

DNSSEC Implementation

1) If we take akamai.com

- there are basically 3 major steps which have to be done in each zone.

a) '.' (root zone)

i) Have to verify the RRSig of the DNSKEY-RRSET with the KSK of this zone which is present in DNSKEY-RRSET.

(ii) Have to verify the RRSig of the DS-Record RRSET with the ZSK of this zone which is present in the DNSKEY RRSET.

(iii) Have to verify the hash of KSK present in the previous/parent domain to the public key KSK present in DNSKEY-RRSET of this domain.
(have to generate hash of this key & compare it with parent hash)

b) 'com.' (next sub-domain)

- all the three steps have to be formed here also.

c) 'akamai.com.' (last zone)

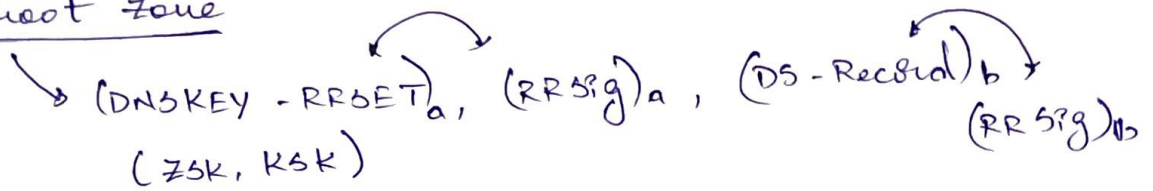
- all the three steps have to be formed here also

i) The only difference here is we have to verify RRSig of A-record instead of RRSig of DS-record

Exp 2

akamai.com

1) '.' root zone

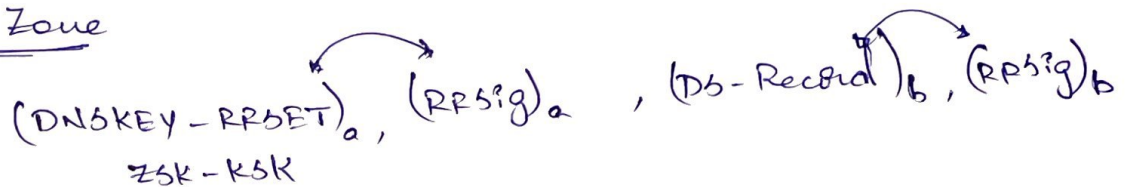


a) $(\text{RRSig})_a \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{KSK}}$

b) $(\text{RRSig})_b \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{ZSK}}$

c) Verify KSK using public key (from IANA)
 $(\text{DS-Record})_b$ - will consist of KSK hash (Next domain)

2) 'com.' zone

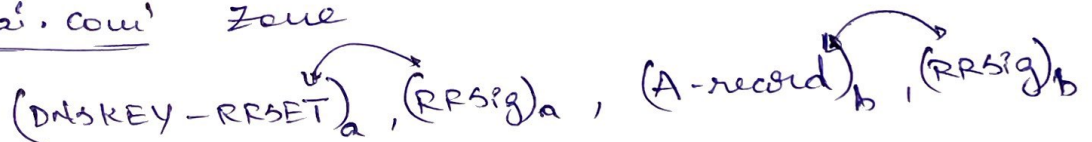


a) $(\text{RRSig})_a \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{KSK}}$

b) $(\text{RRSig})_b \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{ZSK}}$

c) $(\text{KSK}) \rightarrow \text{Hash} \longleftrightarrow \text{Verify with the same.}$

3) 'akamai.com' zone



a) $(\text{RRSig})_a \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{KSK}}$

b) $(\text{RRSig})_b \longleftrightarrow (\text{DNSKEY-RRSET})_{\text{ZSK}}$

c) Verify KSK hash \longleftrightarrow previous DS-Record has KSK hash.