

Rozszerzenie bezpieczeństwa protokołu DNS

Warsztaty

DNSSEC

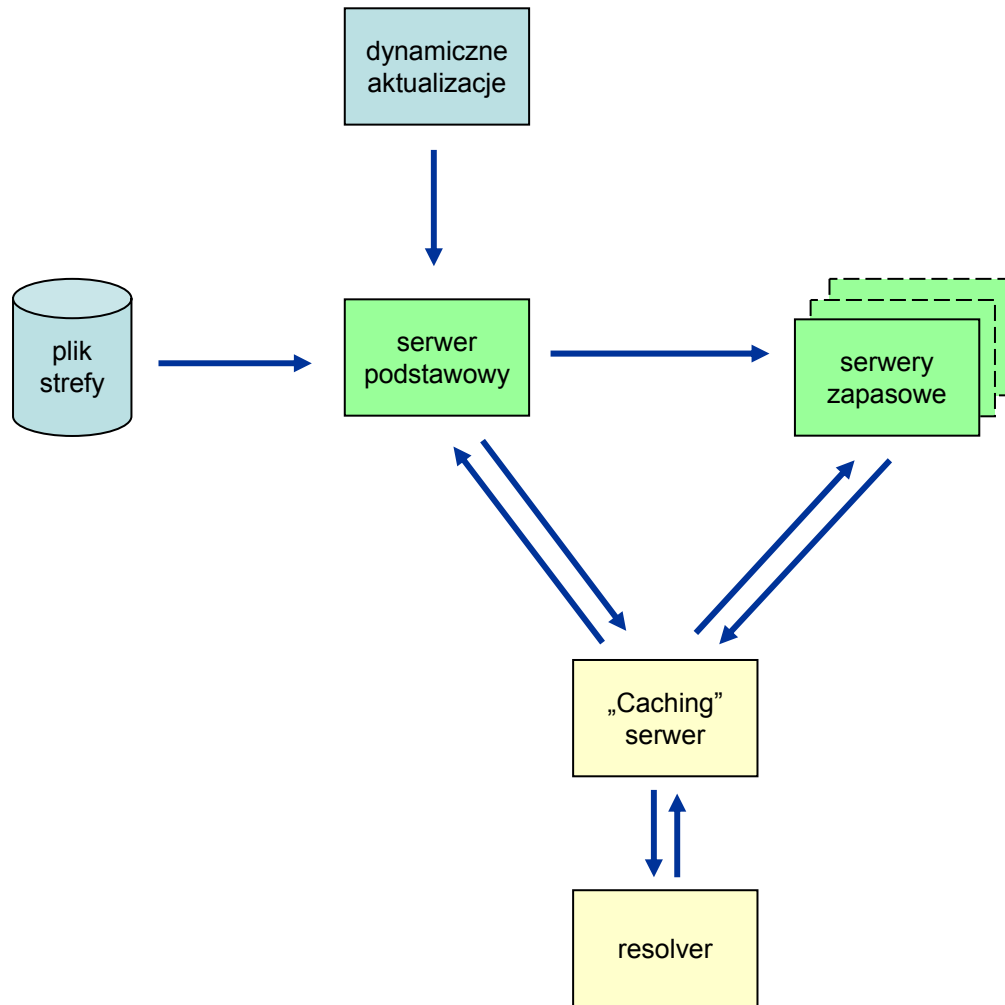
Po co DNSSEC?

- DNS (RFC 1034, RFC 1035) nie jest doskonały
- Wady i zagrożenia są dobrze znane
 - ✓ Amplification Attacks
 - ✓ Cache Poisoning
 - ✓ Distributed Denial of Service (DDoS) Attack
 - ✓ Monkey-in-the-Middle Attack
 - ✓ Pharming Attacks
 - ✓ Spoofing

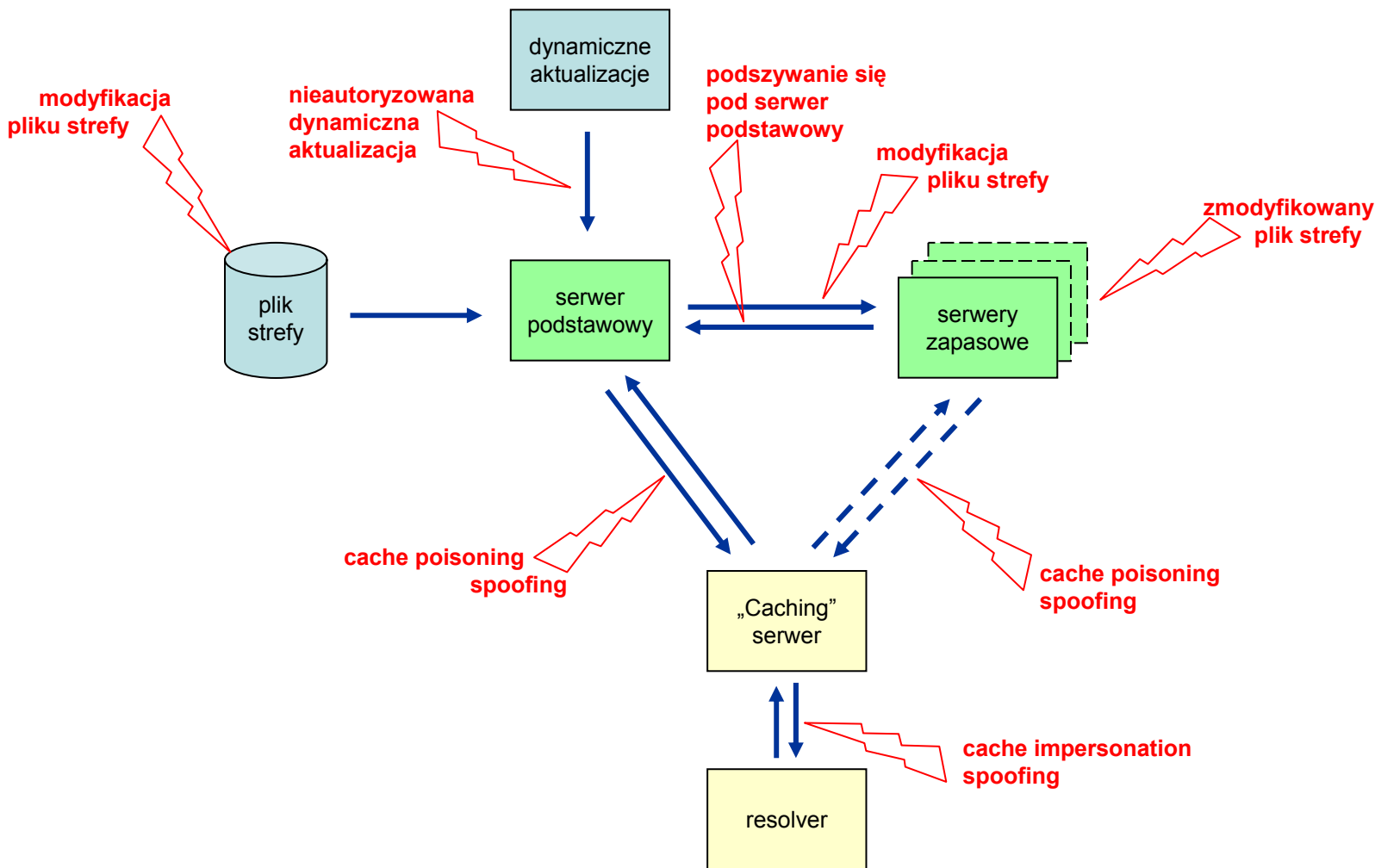
Literatura:

- RFC 3833 Threat Analysis of the Domain Name System (DNS)
- Schuba, C., "Addressing Weaknesses in the Domain Name System Protocol", Master's thesis, Purdue University Department of Computer Sciences, August 1993.
- <http://www.dnssec.net/dns-threats>

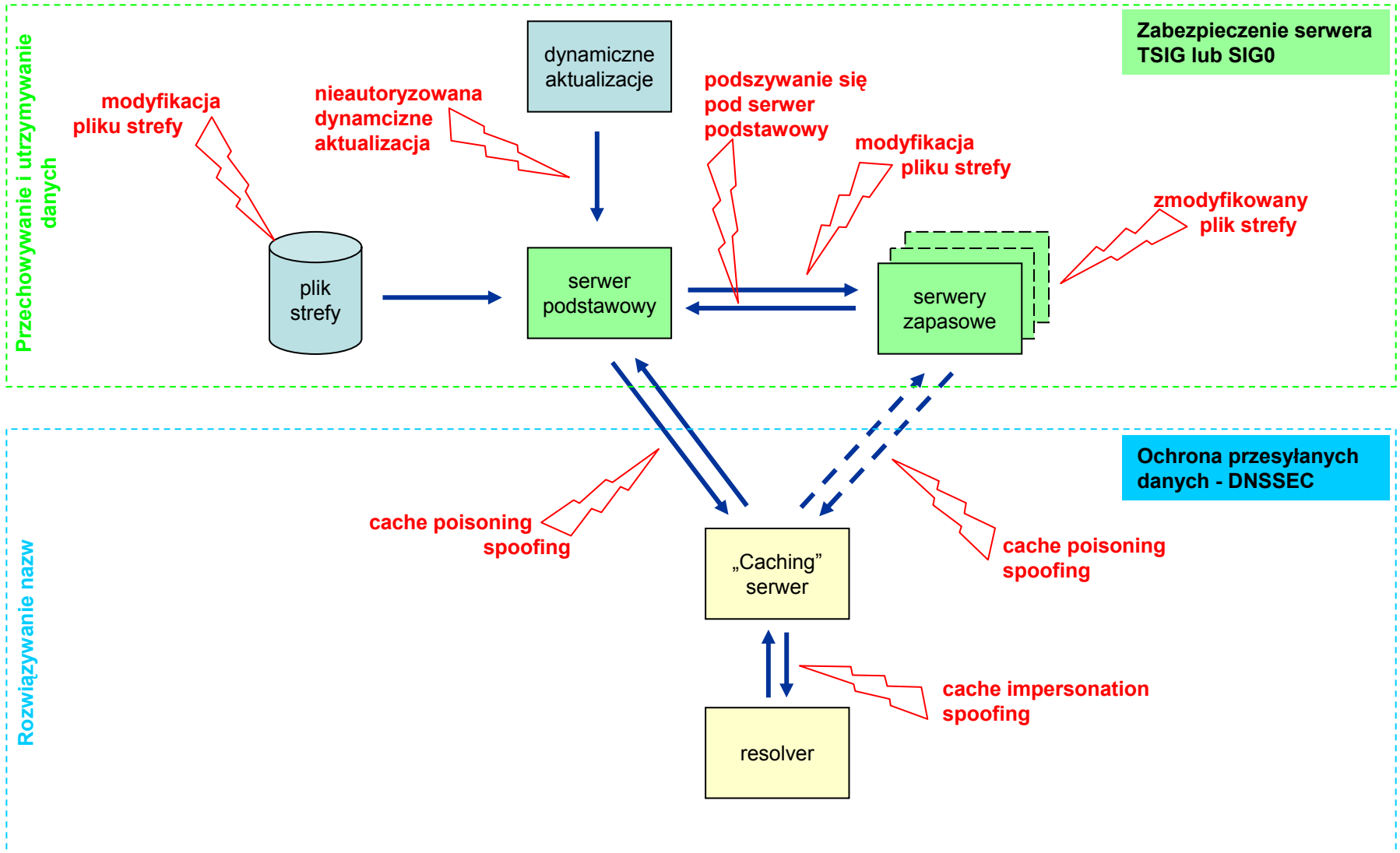
Przepływ danych w DNS



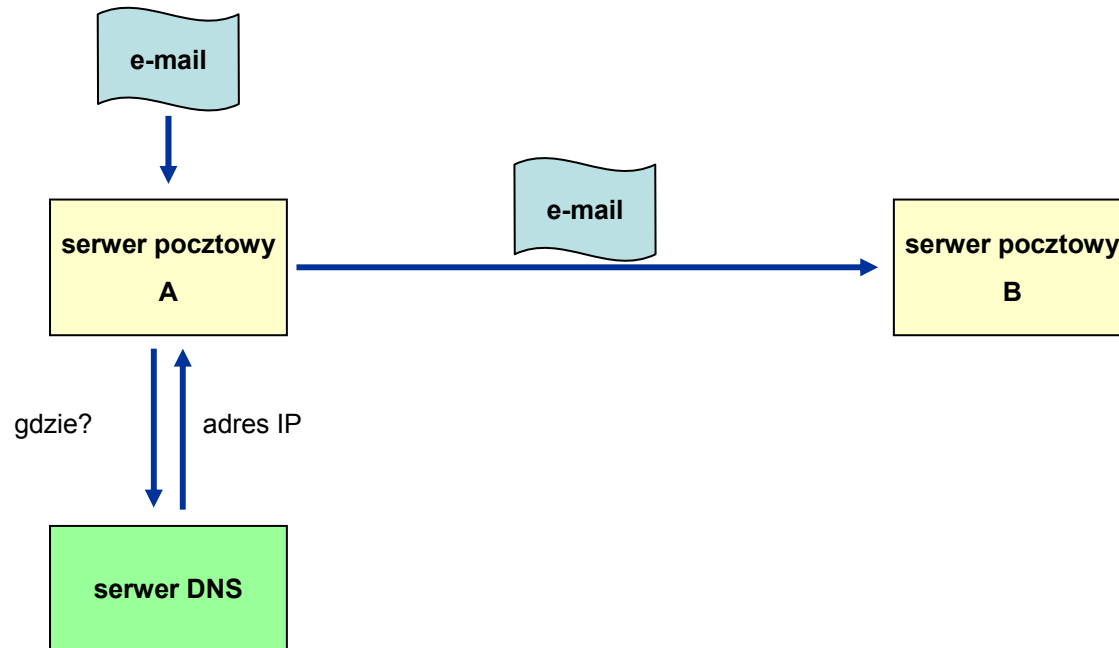
Zagrożenia w DNS



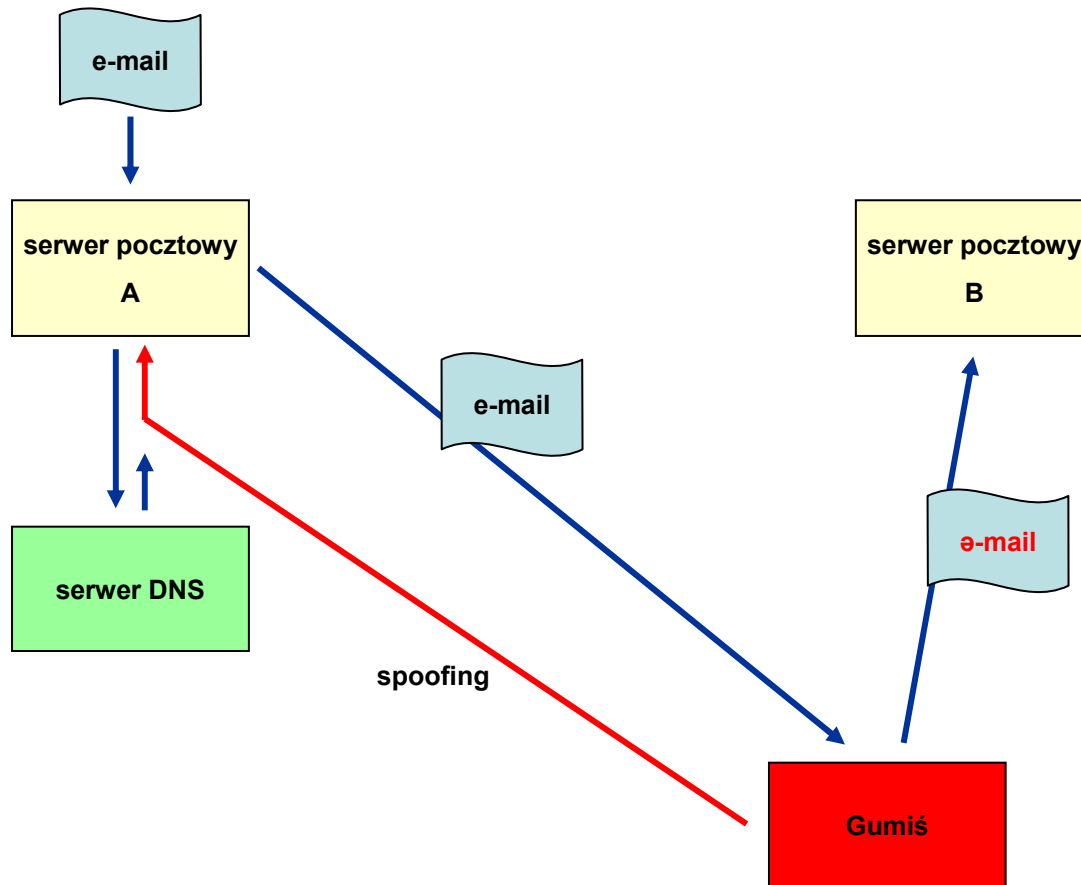
Zabezpieczenia



Jeszcze jeden przykład



Jeszcze jeden przykład



Właściwości DNSSEC

- DNSSEC dostarcza mechanizmy obrony przed:
 - ✓ spoofing'iem
 - ✓ modyfikacją/fałszowaniem wiadomości DNS
- Umożliwia zapewnienie **integralności** i możliwość weryfikacji **autentyczności** pozyskanych danych.
- Opiera się na kryptografii klucza publicznego (kryptografia asymetryczna)
 - ✓ klucz prywatny wykorzystywany jest do generowania podpisów (RRSIG)
 - ✓ klucz publiczny jest używany do weryfikacji podpisanych danych (DNSKEY)

Właściwości DNSSEC

- Podpisywane są zestawy rekordów zasobów (RR sets).
- Daje możliwość weryfikacji odpowiedzi DNS.
- Daje możliwość weryfikacji odpowiedzi negatywnych (ang. authenticated denial of existence of DNS data).
- Bezkonfliktowo współistnieje z niezabezpieczoną częścią systemu DNS
- DNSSEC nie dostarcza:
 - ✓ mechanizmów autoryzacji
 - ✓ poufności danych

Rys historyczny

- Prace nad DNSSEC rozpoczęto w 1995
- W 1999 opublikowano RFC 2535
- W marcu 2005 opublikowano tzw. **DNSSECbis**
RFC 4033, RFC 4034, RFC 4035

Nowe rekordy DNS

DNSSEC wprowadza następujące nowe rekordy zasobów:

- **DNSKEY**
klucz publiczny do weryfikacji podpisów (rekordów RRSIG)
- **RRSIG**
podpis grupy rekordów
- **NSEC**
zapewnienie spójności danych strefy i umożliwienie weryfikacji informacji o nieistnieniu rekordu lub o braku zabezpieczeń (authenticated denial of existence of data); rekord wskazuje, na następną dostępną nazwę w pliku stref (dane posortowane kanonicznie) oraz wskazuje, które typy rekordów są dostępne dla danej nazwy domenowej.
- **DS**
wskazanie na klucz podpisujący klucz (KSK - key signing key) w strefie podrzędnej, (delegation signer)

(typy rekordów zasobów: <http://www.iana.org/assignments/dns-parameters>)

Serwery DNS wspierające DNSSEC

- **Bind 9.3+**
<http://www.isc.org/sw/bind/> (zalecany 9.3.2 lub nowszy)
- **NSD**
<http://www.nlnetlabs.nl/nsd/>
- **Nominium ANS**
<http://www.nominium.com/products.php?id=2>
- **Nominium CNS**
<http://www.nominium.com/products.php?id=1>

Więcej informacji o narzędziach DNSSEC na <http://www.dnssec.net/software>

Autentyczność i integralność danych

- **Autentyczność**

DNSSEC dostarcza mechanizm, który umożliwia zweryfikowanie źródła informacji

- **Integralność**

DNSSEC zapewnia integralności komunikacji, umożliwiając stwierdzenie czy odebrana informacja jest w takiej postaci, w jakiej została wysłana.

Stan weryfikowanych danych

Resolver walidujący dane może je określić jako:

- **zabezpieczone (secure)**

zestaw rekordów (RRset) i ich podpis (RRSIG) zostały poprawnie zweryfikowane odpowiednim kluczem publicznym (DNSKEY), dla którego resolver ustalił łańcuch zaufania; resolver posiada punkt zaufania (trust anchor) dla danego fragmentu przestrzeni DNS

- **niezabezpieczone (insecure)**

resolver posiada punkt zaufania dla danego fragmentu przestrzeni DNS lecz dane nie są podpisane a w strefie nadrzędnej brak rekordu DS

- **fałszywe (bogus)**

resolver posiada skonfigurowany punkt zaufania (trust anchor), rekord DS wskazujący, że dane pochodzą z zabezpieczonej strefy, jednak z jakiegoś powodu nie może ich poprawnie zweryfikować (np. brak podpisu, podpis utracił swoją ważność, dane podpisane algorytmem, który nie jest wspierany, itp)

- **nieokreślone (indeterminate)**

resolver nie posiada punktu zaufania, dla danego fragmentu przestrzeni DNS

Rekord DNS a zestaw rekordów (RRset)

- Pojedynczy rekord DNS

a-dns.pl.	86400	IN	A	195.187.245.44
a-dns.pl.	86400	IN	AAAA	2001:a10:1:1::44

- Zestaw rekordów

pl.	86400	IN	NS	c-dns.pl.
pl.	86400	IN	NS	d-dns.pl.
pl.	86400	IN	NS	e-dns.pl.
pl.	86400	IN	NS	f-dns.pl.
pl.	86400	IN	NS	g-dns.pl.
pl.	86400	IN	NS	a-dns.pl.
pl.	86400	IN	NS	b-dns.pl.

NAME	TTL	CLASS	TYPE	RDATA
-------------	------------	--------------	-------------	--------------

- Podpisywane są tylko zestawy rekordów, a nie indywidualne rekordy
- Podpisywane są tylko rekordy autorytatywne

Rekord DNS a zestaw rekordów (RRset)

[...]

```
pl.      86400 IN NS d-dns.pl.
pl.      86400 IN NS e-dns.pl.
pl.      86400 IN NS f-dns.pl.
pl.      86400 IN NS g-dns.pl.
pl.      86400 IN NS a-dns.pl.
pl.      86400 IN NS b-dns.pl.
pl.      86400 IN NS c-dns.pl.
pl.      86400 IN RRSIG NS 5 1 86400 20060910092108 (
          20060811092108 5891 pl.
          gKJrJrdyckVEYi3w5OmofrBu6/G6r1EmqcRF0aWQwd+cqh
          +0wIHZD4ca47DjfoeySWKt1RNdBfF4qEfAGCAY2QQvM/
          M91I4Wb0Omg6FqfkKeRutAsedyK7It2eKOhfMJVl5ya3
          R0YwoMEz/ZV2uE0ocZ2Oaw2Cn1Dw2SC9PDP5S9A= )

pl.      86400 IN TXT "ccTLD of Poland"
pl.      86400 IN RRSIG TXT 5 1 86400 20060910092108 (
          20060811092108 5891 pl.
          irSmpvu1Xb8Ucd1KWJarobFRkkPMVdJtj0sAC7rCSpGr
          MHKfbsKvZa+7lQJpVYzBMLExKkipprzz40Qoc0fMdiAZ
          RhdhByIKRCcNm3/iMI0jQyxKgPfrh8ZyfsPHCXZ7DVSy
          HFa9Wsn1LxroB0rPir7VHvX1Urd0JciZxfOIPmQ= )
```

**Podpisany
zestaw rekordów**

**Podpisany
pojedynczy rekord**

[...]

Rekord DNSKEY

- **flaga (16 bitów)**
może przyjąć trzy wartości 0, 256, 257. Wartość 256 wskazuje, że jest to klucz ZSK (zone signing key), natomiast wartość 257 informuje, że jest to KSK (key signing key)
- **protokół (8 bitów)**
musi mieć wartość 3; inne wartości spowodują, że klucz zostanie uznany za nieprawidłowy
- **algorytm (8 bitów)**
RFC 4034, Appendix A.1
- **klucz publiczny (n*32 bity)**
reprezentowane jako Base64 (RFC 3548)
- **ID klucza**
stanowi fragment nazwy pliku z kluczem; jest wstawiane automatycznie jako komentarz podczas podpisywania strefy.

```
p1.                86400 IN DNSKEY 256 3 5 (
                    AQQ01MgGQTTAbRX107Bo8A7qzAn050Hd9QhLqqvXZSAO
                    /IAq+gG/HheXzLC9PgbtiC+q4/eHK011M8m9h2qdJT1j
                    nZM8fEhi95dLS9XPN/I1070vaii0h3gAk+UWGQ/rt2q6
                    oRt6VcJI0VXgCqJn4IBICKhpVTzIy1+VXe5gvw5Wqw==
                    ) ; key id = 50099
```

Typy algorytmów w DNSSEC

- RFC 4034, Appendix A.1

Value	Algorithm [Mnemonic]	Signing	References	Status
0	reserved			
1	RSA/MD5 [RSAMD5]	n	[RFC 2537]	NOT RECOMMENDED
2	Diffie-Hellman [DH]	n	[RFC 2539]	-
3	DSA/SHA-1 [DSA]	y	[RFC 2536]	OPTIONAL
4	Elliptic Curve [ECC]		TBA	-
5	RSA/SHA-1 [RSASHA1]	y	[RFC 3110]	MANDATORY
252	Indirect [INDIRECT]	n		-
253	Private [PRIVATEDNS]	y	see below	OPTIONAL
254	Private [PRIVATEOID]	y	see below	OPTIONAL
255	reserved			

6 - 251 Available for assignment by IETF Standards Action.

Funkcje skrótu w DNSSEC

- RFC 4034, Appendix A.2

VALUE	Algorithm	STATUS
0	Reserved	-
1	SHA-1	MANDATORY
2-255	Unassigned	-

Rekord RRSIG

- typ podpisanych rekordów (16 bitów)
- algorytm (8 bitów)
- ilość etykiet (8 bitów)
- TTL podpisanych rekordów (32 bity)
- data ważności podpisu (32 bity)
czas UTC
- data początku ważności podpisu (32 bity)
- ID klucza (16 bitów)
- nazwa właściciela rekordu DNSKEY
- podpis

```
pl.      86400 IN RRSIG DNSKEY 5 1 86400 20060910092108 (
        20060811092108 5891 pl.
        gnVIu1N1XJSM1Aspt2bQrFJ/Ib0cTOic+DHOQDpn/tAG
        DFZtOscRHwWUCtKf7zp0CpkxnDZ+ReG1qUYh2rc7ydHm
        pgCWv5A6G5iMh6cy+a3SVHW7QnT1ud7PmIazZkFGy5pH
        OKtoR+RwDJUvfqz1tbpX76bDF6FRVtIfRWkxNo0= )
```

Rekord DS

- Wskazuje, że strefa jest zabezpieczona (podpisana cyfrowo)
- Wskazuje na klucz w zabezpieczonej strefie
Jeżeli strefa ma klucz KSK, to rekord DS wskazuje na ten klucz
- Występuje **tylko** w strefie macierzystej (nadrzędnej), w punkcie delegacji
- Jest rekordem autorytatywnym w strefie macierzystej

Rekord DS

- ID klucza (16 bitów)
- algorytm (8 bitów)
- typ funkcji skrótu (8 bitów)
- skrót (20 bajtów)
SHA-1

```
pl.          86400      IN DS 39540 5 1 (
              94317A6B91D01166C27C
              E3DB6514B2D908964BE3
              )
```

Wyliczanie skrótu

```
skrót = funkcja_skrótu( nazwa właściciela rekordu DNSKEY | DNSKEY RDATA );
```

"|" oznacza ciąg

```
DNSKEY RDATA = Flaga | Protokół | Algorytm | Klucz publiczny.
```

Rekord NSEC

- Wskazuje na następną domenę w strefie
- Wskazuje typy rekordów jakie posiada „właściciel” rekordu NSEC
- Rekord NSEC dla ostatniej nazwy w strefie wskazuje na pierwszą nazwę w strefie dane w strefie są posortowane kanonicznie (RFC 4043, rozdział 6)
- Wykorzystywany do weryfikacji odpowiedzi negatywnych (authenticated denial of existence of DNS data).
- Jest rekordem autorytatywnym w strefie macierzystej

Rekord NSEC

- Wskazuje na następną domenę w strefie
- Wskazuje typy rekordów jakie posiada „właściciel” rekordu NSEC
- Rekord NSEC dla ostatniej nazwy w strefie wskazuje na pierwszą nazwę w strefie dane w strefie są posortowane kanonicznie (RFC 4043, rozdział 6)
- Wykorzystywany do weryfikacji odpowiedzi negatywnych (authenticated denial of existence of DNS data).
- Jest rekordem autorytatywnym w strefie macierzystej
- Jest generowany automatycznie podczas podpisywania strefy

```
p1.          86400      IN NSEC 0.p1. NS SOA TXT RRSIG NSEC DNSKEY
```

Rekord NSEC - przykład 1

■ Pytanie o nieistniejący rekord

```
[...]  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61306  
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
;; QUESTION SECTION:  
  
;; QUESTION SECTION:  
;pl. IN MX  
  
;; AUTHORITY SECTION:  
pl. 3600 IN SOA a-dns.pl. dnsmaster.nask.pl. ...  
pl. 3600 IN RRSIG SOA 5 1 86400 20060920053241 ...  
pl. 3600 IN NSEC 0.pl. NS SOA TXT RRSIG NSEC DNSKEY  
pl. 3600 IN RRSIG NSEC 5 1 3600 20060920053241 ...  
;; Query time: 1 msec  
[...]
```

Rekord NSEC - przykład 2

■ Pytanie o nieistniejącą domenę

```
[...]  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45523  
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
;; QUESTION SECTION:  
;dnssec-test.pl.          IN ANY  
  
;; AUTHORITY SECTION:  
pl.                      3600 IN SOA a-dns.pl. dnsmaster.nask.pl. ...  
  
pl.                      3600 IN RRSIG SOA 5 1 86400 20060920091144 ...  
pl.                      3600 IN NSEC 0.pl. NS SOA TXT RRSIG NSEC DNSKEY  
pl.                      3600 IN RRSIG NSEC 5 1 3600 20060920053241 ...  
dnssec.pl.             3600 IN NSEC dnsstuff.pl. NS RRSIG NSEC  
dnssec.pl.              3600 IN RRSIG NSEC 5 2 3600 20060920053241 ...  
;; Query time: 1 msec  
[...]
```

Nowe flagi w nagłówku pakietu DNS

DNSSEC wprowadza następujące nowe flagi:

- **DO**
DNSSEC OK; sygnalizuje, że resolver wspiera DNSSEC;
- **AD**
Authenticated Data; wskazuje, że dane zostały zwalidowane poprawnie
- **CD**
Checking Disabled; bit ustawiony przez resolver, który chce sam dokonać walidacji danych

- Extension Mechanisms for DNS, version 0

system sygnalizujący:

- ✓ wsparcie dla DNSSEC (flaga DO)
- ✓ wsparcie dla pakietów DNS większych niż 512B, do 4096B

- Wsparcie dla DNSSEC jest sygnalizowane w meta rekordzie „OPT”, który jest dołączany przez serwer w sekcji „Additional”

dig wyświetla go jako OPT PSEUDOSECTION

```
[...]  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
[...]
```

- Rozmiar pakietów DNS można kontrolować

```
options {  
    ...  
    edns-udp-size 512;  
}
```

Opcja przydatna w przypadku firewall'i nie przepuszczających pakietów DNS większych niż 512B.

Zabezpieczanie strefy

- Generujemy parę kluczy
dnssec-keygen
- Podpisujemy strefę
dnssec-signzone
- Konfigurujemy serwer do obsługi DNSSEC
 - ✓ options {
...
dnssec-enable yes;
};
 - ✓ trusted-keys
- Sprawdzamy konfigurację i przeładujemy serwer
named-checkzone, named-checkconf
- Publikujemy rekord DS w strefie nadrzędnej

Generowanie pary kluczy

■ Generowanie klucza ZSK (zone signing key)

```
# dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024 -n ZONE dnssec.pl  
Kdnssec.pl.+005+44240
```

■ Generowanie klucza KSK (key signing key)

```
# dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 1024 -n ZONE dnssec.pl  
Kdnssec.pl.+005+33612
```

■ Operacja dnssec-keygen generuje dwa pliki

- ✓ K<name>+<alg>+<id>.key - zawiera klucz publiczny publikowany w pliku strefy
- ✓ K<name>+<alg>+<id>.private - zawiera klucz prywatny

Usage:

```
dnssec-keygen -a alg -b bits -n type [options] name  
[...]  
-a algorithm: RSA | RSAMD5 | DH | DSA | RSASHA1 | HMAC-MD5  
-b key size, in bits:  
-n nametype: ZONE | HOST | ENTITY | USER | OTHER  
name: owner of the key  
[...]  
-f keyflag: KSK  
[...]
```

Output:

```
K<name>+<alg>+<id>.key, K<name>+<alg>+<id>.private
```

Pliki z kluczami

- Zawartość pliku Kdnssec.pl.+005+44240.key

```
# cat Kdnssec.pl.+005+44240.key
dnssec.pl. IN DNSKEY 256 3 5
AQO99gBymVUPXbmgFvVe5K/jVjB7vUqPqS/jXdmdZFsrVzVOMiS/Z+r8
4SlJofJX1bL9zHWu3gNHU0h6p7aGYa2b7OicWMHmlaSGo50MVV/2/XWG
N8g4sQWbWJLZ1v9Ib7re7lIxsmmj9ZCNt8Z9gdEo9OYlwkuMJNiiBiD7
xY/XRw==
```

- Zawartość pliku Kdnssec.pl.+005+44240.private

```
# cat Kdnssec.pl.+005+44240.private
Private-key-format: v1.2
Algorithm: 5 (RSASHA1)
Modulus: vfYAcplVD125oBb1XuSv41Ywe71Kj6kv413ZnWRbEVcl...
PublicExponent: Aw==
PrivateExponent: fqQATGY4tOkmarn46e3K147K/SjcX8Yf7Ok7...
Prime1: 4+gyrtX+DhgbsCBERR/X8tuAUP2+WS7PXx+r6v49b00X3...
Prime2: 1WBh8+ijmWJJtgejlKifgcA+BS3usaPqN+ztTXosMzkhS...
Exponent1: 1/AhyeP+tBASdWrYLyqP9z0ANf5+5h806hUdR1Qo9N...
Exponent2: jkBBTUXCZkGGeVptDcW/q9V+rh6fIRfxep3ziPwdd3...
Coefficient: XhXDaESjum+hR7eFUwX8s7TSO4+oK2VrjQAi0ZTI...
```

Podpisywanie strefy 1

- W pliku strefy podpisywane są tylko dane autorytatywne
- Rekord NSEC oraz DS należą do danych autorytatywnych strefy
- Rekordy „glue” (A) oraz rekordy NS w punkcie delegacji (zone cut) nie są podpisywane - nie są danymi autorytatywnymi

Podpisywanie strefy 2

- Umieszczamy klucze w pliku strefy

```
@           IN      SOA      stargate.nask.waw.pl.  dnsmaster.nask.pl. (
                                2006070601
                                7200
                                1800
                                2592000
                                3600
                                )

;; ZSK public key, inserted 20060706
$include Kdnssec.pl.+005+44240.key
;; KSK public key, inserted 20060706
$include Kdnssec.pl.+005+33612.key

           IN      NS      stargate.nask.waw.pl.
           IN      MX      10 mail.dnssec.pl.

[...]
```

- Zwiększamy numer seryjny o 1
- Sprawdzamy czy plik nie zawiera błędów
named-checkzone

Podpisywanie strefy 3

■ Podpisujemy strefę

```
# dnssec-signzone \  
> -r /dev/random \  
> -o dnssec.pl \  
> -k /var/named/Kdnssec.pl.+005+33612.key \  
> pl.dnssec \  
> /var/named/Kdnssec.pl.+005+44240.key  
pl.dnssec.signed
```

Usage:

```
dnssec-signzone [options] zonefile [keys]  
[...]  
-g:      generate DS records from keyset files  
-s [YYYYMMDDHHMMSS|+offset]:  
        RRSIG start time - absolute|offset (now - 1 hour)  
-e [YYYYMMDDHHMMSS|+offset|"now"+offset]:  
        RRSIG end time - absolute|from start|from now (now + 30 days)  
-i interval:  
        cycle interval - resign if < interval from end ( (end-start)/4 )  
-o origin:  
        zone origin (name of zonefile)  
-r randomdev:  
        a file containing random data  
-k key_signing_key  
keyfile (Kname+alg+tag)
```

Podpisywanie strefy 4

- Narzędzie `dnssec-signzone` podczas podpisywania strefy generuje dwa pliki:

- ✓ `dsset-<domena>`

Plik "dsset" zawiera rekordy DS odnoszące się do kluczy KSK opublikowanych w strefie

- ✓ `keyset-<domena>`

Plik "keyset" zawiera klucz KSK opublikowany w strefie.

- Zawartość pliku "dsset"

```
# cat dsset-dnssec.pl.  
dnssec.pl.          IN DS 33612 5 1  
8407ED418EB46545A63B57F1B2DA07F3B63B4B11
```

- Zawartość pliku "keyset"

```
# cat keyset-dnssec.pl.  
$ORIGIN .  
dnssec.pl          3600   IN DNSKEY 257 3 5 (  
                    AQO+awA1AFkhSgbabKY1b26zA//oxJkGJMET  
                    wR2Mp71e7PzHyIqFiqQ4uCTPgSwruCFHI1oX  
                    Ip36suR3PTiwj6KCAIZBRDC7s+dWwYdBfTrE  
                    X+z25DAqQLV6GKrmLIM0bO5f40xda8ap81Pl  
                    GBgHgwRNqyrQ44/2768AnDRHA4Rrzw==  
                    ) ; key id = 33612
```

Publikowanie podpisanej strefy

- Edytujemy named.conf

- ✓ modyfikujemy dyrektywę zone

```
zone "dnssec.pl" {  
    type master;  
    file "master/pl.dnssec.signed";  
    allow-transfer { key master-slave.dnssec.pl; };  
};
```

- ✓ instruujemy serwer, aby wspierał dnssec

```
options {  
    ...  
    dnssec-enable yes;  
}
```

- Sprawdzamy składnię pliku named.conf

```
named-checkconf
```

- Przeładujemy serwer

- Test

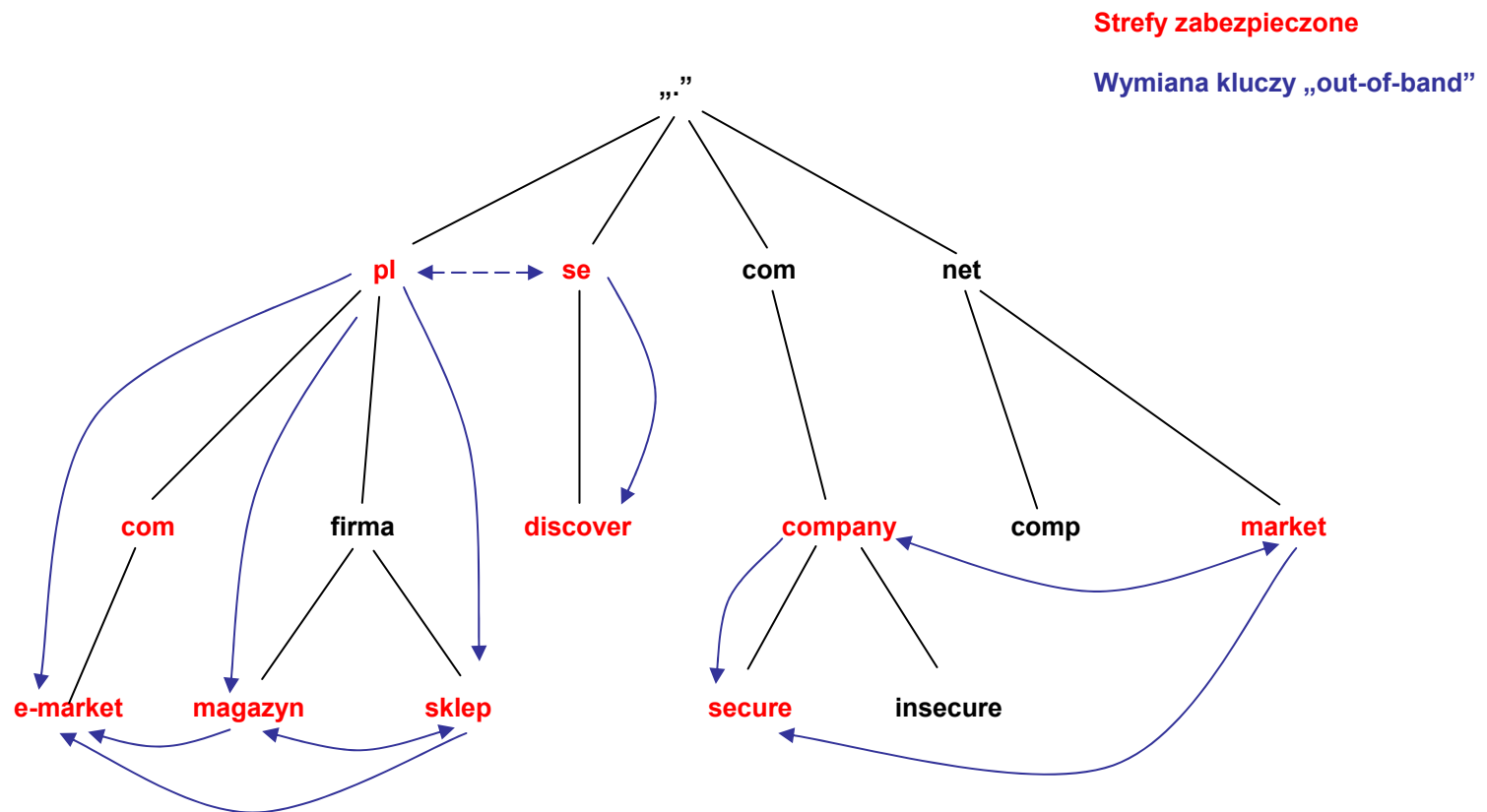
```
dig SOA dnssec.pl. @localhost +dnssec
```

Przegotowanie resolvera

- W celu weryfikacji danych z zabezpieczonej strefy, której ufamy, musimy poinstruować nasz serwer, aby ufał kluczowi z tej strefy
- Wymiana kluczy między administratorami zabezpieczonych stref powinna odbywać się w sposób bezpieczny, np. przy użyciu PGP.
- Klucz, któremu chcemy ufać, należy podać w dyrektywie trusted-keys edytujemy plik named.conf

```
trusted-keys {  
    dnssec.pl. 257 3 5 "AwEAAaxPMcR2x0HbQV4WeZB6oEDX+r0QM65KbhTjrW1Z  
    ...  
    WR8BW/hWdzOvnSCTh1Hf3xiYleDbt/o10TQ09A0=";  
};
```

Wyspy bezpieczeństwa



Łańcuch zaufania

- Ufamy danym podpisanym przez ZSK
- Możemy zaufać ZSK jeśli jest podpisany przez KSK
- Ufamy KSK, jeśli jest wskazany przez rekord DS w strefie nadrzędnej
- Ufamy rekordowi DS jeśli jest podpisany przez ZSK, itd.
- Jeśli trafimy na klucz (SEP - Secure Entry Point), któremu ufamy (tzn. jest zapisany w pliku named.conf, dyrektywa trusted-keys), to oznacza, że zbudowaliśmy łańcuch zaufania i dane są zweryfikowane.

Zarządzanie kluczami

- Używaj kluczy ZSK i KSK - łatwiejsza wymiana kluczy.
 - ✓ ZSK podpisuje autorytatywne rekordy w strefie
 - ✓ KSK podpisuje tylko rekordy DNSKEY; zestaw rekordów DNSKEY będzie posiadał co najmniej dwa podpisy, jeden wygenerowany kluczem ZSK, drugi - kluczem KSK.
- Większy klucz lepszy - bardziej bezpieczny
 - ✓ większe klucze, to większe pliki stref - większe podpisy
 - ✓ dłuższy czas podpisywania strefy i weryfikowania odpowiedzi
- Używaj mocnego KSK oraz mniejszy ZSK lecz częściej wymieniany
- Rekord DS wskazujący na klucz KSK musi być dostarczony bezpiecznym kanałem jednostce zarządzającej strefą nadrzędną
- Podpisuj regularnie strefę, nie dopuść do wygaśnięcia podpisów
- W regularnych odstępach wymieniaj klucze - „key rollovers”

Wymiana kluczy

- Wymiana klucza ZSK, metoda „pre-publish”
 1. Wygeneruj klucz ZSK
 2. Opublikuj go w strefie; mamy dwa ZSK, jeden aktywny, drugi „pasywny”
 3. Czekaj, aż nowy klucz rozpropaguje się (TTL)
 4. Podpisz strefę nowym kluczem, nie usuwaj starego klucza
 5. Czekaj na propagację nowych danych i expirację starych.
 6. Usuń stary klucz

- Wymiana klucza KSK, metoda „double signature”
 1. Wygeneruj nowy KSK
 2. Podpisz strefę dwoma kluczami KSK (starym i nowym)
 3. Dodaj nowy rekord DS w strefie nadrzędnej
 4. Czekaj na propagację nowego rekordu DS i klucza KSK w sieci
 5. Usuń stary rekord DS
 6. Czekaj na expirację usuniętego rekordu DS
 7. Usuń stary klucz KSK

Wpływ DNSSEC na środowisko DNS

- Wzrost wysycenia łącz od 2 do 3 razy
- Średni rozmiar pakietu UDP większy ok. 3 razy
- Zużycie pamięci wirtualnej od 2 do 4 razy większe
- Znaczący wzrost rozmiaru pliku strefy
dla klucza o długości 1024 plik dla strefy .pl zwiększy rozmiar z 17MB do 120MB
- Serwowanie strefy podpisanej nie powoduje większego obciążenia procesora

KONIEC