DNSSEC

Terminology

DNSSEC DNS extensions to ensure the integrity of data returned by domain name lookups. Incorporates a "chain of trust" to DNS hierarchy using public key cryptography.

DNSSEC Resource Records DNSKEY, RRSIG, & NSEC record provide mechanisms to establish authenticity & integrity of data. DS record is to delegate trust to public keys of third parties

RRSIG (Digital Signature)

A DNSSEC record type which private part of the key-pair is used to sign the resource record set (RRset) and digital signature per RRset is saved in an RRSIG record

```
www.abc.com. 299 IN A 104.27.143.238
www.abc.com. 299 IN RRSIG A 13 3 300 201801130933 (
                    20180111073300 35273 abc.com.
                    gbdj/V7rP/d35XE8EGUuXUigovL6Z
                    w3+4SNgr7zPOvH9mr4NfhQpyXBqKO
                    0vF7UG8RqRbhYIUu3/33jblJZXRw)
```

- Record Type
- Public Key Algorithm
- Number of Labels
- Time to Live (TTL)
- Expiration Time
- Inception Time
- Key Tag (DNSKEY id)
- Signer's name

DNSKEY (DNS Public Key)

Contains the zone's public key, uses public key to sign and authenticate DNS resource record sets (RRsets).

KSK (Key Signing Key) which signs other keys, usually larger and stronger than ZSK, it's used as the trust anchor and ceritified by the parent zone in the DNS

ZSK (Zone Signing Key) sign all data in the zone (RRsets) & ususally lower strength & impose less computational overhead

```
www.abc.com. 3599 IN DNSKEY 256 3 13 (
                    koPbw9wmYZ7ggcjnQ6ayHyhHaDNMY
                    ELKTqT+qRGrZpWSccr/lBcrm10Z1P
                    uQHB3Azhii+sb0PYFkH1ruxLhe5g=
                    ) ; key id = 35273
```

- Key Type (KSK, ZSK)
- Time to Live (TTL)
- Protocol Value
- Public Key algorithm
- Key ID

Delegation Signer (DS)

Establishes the chain of trust from parent to child zones. It's hash of the KSK of the child zone which stored in parent zone, together with the NS RRs indicating a delegation of the child zone

```
www.abc.com. 299 IN NS ns1.abc.com.
www.abc.com. 299 IN DS 2371 13 2 (
                    4ED6BEC508C47E84E6F022DD9D1CD
                    DC05BBFDCB908FC3BDADD5A171D6D
                    2D9ABA )
```

- Key ID
- DNSKEY algorithm
- Digest/Hash Type

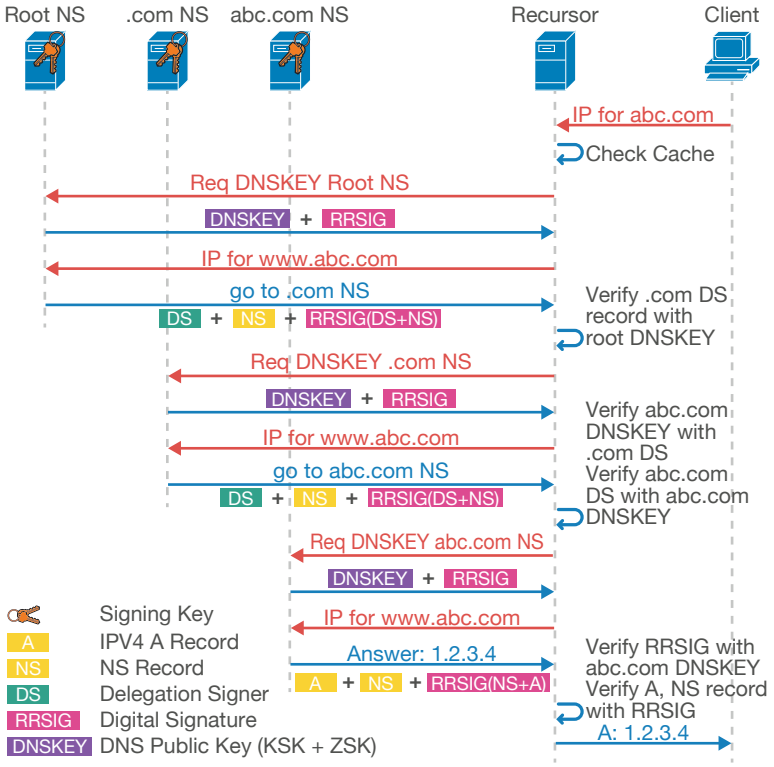
NSEC & NSEC3

NSEC proves the non-existence of a domain. It list next owner name and set of RR types availble. **NSEC3** hash the owner names to provides defense against zone enumeration/walking

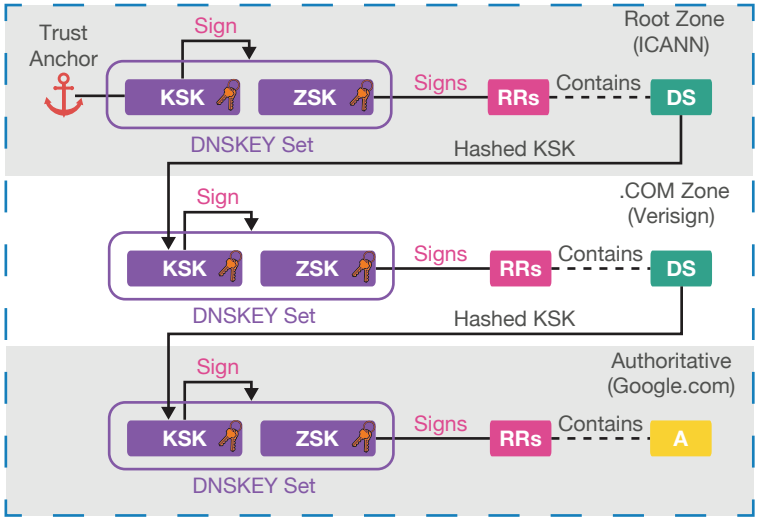
```
www.pir.org. 299 IN NSEC zope.pir.org. A RRSIG NSEC
ec37ns5rqk45a1.icann.org. 299 IN NSEC3 1 0 5 9EBA42
                    28 Q59N9DQ5AV561T6DSV8V8N4A7M
                    9AKRJJ A RRSIG
```

- Owner Name
- Soa min TTL
- Next Owner Name
- Type Bitmap (Assosiated resources to www.pir.org)
- Hash of Owner name
- Next hashed Owner name
- NSEC3 params (algorithm, flags, iterations, salt)

DNS Packet Flow with DNSSEC



Chain of Trust



An authentication chain leads from root to leaf-domain. Each level contains DS records that point to DNSKEY records in a subdomain

DNSSEC Header Flags

Authenticated Data (AD) resolver sets this flag in responses when the queried record is singed with a valid, unexpired signature and an authenticated chains of trust all the way to a configured trust anchor (which could be preconfigured/tracked root key)

Checking Disabled (CD) querier set CD flag to indicate that "pending" (non-authenticated data) is acceptable to it. I.e. it is willing to do its own cryptographic validation of the signatures

DNSSEC OK (DO) a new EDNS0 option to indicate that client is requesting and able to accept DNSSEC RRs in query response

Last update January 13, 2018 (version 1.00)
References: https://cloudpacket.net/bookmarks/

Prepared By **Shakib Shaygan**