den údaj, který je jen informativní a není zaručena jeho jedinečnost, a tím je keytag (nebo také id) klíče – 16bitové číslo používané pro rychlou identifikaci.

Obecné doporučení je používat dva druhy klíčů – ZSK (Zone Signing Key) a KSK (Key Signing Key). Z názvů těchto klíčů vyplývá, že první typ bude použit pro podpis samotného obsahu zóny a druhý se bude používat pouze pro podepisování klíčů.

Toto rozdělení je čistě praktické – výměna klíčů v nadřazené zóně není triviální operací, a proto byla i v rámci klíčů zavedena hierarchie.

KSK je klíč, který může být silnější (má větší počet bitů), výsledný podpis je větší, podepisování tímto klíčem je výpočetně náročnější a také validace podpisů vytvořených tímto klíčem je výpočetně náročnější.

Proto je tento klíč použit pouze pro vytvoření jediného podpisu v celé zóně, a to podpisu všech DNSKEY záznamů. Díky větší síle klíč může být v zóně publikován a používán delší dobu bez ohrožení bezpečnosti. KSK se od ZSK liší pouze jedním bitem v příznacích klíče (257 je KSK a 256 je ZSK).

ZSK je zase klíč, který je slabší a používá se pro podpis všech záznamů v zóně. Protože je klíč slabší, musí být měněn častěji, ale díky hierarchii mezi KSK a ZSK neznamená výměna ZSK žádnou interakci s nadřazenou zónou.

DNSSEC podpis

Další nový RR typ, který je potřeba pro vlastní digitální podpis pomocí DNSSEC – typ záznamu RRSIG. Pokud si ještě vzpomenete na první díl našeho seriálu o technologii DNSSEC, tak jsme hned na začátku mluvili o RRSetech, což jsou RR záznamy, které mají všechny údaje kromě RDATA stejné.

Termín RRSet je pro DNSSEC důležitý, protože digitální podpis se vytváří pro RRSet, a nikoli pro jednotlivé RR záznamy. DNS odpověď s DNSSEC může vypadat například takto:

```
www.dnssec.cz.    7200 IN    RRSIG A 5 3 7200 20110812080302
                  20110729080302 55673 dnssec.cz.
                  PXHDkbh9eud8Tvq42vDR02jBj1zgUbX5vAclyc8Vt46R
                  ikGM2AeDBO8lMufsmkMw2KRfViF7M3O3a6rTDBegeTBq
                  OAdLBM32qaR7FJZJEXi539MudoUBJegsK5n3mLTvlY6Q
                  DpFF3kUGkmho1cvASTivhaiXyWiMoR1BBHSxfdc=
```

Pokud se podíváme na obsah RRSIG záznamu, objevíme položky uvedené v tabulce:

Položky v RRSIG záznamu

A	Typ podepsaného záznamu
5	Použitý algoritmus (5 – RSASHA1)
3	Počet labelů podepisovaného doménového jména
7200	TTL původního záznamu
20110812080302	Datum konce platnosti podpisu
20110729080302	Datum počátku platnosti podpisu
55673	Keytag klíče použitého pro vytvoření podpisu
dnssec.cz.	Vlastník klíče použitého pro vytvoření podpisu (jméno zóny)
PXHDkbh…xfdc=	Textová reprezentace digitálního podpisu

K čemu je tento záznam dobrý? Pokud máte správně nakonfigurovaný rekurzivní DNS server, aby prováděl validaci DNSSEC podpisů (dále také validující resolver), může ověřit, že data nebyla v průběhu transportu změněna nebo kompletně podvržena.

To je poměrně důležitá informace – validace podpisů se vždy provádí na straně klienta a podpis je vždy předpočítán dopředu, takže samotný DNSSEC nezatěžuje autoritativní DNS servery.

Z uživatelského hlediska je obsah záznamu RRSIG nezajímavý – pokud hledáme chybu, pak můžeme pouze zkontrolovat údaje, jako jsou datum počátku a konce platnosti, keytag klíče a vlastníka klíče. Ověření platnosti samotného digitálního podpisu není v silách normálních smrtelníků.

V příkladu výše jsme se ptali přímo autoritativního serveru, který neprovádí validaci. Pokud stejný dotaz položíme nakonfigurovanému validujícímu resolveru, bude vypadat například takto:

```
; <<>> DiG 9.7.3 <<>> +multi +dnssec www.dnssec.cz @217.31.204.130
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31013
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, […]

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.dnssec.cz.   IN A

;; ANSWER SECTION:
www.dnssec.cz.    7200 IN    A 217.31.205.51
www.dnssec.cz.    7200 IN    RRSIG A 5 3 7200 20110812080302 (
                  20110729080302 55673 dnssec.cz.
                  PXHDkbh9eud8Tvq42vDR02jBj1zgUbX5vAclyc8Vt46R
                  ikGM2AeDBO8lMufsmkMw2KRfViF7M3O3a6rTDBegeTBq
                  OAdLBM32qaR7FJZJEXi539MudoUBJegsK5n3mLTvlY6Q
                  DpFF3kUGkmho1cvASTivhaiXyWiMoR1BBHSxfdc= )
[...]
```

V příznacích DNS zprávy přibyl příznak AD (Authenticated Data). Ten indikuje, že validující resolver ověřil platnost DNSSEC podpisu a data v DNS odpovědi jsou správná a nebyla pozměněna.

Tento příznak ovšem dostaneme pouze tehdy, pokud použijeme volbu +dnssec na příkazové řádce nástroje dig, která v DNS dotazu nastaví příznak DO (DNSSEC OK). Pokud bychom tento příznak nenastavili, tak v DNS odpovědi nepoznáme, že RR záznamy byly validovány.

Takto je zajištěna zpětná kompatibilita s klienty, kteří DNSSEC neznají. Možná vás v tuto chvíli napadlo – a jak tedy klient pozná, pokud byla data podvržena a digitální podpis nesouhlasí? V takovém případě se DNS odpověď vrátí s chybovým příznakem SERVFAIL a špatná odpověď se ke klientovi vůbec nedostane.

Návratový kód SERVFAIL bude nastaven i v případě, že „jen“ vyprší časová platnost podpisu. I tehdy již není RRSIG podpis platný a nebude validován. Proto je potřeba podpisy v zónovém souboru pravidelně obnovovat.

Pro odlišení normální chyby serveru a chyby ve validaci DNSSEC podpisu byl zaveden speciální příznak CD (Checking Disabled), který nastavuje klient v dotazu na validující resolver. Tento příznak způsobí návrat dat v DNS odpovědi i v případě, že podpis není validní.

Podpis neexistujícího záznamu

V předchozím odstavci jsme si ukázali, jak vypadá podpis pomocí DNSSEC. Jistě jste si všimli, že podepsané jsou DNS záznamy. V případě, že dotazovaný záznam neexistuje, je v DNS odpovědi nastaven návratový kód na hodnotu NXDOMAIN.

DNS odpověď, která v sobě neobsahuje žádná data, ovšem nemůže být podepsána. A v tuto chvíli nastupuje další typ RR záznamu – NSEC:

```
www.dnssec.cz.  7193 IN    NSEC dnssec.cz. A AAAA RRSIG NSEC
```

NSEC je RR záznam, který ve svých RDatech obsahuje informaci