DNSSEC Implementation - Java

If DNSSEC is not Enabled (boolean) output: "DNSSEC not supported" else perform the following :

When we send a message to the root server using the SimpleResolver, along with ANSWER, AUTHORITY and ADDITIONAL sections we also get the RRSets which is basically a group of records of the same type. We do the following for each set :

- Obtain the RRSIGs using rrSet.sigs() which returns an Iterator with RRSIGRecords.
- Obtain the owner and KeyID(footprint) for each of the signatureRecord using record.getSigner() and record.getFootprint() respectively.
- Create another SimpleResolver to obtain the DNSKey as follows:
    1. Set the EDNS of the resolver:
       resolver.setEDNS(0, 0, ExtendedFlags.DO, null);
    2. Create a Record with Name:owner and Type:Type.DNSKEY
    3. Create a Message with Message.newQuery(r) with the record created above.
    4. Send this message using the resolver to obtain the RRSets again in the response.
    5. Loop through each RRSet, get the data records of each using rec.rrs() which returns an Iterator of DNSKEYRecords.
    6. Loop through each of the DNSKeyRecords and check if the footprint matches with parent KeyID. If yes, the keyRecord(DNSKey) is obtained.
- Verification with KSK:
    1. We have obtained data records of each RRset already, now we have to obtain the signatures on each using rr.sigs()
    2. If the current signature's footprint matches with the KeyID, then verify using DNSSEC.verify(rec, currentSigRecord, keyRec) where rec - (child)current RRSet, (child)currentSignature and keyRec is DNSKey obtained above.
    3. If an exception is thrown, output : "DNSSEC is configured but the digital signature could NOT be verified" then Verification Failed using KSK
    4. Else verified with KSK .
- Verification with ZSK:

1. Once the verification is successful with KSK, we perform DNSSEC.verify(rrSet, record, keyRec) where rrSet is parent RRSet, record is parent signature and keyRec is DNSKey obtained above.
2. If an exception is thrown, output "DNSSEC is configured but the digital signature could NOT be verified" and Verification Failed.
3. Else verified with ZSK.

- If both of them are verified successfully, output: "DNSSEC is configured and everything is verified"