DNSKEY Resource Records

When an authoritative name server digitally signs a zone, it typically generates two key pairs, a zone-signing key (ZSK) pair and a key-signing key (KSK) pair. The name server uses the private key of the ZSK pair to sign each RRset in a zone. (An RRset is a group of resource records that are of the same owner, class, and type.) It stores the public key of the ZSK pair in a DNSKEY record. The name server then uses the private key of the KSK pair to sign all DNSKEY records, including its own, and stores the corresponding public key in another DNSKEY record. As a result, a zone typically has two DNSKEY records; a DNSKEY record that holds the public key of the ZSK pair, and another DNSKEY record for the public key of the KSK pair.

Note: For the remainder of this chapter, the DNSKEY record that holds the public key of the ZSK pair is referred to as the ZSK and the DNSKEY record that holds the public key of the KSK is referred to as the KSK.

The purpose of the KSK is two-fold. First, it is referenced in the Delegation Signer (DS) RR that is stored in a parent zone. The DS record is used to authenticate the KSK of the child zone, so a resolver can establish a chain of trust from the parent zone to its child zone. (For more information about the DS RR, see DS Resource Records.)

Second, if a zone does not have a chain of trust from a parent zone, security aware resolvers can configure the KSK as a trust anchor; that is, the starting point from which it can build a chain of trust from that zone to its child zones.

Note that though the two key pairs, KSK and ZSK, are used in most DNSSEC environments, their use is not required by the RFCs. A zone administrator can use a single private/public key pair to sign all zone data. (Note that Infoblox appliances require two key pairs.)

Following is an example of a DNSKEY RR:

```
.corpxz.com 1296000 IN DNSKEY 257 3 5 20131231235939hiZso1gPtqlKeVuG6bAchP8dq
4vSmxSxzBsqzueQWdJ7yGCBsOdB77Y95zkdrAcPnx
ZBwvQMOgE07dxa0PeTwpqDvp6EOY2LwWBinmv
17XhOjjarzM6mT1P1J+4ax1KrqB11Fy3693[ChyL8sMT
0EiwSDLEaWd7IsvZ2Wi24cE=)
```

The first four fields specify the domain name of the zone that owns the key, the resource record TTL, class, and RR type. The succeeding fields are:

- **Flags Field:** In its wire format, this field is two bytes long. (The wire format is used in DNS queries and responses.) Bits 0 through 6 and 8 through 14 are reserved, and have a value of 0. Bit 7 indicates if the record holds a DNS zone key. Bit 15 is the Secure Entry Point (SEP) flag, which serves as a hint that indicates whether the DNSKEY record contains a ZSK or a KSK, as described in RFC 3757, DNSKEY R R SEP Flag. Zone administrators typically set the SEP flag of a DNSKEY record of a zone when it contains the KSK, to indicate that it can be used as a trust anchor. However, a DNSKEY record that does not have the SEP flag set can also be used as a trust anchor.

Given the currently defined flags, in its text format, the flags field is represented as an unsigned decimal integer with the possible values of 0, 256 and 257. A value of 256 indicates that the DNSKEY record holds the ZSK and a value of 257 indicates that it contains the KSK. In general, this field contains an odd number when the DNSKEY record holds the KSK.

- **Protocol:** This always has a value of 3, for DNSSEC.
- **Algorithm:** Identifies the public key's cryptographic algorithm. The available types are:
  - 1 = RSA/MD5
  - 2 = Diffie-Hellman (This is not supported by BIND and Infoblox appliances.)
  - 3 = DSA
  - 4 = Reserved
  - 5 = RSA/SHA1
  - 6 = RSA/SHA1/NSEC3
  - 7 = RSA/SHA1/NSEC3
  - 8 = RSA/SHA-256
  - 10 = RSA/SHA-512
- **Public Key:** The public key encoded in Base64.