{ksk} - D_{reg} - I_{pub}$
- $I_{ret} = D_{prpP} + TTL_{ds}$

.se