Hands-on course

DNSSEC

(and OpenDNSSEC)

DNS

- ✘ Distributed name look-up system
- ✘ You'd like to trust the answer to a retrieval query you pose
- ✘ Did is come from the owner of the zone
  - Authoritative answer aren't from the owner of the zone
  - Answers may be cached, recursors, secondaries, plain text transfers
- ✘ Instead of securing transport, be able to verify answer itself.
  The answer should come with some kind of proof.

Nutshell

Domain Name Security Extension

True extension:

non-DNSSEC aware applications, resolvers and authoritative nameservers will not break.

It is something added to the result.

Adds authenticity and integrity to the DNS answers.

Does not provide confidentiality to DNS.

Signatures and Keys

Typical Lookup

Output from command "dig +noauthority +noadditional dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    60    IN    A    10.10.10.10
```

By default no DNSSEC related information

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyeqmGg==
```

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyeqmGg==
```

This is the normal answer

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.     36     IN     A     10.10.10.10
example.dnslab.uk.     36     IN     RRSIG     A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyeqmGg==
```

This is the proof the answer is authentic and unmodified.

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

It is a signature.

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

Regarding the A record that was returned.

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A  8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

We are using algorithm 8 (RSA encryption with SHA256 hashes).

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8  3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

The depth of the label is 3 ("example" + "dnslab" + "uk").

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3  60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

The original TTL of this record is 60.

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

It is valid from September 20, 2021 09:11.23

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

Until one month later.

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123  6930 dnslab.uk.
          P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyoqmCg==
```

The signer is the owner of domain "dnslab.uk" and the key used has the tag 6930

Typical Lookup

Output from command "dig +noauthority +noadditional +dnssec dnssec.dnslab.uk A":

```
;; ANSWER SECTION:
example.dnslab.uk.    36    IN    A    10.10.10.10
example.dnslab.uk.    36    IN    RRSIG    A 8 3 60
          20211020091123 20210920091123 6930 dnslab.uk.
           P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9p+3O/XlbKRB175
X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxHOYk31kaGTkXyp50Ej+FlVRVqGqpb
fTIKU5Lq9te7KnFXVQL3uH6KQm+WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UI
MCXSkt8/PNSdAuzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi/
ePBq
mEiDg1RZdf1TyeqmGg==
```

The proof: a signature: an encrypted hash.

Hash

Turn data in fixed length "identifier" or checksum.

- Original content not recoverable
- Hard to predict: irreversible
- Same text always yields same result
- Multiple inputs map to same result

Can be used as fingerprint to uniquely identify an item with reasonable security that is cannot be faked.

Some hashing algorithms are better than others. MD5 is broken and SHA1 should not be used for sensitive items.

When two inputs yields the same hash code, this is a collision.

Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.

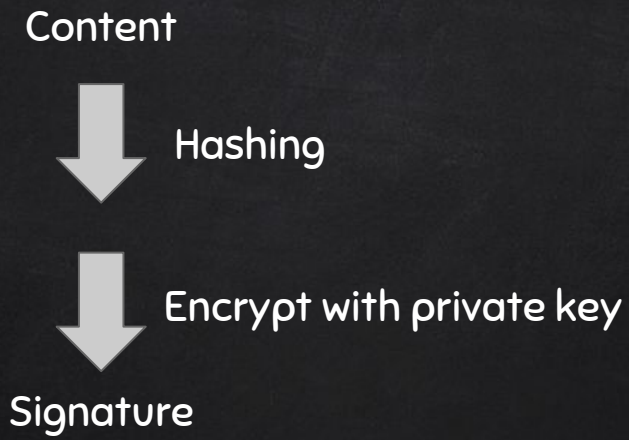
Content

Hashing

Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.



Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.

Content

Hashing

Encrypt with private key

Signature

Content

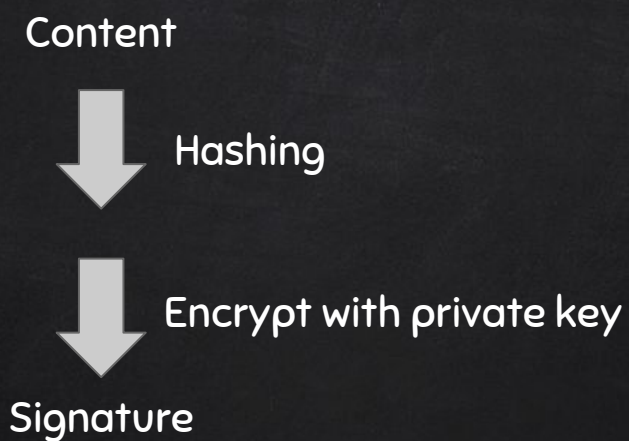
Signature

To verify integrity we need to have both original content and signature

Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.

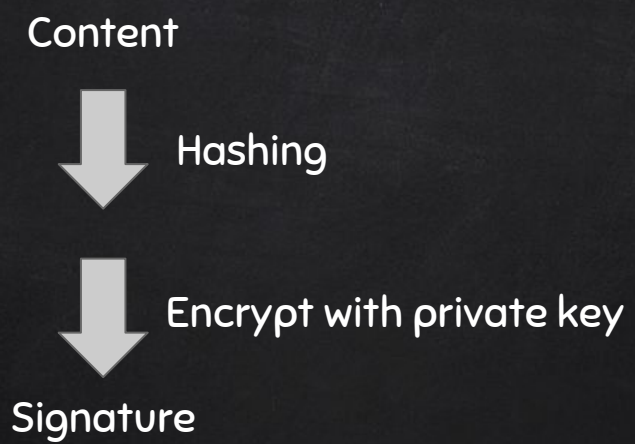


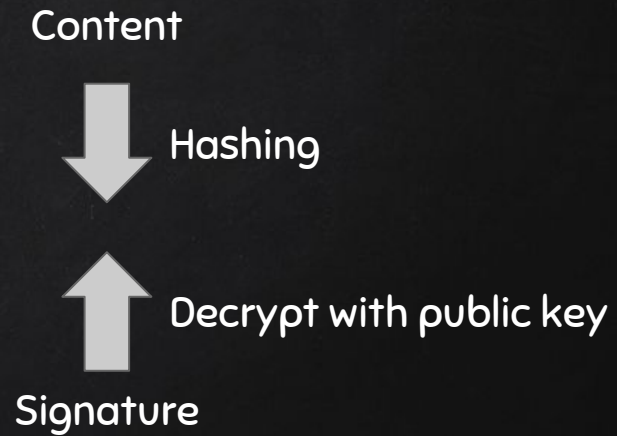
To verify integrity we need to have both original content and signature

Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.



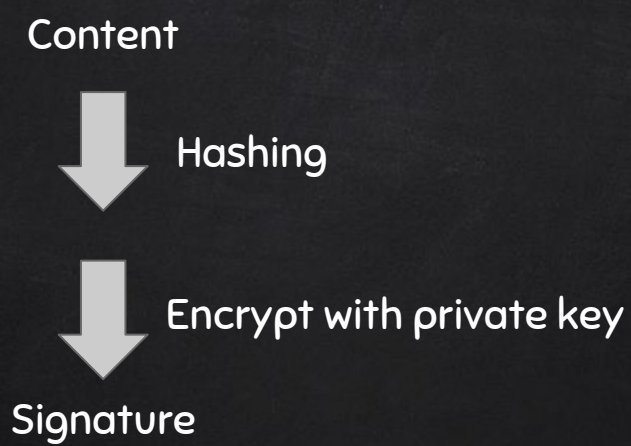


To verify integrity we need to have both original content and signature

Signature

Encrypted hash code using a private key.

Can be verified by decrypted using public key.



To verify integrity we need to have both original content and signature

Dig / Drill flags

From ISC bind suite “dig”. NLnet Labs equivalent “drill”

DO +dnssec dnssec ok, return dnssec information

CD +cdflag: checking disabled

AD authenticated data

AA authoritative answer

An domain / answer can be:
- Secure
- Insecure
- Bogus

Verification process

```
;; ANSWER SECTION:
example.dnslab.uk.    53    IN    A    83.161.152.165
example.dnslab.uk.    53    IN    RRSIG    A 8 3 60
20210920111738 20210917111238 14913 halderen.net.
SCJBfoIPPtMndihVPOjQ3Ne9zbMePC1l3g2EyTQmLJwJp6e1/+qK5C4
t
+UCCcq+0FUNQzdWBMC02tXxqxvaePkJ3WXu7hoHueSQ7SuKn8JiXZnO
q
3UM3lge///00CwP/6x79dNGkyZ5d/oqj3fufna+76Y1tXrhyvXUIrma
k Z88=
```

Computed hash

Create hash using algorithm specified by 8 of:

original TTL + labels + the type + content + label-count and inception/expiration

Verification process

```
;; ANSWER SECTION:
example.dnslab.uk.    53    IN    A    83.161.152.165
example.dnslab.uk.    53    IN    RRSIG    A 8 3  60
20210920111738 20210917111238 14913 halderen.net.
SCJBfoIPPtMndihVPOjQ3Ne9zbMePC1l3g2EyTQmLJwJp6e1/+qK5C4
t
+UCCcq+0FUNQzdWBMC02tXxqxvaePkJ3WXu7hoHueSQ7SuKn8JiXZnO
q
3UM3lge///00CwP/6x79dNGkyZ5d/oqj3fufna+76Y1tXrhyvXUIrma
k Z88=
```

Computed hash

Decrypted hash

Use the domain's private key to decrypt using algorithm specified by 8.

If the decrypted output is equal to the hash we computed, then the answer is authentic (the hash computed by the zone signer is the same) The fingerprint matches.

Why use hashes

- ✘ DNSSEC is an extension, just return some additional records
  which is already practise in DNS and can be ignored.
- ✘ Answers are not dependent on transport and can easily be cached and transported

- ✘ Hashes are good enough as fingerprint
  No need to encrypt the original data
  - Much smaller to transmit
    We are working with the limits of packets
  - Does require to recompute the hash

RRSIG fields

```
example.dnslab.uk.    36   IN   RRSIG    A 8 3 60
         20211020091123 20210920091123 6930 dnslab.uk.
         P6o1YZg0zh53067TRXFWxNLQUxKhdJ6QFKAgIWTvuYC+
OL8Au8ebgAHFfV7NuKK3Ht8NAsGvJ8ex8pnEyMWiIvUrPzG5LTGB6E9
p+3O/XlbKRB175X+oJPkNOkCkWf2/D7B9WnC93cVImDkSVZQX53zsxH
OYk31kaGTkXyp50Ej+FlVRVqGqpbfTIKU5Lq9te7KnFXVQL3uH6KQm+
WZVqLkbv/SkF96Xy8oCM4fjrMRrOc9fUmLjYBn/0UIMCXSkt8/PNSdA
uzQL4MZTWMlp2E/ZsLRG3mz3a4wNAVkhrNT8o99KeHgzAiOLGBaAryi
/ePBq
mEiDg1RZdf1TyeqmGg==
```

RRSIG type record type used to return the result.

A RRSIGs are returned per answer returned. Answers are always given for RRsets

So the hash is computed over all RRs in the RRset

RRsets

For hashing to work, the input that is supposed to create a stable hash always has to be the same form.

Hash is computed over all the resource records (RRs) in the set (RRset).
The records with the same RR-type (e.g. A-records) on the same label belong to same set.
No duplicates allowed. All records in the RRset must have the same TTL.

To create a hash, there must be a fixed (canonical) ordering of the individual RRs in the RRset.

Also because the signature is computed on the original TTL, but this is modified on the wire; the original TTL must be included.

Algorithms

1	RSA for encryption / MD5 for hashes	RSAMD5
2	Diffie Hellman	DH
3	DSA/SHA1	DSA
5	RSA/SHA1	RSASHA1
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256- NSEC	RSASHA256
10	RSA/SHA-512	RSASHA512
12	GOST R 34.10-2001	ECC-GOST
13	ECDSA Curve P-256 with SHA256	ECDSA2564SHA256
14	ECDSA Curve P-384 with Sha384	ECDSAP384SHA384
15	ED25519	ED25519
16	ED448	ED448

Replay attacks

The Time-To-Live (TTL) value of a signature record (RRSIG) isn't enough.

If you want to move your server, you do not want your old server information to be republished by a malicious party to perform a denial-of-service.

Even worse if the attacker would be able to place his own software on the IP address returned by the old record.

To combat signatures have a validity that is limited, though still much larger of the TTL. So you can still move a service quickly enough.

The key

In order to validate the result we need:

1. The plain text answer
2. The signature: the encrypted fingerprint
3. The public key to decrypt the fingerprint

So we need the public key.

DNSSEC solution: retrieve public key using a lookup using DNS.

The apex of the domain is known, the RRSIG field contains a reference to it.

The signature / RRSIG records are returned on the answer itself.
The records containing the public key, DNSKEY, are retrieved, and cached, separately.

Typical Lookup

Command "drill +noauthority +noadditional -D -t example.com DNSKEY":

```
example.com.  60 DNSKEY  256 3 8 AwEAAd0r756MOcFM1jtDwNY/45mvMBIvpnxz7X7pI
Z/KzhFuBQ8n7WloKUCvlrlF6hljlsO0dXDJUvY9N1Q+kjWGTVQjXRHwEngIfU8cVwOraYoMbIcp9t
y
0hSXqgijNu7sVVRrWfhsfyFI82AFMjXpoKwyaMUe8/VT4OUklE5gdYXAR
example.com.  60 DNSKEY  257 3 8 AwEAAZ0aqu1rJ6orJynrRfNpPmayJZoAx9Ic2/Rl9
VQWLMHyjxxem3VUSoNUIFXERQbj0A9Ogp0zDM9YIccKLRd6LmWiDCt7UJQxVdD+heb5Ec4qlqGmyX
9MDabkvX2NvMwsUecbYBq8oXeTT9LRmCUt9KUt/WOi6DKECxoG/bWTykrXyBR8elD+SQY43OAVjlW
rVltHxgp4/rhBCvRbmdflunaPIgu27eE2U4myDSLT8a4A0rB5uHG4PkOa9dIRs9y00M2mWf4lyPee
7vi5few2dbayHXmieGcaAHrx76NGAABeY393xjlmDNcUkF1gpNWUla4fWZbbaYQzA93mLdrng+M=

example.com. 60 RRSIG DNSKEY 8 2 60 20211008172400 20210917183639 31406
                        example.com.
FxvTJN+ZyfYr6bwN4cDvl71Cao6gyFqM3CSwMKOgU
NI3F6uXu414iWj9KZuKSG6QXO9OQn9Johau/umT/ENmZgUobeJnxxXnGR22k42Huw4IfuVweM6pu7
W0TV8fF1aYxX1q3M8Jv86QTrLwmjMOcwOVvdPwFdprIPeUIl8F4EfhwDkTNeohQqMRg+6xP1RFhFe
3WhTlTRhe99TFLF5sHK7bJXZK91M80kH6r7Dc59mVuFQpAQN1wRGFLCnOCXv9m5fBmAch4eIJNljS
```

DNSKEY RR

There can be more than one key being returned, usually two.

A key used to sign the DNSKEY RR:

The Key Signing Key KSK

A key user to sign all other RRs:

The Zone Signing Key ZSK

The signature (RRSIG) returned along with the key set (all DNSKEY RRs) has the same format, is produced the same and can be validated the same way. It just uses a different key in the encryption/decryption.

DNSKEY fields

```
example.com.  60 IN  DNSKEY  256 3 8
AwEAAd0r756MOcFM1jtDwNY/45mvMBIvpnxz7X7pIZ/KzhFuBQ8n7Wl
oKUCvlrlF6hljlsO0dXDJUvY9N1Q+kjWGTVQjXRHwEngIfU8cVwOraY
oMbIcp9ty0hSXqgijNu7sVVRrWfhsfyFI82AFMjXpoKwyaMUe8/VT4O
UklE5gdYXAR
```

1. The record type DNSKEY
2. Flags; either 256 for ZSK or 257 for KSK
3. Protocol: always 3 (envisioned for future expansion)
4. Algorithm (the same as the earlier algorithm in the RRSIG)
5. The public key, base64 encoded here

Note there is no keytag here. This key identifier is computed from the public key part.

Keytag

- ✘ Is computed from the public key plus some additional information such as the zone apex.
- ✘ Is 32 bit identifier; non-uniform
- ✘ Same keytag between zones will occur -- not a problem
- ✘ Collisions within a zone is not impossible to ever occur.
- ✘ Keytags are just hints to the resolver which key to try first.
- ✘ Therefore collisions may involve small performance hit on resolvers, but no errors in signing or resolving should occur.
- ✘ Some software will avoid using keys with the same keytag within one zone

Hands-on

Simple zone signing

http://dnslab.uk/