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 (public key) of this Zone which is present in DNSKEY-RRSET.

(ii) Have to Verify the RRSig of the DS-Record RRSET with the ZSK (public key) 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 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

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

Exp: akamai.com

1) '.' root zone

→ (DNSKEY - RRSET)$_a$, (RRSig)$_a$, (DS - Record)$_b$, (RRSig)$_b$
(ZSK, KSK)

a) (RRSig)$_a$ ⟷ (DNSKEY - RRSET)$_{KSK}$

b) (RRSig)$_b$ ⟷ (DNSKEY - RRSET)$_{ZSK}$

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

2) 'com.' Zone

(DNSKEY - RRSET)$_a$, (RRSig)$_a$, (DS - Record)$_b$, (RRSig)$_b$
ZSK - KSK

a) (RRSig)$_a$ ⟷ (DNSKEY - RRSET)$_{KSK}$

b) (RRSig)$_b$ ⟷ (DNSKEY - RRSET)$_{ZSK}$

c) (KSK) → Hash ⟷ Verify with the same.

3) 'akamai.com' Zone

(DNSKEY - RRSET)$_a$, (RRSig)$_a$, (A-record)$_b$, (RRSig)$_b$

a) (RRSig)$_a$ ⟷ (DNSKEY - RRSET)$_{KSK}$

b) (RRSig)$_b$ ⟷ (DNSKEY - RRSET)$_{ZSK}$

c) Verify KSK hash ⟷ previous DS-Record has KSK hash.