DNSSEC IMPLEMENTATION DETAILS

Terminology:

Public ksk : The servers key signing key, used to sign the dnskey record
Public zsk : The servers zone signing key, used to sign the records other than dnskey record
DS record : The fingerprint of public ksk of child zone
RRset : The set of records of any type like A, AAAA, NS, DS, DNSKEY, MX
RRsig : The hash of RRset , the hash is done using public zsk , but for DNSKEY it is done using public ksk

Note: we already know the DS fingerprint of public ksk of root server. (it is present on the ICANN site)
For a domain name, first query the dns parent server using tcp to get the dns key record of the parent server. Also query for the ip of the current domain, get the public ksk from that dns keyrecord and make fingerprint of that key and compare it to the already present DS record of the parent server, if it does not match terminate the program.otherwise , validate the dnskey record using public ksk retrieved from the parent server.

Now from the authority section get the ds record of the child zone and validate it using public zsk of current server against rrsig from authority section, if does not match terminate the program, else populate child server and save this ds record

Repeat the above process for the child servers, to establish a chain of trust from the root server to the authoritative dns server of the domain in consideration. If trust fails anytime before authoritative of domain in consideration, terminate the program.

When we reach the authoritative server and query it for the domain, it gives A record of the domain and also rrsig of the domain, verify the A records using public zsk against the rrsig. If validation fails, terminate the program else return A records.