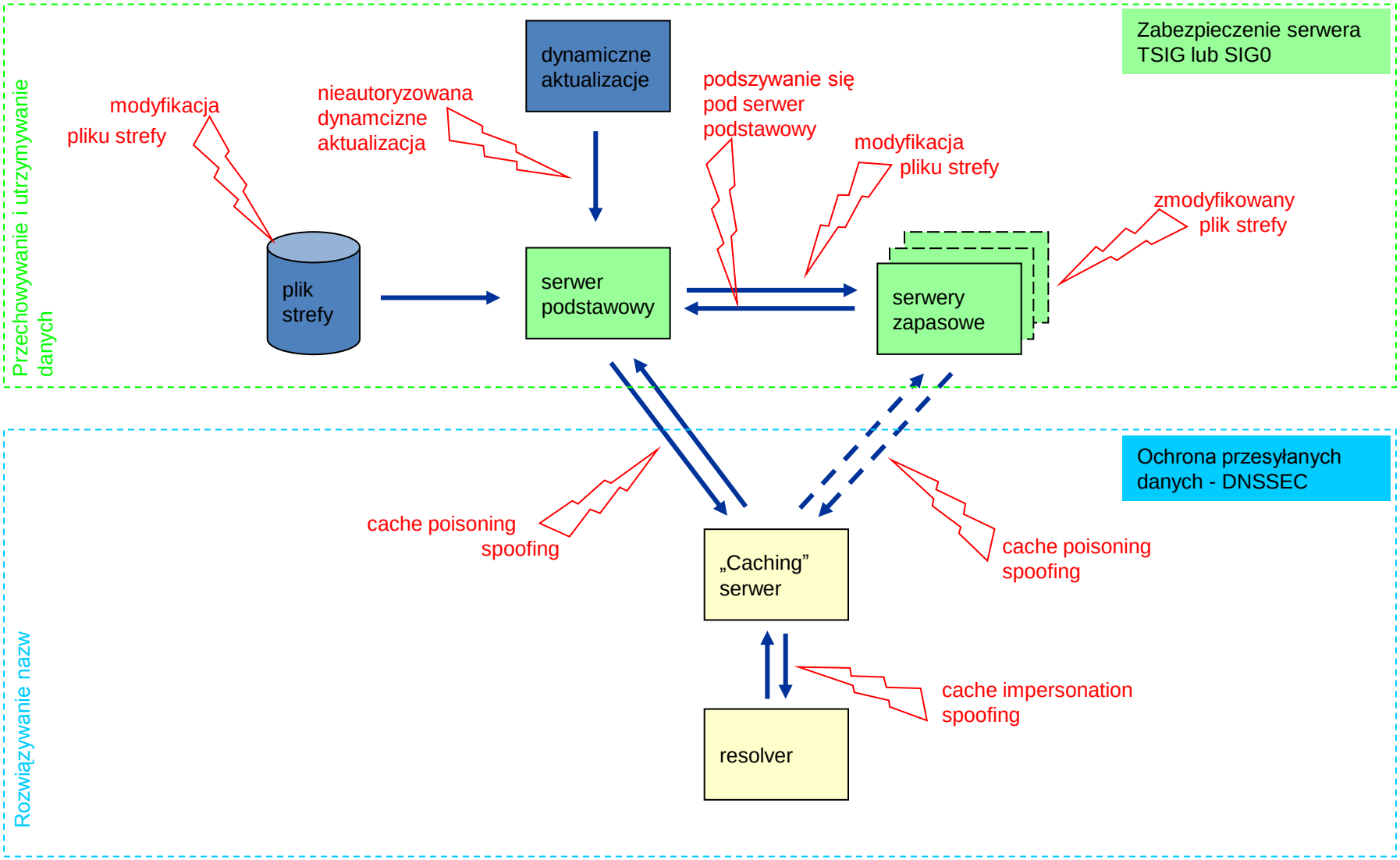
NASK

DNSSEC

Zbigniew Jasiński

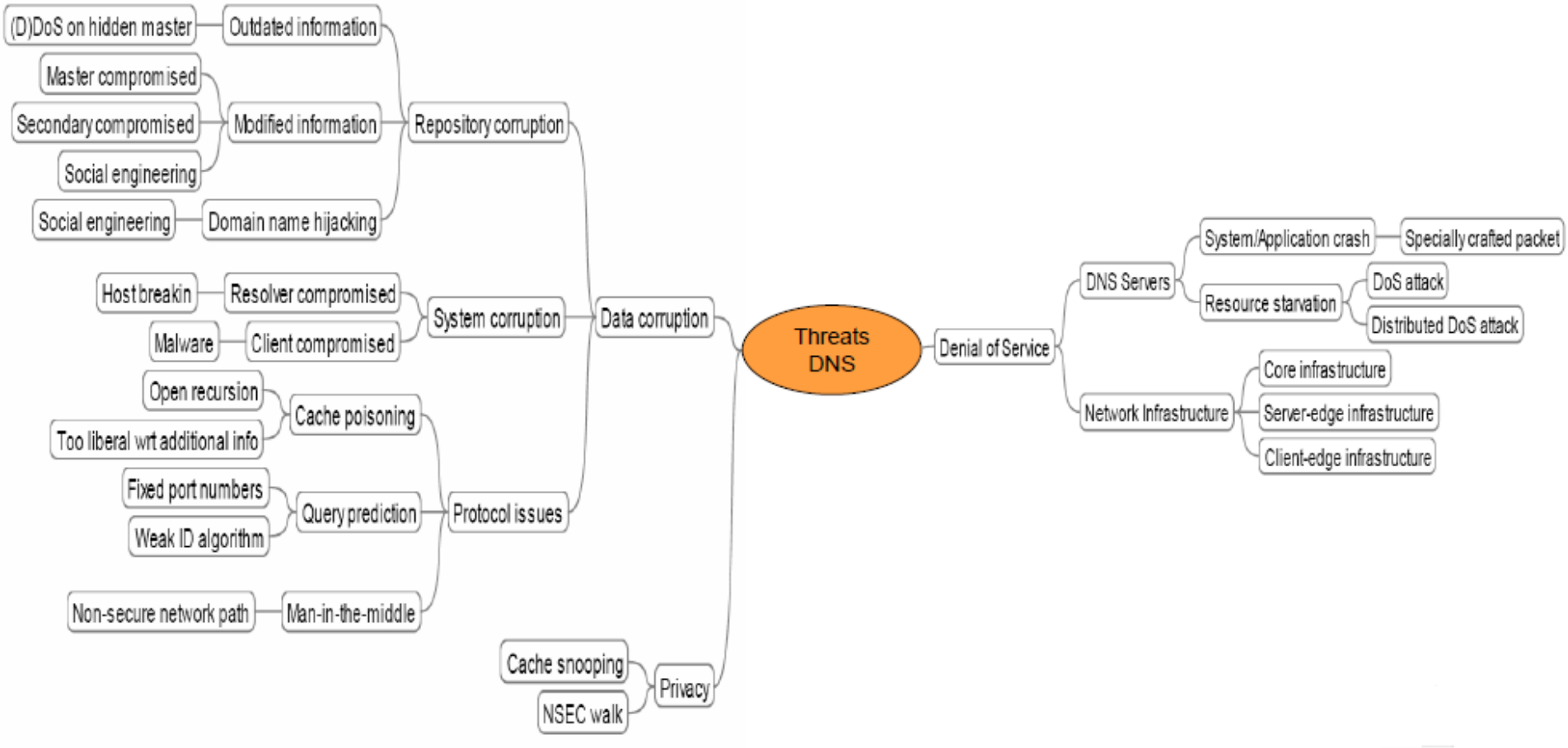
NASK

Przegląd zagrożeń związanych z DNS



NASK

Przegląd zagrożen związanych z DNS



DNSSEC Experiences of .SE
Anne-Marie Eklund Löwinder

NASK

Przepływ danych

- Odpowiedzi przychodzą na ten sam port UDP z którego zostały wysłane
- Sekcja ‘question’ duplikowana w odpowiedzi zgadza się z tą z zapytania
- Query ID odpowiedzi zgadza się z QID zapytania
- Sekcje ‘authority’ i ‘additional’ zawierają nazwy domenowe znajdujące się w domenie z zapytania

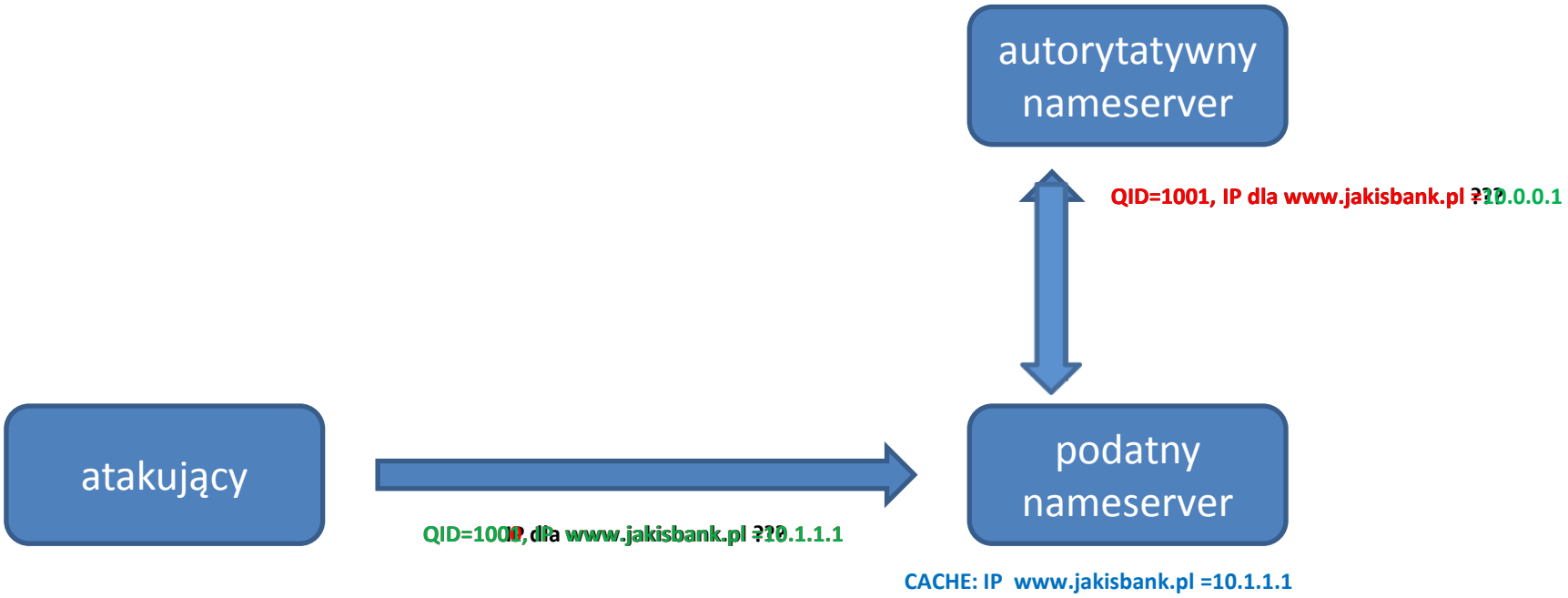
NASK

Przepływ danych

- Problem:
  - QID = 16bit
- Obejście problemu:
  - Randomizacja portów

Przegląd zagrożeń związanych z DNS

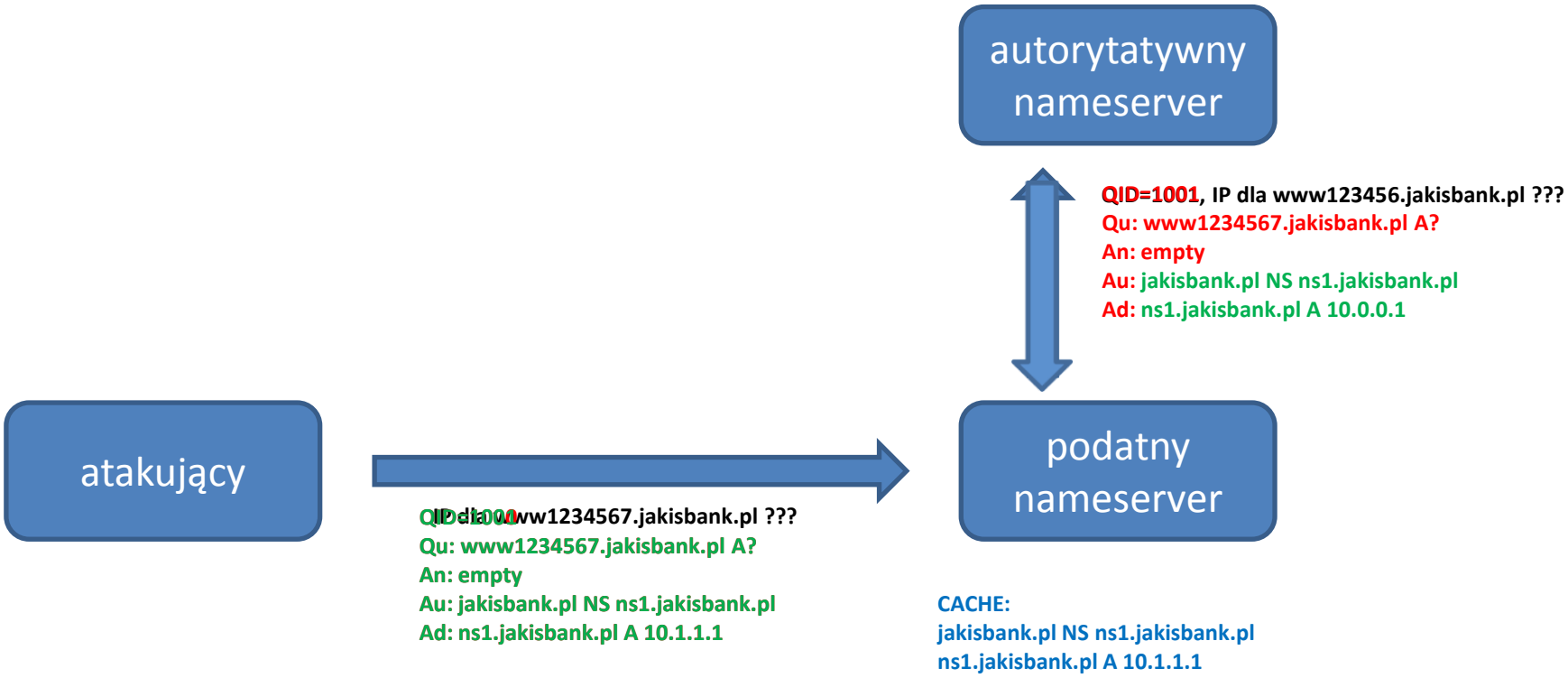
- Cache poisoning



NASK

Przegląd zagrożeń związanych z DNS

- Kaminsky bug



NASK

Co nam daje DNSSEC

- Zapewnia integralność odpowiedzi DNS
- Daje możliwość weryfikacji odpowiedzi negatywnych
- Nie szyfruje danych w pakietach DNS

NASK

Jak działa DNSSEC

- DNSSEC opiera się na kryptografii kluczy asymetrycznych
- Zabezpieczona strefa posiada swój klucz prywatny i klucz publiczny
- Klucz prywatny wykorzystywany jest do podpisywania danych przechowywanych w DNS
- Klucz publiczny jest używany do weryfikacji podpisanych danych i jest publikowany w zabezpieczonej strefie

NASK

Nowe rekordy DNS

- DNSKEY – rekord zawiera klucz publiczny do weryfikacji podpisów (rekordów RRSIG)
- RRSIG – podpis grupy rekordów
- NSEC/NSEC3 – umożliwia weryfikację informacji o nieistnieniu rekordu lub o braku zabezpieczeń
- DS – wskazuje na klucz podpisujący dane w strefie podrzędnej

NASK

Nowe flagi w nagłówku pakietu DNS

- DNSSEC wprowadza następujące nowe flagi:
  - DO, DNSSEC OK, sygnalizuje że resolver wspiera DNSSEC
  - AD, Authenticated Data, wskazuje ze dane zostały sprawdzone i są poprawne
  - CD, Checking Disabled, bit ustawiany przez resolver który sam chce dokonać sprawdzenia danych

NASK

Rekord DNS a zestaw rekordów (RRset)

- Pojedynczy rekord DNS

```
f-dns.pl.               86400   IN      A       217.17.46.189
f-dns.pl.               86400   IN      AAAA    2001:1a68:0:10::189
```

- Zestaw rekordów

```
pl.                     86400   IN      NS      a-dns.pl.
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      h-dns.pl.
pl.                     86400   IN      NS      i-dns.pl.
```

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

Rekord DNS a zestaw rekordów (RRset)

```
pl.                     86400 IN NS c-dns.pl.
pl.                     86400 IN NS g-dns.pl.
pl.                     86400 IN NS d-dns.pl.
pl.                     86400 IN NS f-dns.pl.
pl.                     86400 IN NS i-dns.pl.
pl.                     86400 IN NS a-dns.pl.
pl.                     86400 IN NS e-dns.pl.
pl.                     86400 IN NS h-dns.pl.
pl.                     86400 IN RRSIG NS 10 1 86400 20110107151429 (
                                20101208141429 34730 pl.
                                quiuKJC7+pZw1gdaqUMB0mkHYLm1Yor777wYxQI/EhIt
                                0agtl+e56rdt9ii1Yp6SB2/qdqbYAWepAv3PI52/5Ouv
                                9Px+YlsrewH9+mg6v1xI/9MuA/WMl1nml+QOsBVT2071
                                mOeGRI+7A5YhhXU3smLSwtQ2mVPRc0SQBnSb6V0C/L+4
                                nZ/S2hJwnrhN675QTSxSGXLDR4VKM3fcewd+jz2AB1LD
                                VrFUwaJcu+L2QJ++LyipiKkMrCzcpgSTal8laFeODNHZ
                                rJyr4ZGV3/JfEkCW5tQGMxlc0GhXwtIm8QutqVJ1zKOa
                                9/8T78MbH29sUWvGgzZisJM8l1rG5DoWeg== )
pl.                     86400 IN TXT "ccTLD of Poland"
pl.                     86400 IN RRSIG TXT 10 1 86400 20110107151429 (
                                20101208141429 34730 pl.
                                jAqvWx+S/T76AlsnOEyw2shph3efCxY4ImgpWGaFEYHF
                                vu574ZA4T24aMP6IcA0zSdzTpTNlbQIUzmSSd6RZAH7Q
                                N1HK++2svsUmJeRPgxwxMY/3k5X0I23XqkGwVUExlVeX
                                1+CJ6FFaSJNvt3uKR6jn2OZk9rSQhw0/nh0L8TEtChpx
                                sR4GpWXLedW3wG9yLKpMvdYC4bphltrQlVRx7fsFLCQk
                                8dvEszthwPVLKYuDNqKXK7tVtIcPfTwhDF6i6p+bFSfP
                                kiIVaI7CZ8/7VVdlHp6JDwNHIg5zI2p1p0tmmIQ/LZsi
                                0yXVnMKLxEucvSOnyfL2GwZGHAQ2IDPQ9Q== )
```

Podpisany zestaw rekordów

Podpisany pojedynczy rekord

NASK

Klasyczna odpowiedź

```
dig @dnssec.nask.waw.pl dnssec.pl ns

; <<>> DiG 9.7.1-RedHat-9.7.1-11.P2.fc13 <<>> @dnssec.nask.waw.pl dnssec.pl ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39618
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnssec.pl.                     IN      NS

;; ANSWER SECTION:
dnssec.pl.              3600    IN      NS      ns2-dnssec.nask.waw.pl.
dnssec.pl.              3600    IN      NS      ns1-dnssec.nask.waw.pl.

;; Query time: 4 msec
;; SERVER: 193.59.201.189#53(193.59.201.189)
;; WHEN: Mon Jan 17 14:03:26 2011
;; MSG SIZE  rcvd: 86
```

NASK

Podpisana odzpowiedź

```
dig @dnssec.nask.waw.pl dnssec.pl ns +dnssec +multi

; <<>> DiG 9.7.1-RedHat-9.7.1-11.P2.fc13 <<>> @dnssec.nask.waw.pl dnssec.pl ns +dnssec +multi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4721
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec.pl.          IN NS

;; ANSWER SECTION:
dnssec.pl.          3600 IN NS ns1-dnssec.nask.waw.pl.
dnssec.pl.          3600 IN NS ns2-dnssec.nask.waw.pl.
dnssec.pl.          3600 IN RRSIG NS 10 2 3600 20110216103018 (
                    20110117103018 7172 dnssec.pl.
                    ZnjFy7PElfGL+J1MDM6CpHP5jPbyMZ1STvNM3iRQ4KHT
                    s1AtYfIMFLH10rLB1KYr6g1/rup1AK+Or+jWm86GBc5S
                    QO4HtHZseeVJq+SZFrz4p6hsvwEXpXh8e4ykxJJHF7Mi
                    qXN2leRMdjkXU7Czcxm2QYDAEmFRMito8DFAStkxKr2V
                    IA/KLZu11937zO0xcEqgNdXBXhakZuVDRqPMSQu/PgK6
                    RkhkBlJ4UNl20LIbj+x77nz/hX3ix744fEvGdq/tCxvm
                    phmK2dW14cAxMfRv+cM50SB9HqxCZfgk77SJpbqOMnyR
                    MUSZRIGJW3mxAYRKWypTgtkE8S76awj7dQ== )

;; Query time: 4 msec
;; SERVER: 193.59.201.189#53(193.59.201.189)
;; WHEN: Mon Jan 17 14:04:31 2011
;; MSG SIZE  rcvd: 394
```

NASK

Odpowiedź na zapytanie o klucze

```
dig @dnssec.nask.waw.pl dnssec.pl dnskey +dnssec +multiline

; <<>> DiG 9.7.1-RedHat-9.7.1-11.P2.fc13 <<>> @dnssec.nask.waw.pl dnssec.pl dnskey +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47722
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec.pl.          IN DNSKEY

;; ANSWER SECTION:
dnssec.pl.          3600 IN DNSKEY 257 3 10 (
                    AwEAAeKv8BMj9yNBGDYDPFCEI1ufEQRTlrvSlLWXxn0H
                    gK8mss3cjwGXBuFoXsd8sxV9lxBwWx4uSgu3Mvs1NPOz
                    WKTSP4+Eh4c04ZU6zfVvsK6rumXLIehevFHtf9V2x0tp
                    2PorI5jAqCeT3tRuIgvgoPJEpCxdUXZoMWTZSHGx0Qvk
                    6XkzTvIhKdi6ZHFPcXm5ckCaeIu2iYGCEVtRVu2ixG1O
                    QwCCMk8YNHUQTjwNAKC+yfq30gE3FGyNHkxRW6ZapaDz
                    ZGLNMo3j+XMb1NXjhsewMjfLQUxIO42z6Giog+cXqP8X
                    sOJfvLc/u0uiJZjhRlWPbiusiBFcQSurAHUSEtsUSqo3
                    7pX5zaychvyjn96X3JGS6bgs961xNmPAhWmZi68oXvyV
                    ipz3ztHDVqYwZjR55CgSsY6/nPX+xzBl2hMsqYTJIZr1
                    LvPLafkpgoIK1W/n/4tj5O/p4sZzK/WLZnwvRBw4P7/l
                    FRnwt/0MYxbA+iVdXD2EmWN0d3ji+OM8NJY+Cy1JCDUP
                    YBPBcUwyjnNoZy+uTJLROsvZCpQvtSZmwpvsH+FvDtxl
                    OlHiD90qJxy1zsozG4t5RMeDIYikX/Fmd0aLBeMSATt7
                    Ywv8lami5yYVtTnJ+fDbIWkjDTYSgvtLls41Aqyd15OG
                    AIPcWr5IEehp5ydOYJXP86TK5aqZ
                    ) ; key id = 24414
dnssec.pl.          3600 IN DNSKEY 256 3 10 (
                    AwEAAcomRg1LF8yIpQKKsholZIG4QjwOPE9reUyOJu6z
                    7ZQhk3GnAVByLVnpdzES4Xywrd0q8nKTKHBYmhBajXqf
                    rkuocxmG12FJ6qiFBaW7xHh+GElbW5SAL5xmdllLyVYx
                    aEAeWHnB5zrimYgOSth26Cu6jv9HlZhhdvH4y1sW5Efj
                    +pKSxfs6PiD+7LZ+kAjdXXDNMEInOfw8xMSUQeucztg7
                    XbhQ8vW27eeRB3A0LAZhZfxdPBk23TMj8pLoZakcSEL+
                    O19aIq1JF9/gi/rT0ZD0GTKYqzqClOmdVGv9DqzqDEmA
                    wbnVagVKwe/3gPrmQ2oBRO9SLaWSR99fTHgO87s=
                    ) ; key id = 7172
```

Odpowiedź na zapytanie o klucze

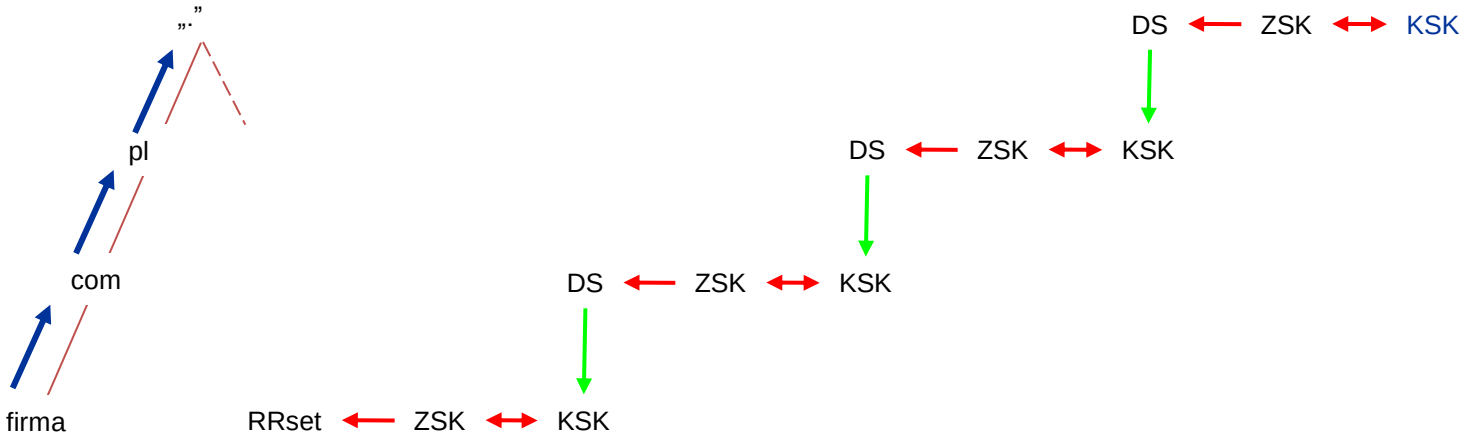
```
dnssec.pl.      3600 IN RRSIG DNSKEY 10 2 3600 20110216103018 (
                20110117103018 7172 dnssec.pl.
                Cwz29zGtlUGzuUSFQ0JhLeK+IJfCJlHjkcr/ncWID0to
                cJyhsaXbT5hjQzRtQCo7ymOKxTNbYPO10tAlfpHwxn82
                Z9RowQLjrTd9bINdO+ouK3dudhoBX6k+cYlyd+yRyRxB
                oQ8VY8fTbkDQxFpR/DhRMZBvlRlEoizkVQJMkRuIxk++
                l+kIU51/TmUdSAOjO6Wz+10Dw8HO1v1St0XmkgPO1R77
                okwZ1bXzqymOF50sn7yjDKPRO2W8djzEyW0oONRNmJFY
                7nk6bjzNK0i7lx6VHhVlMqYvSeMJ6Fy0D9uBPm3x2TzM
                zuRbRWzWEqc4WfM/+cA9kNDbcoEhJrF0sw== )
dnssec.pl.      3600 IN RRSIG DNSKEY 10 2 3600 20110216103018 (
                20110117103018 24414 dnssec.pl.
                Yt/OeLu9bcu9OOUpWHPQMFuEwL38eHhgGYK0BpMlv2bv
                p1adZb2uK8c1n6K82jvCzt7V04Va8w1TuG1QNxhBCh3a
                VbZMtoPZiHzDF6Upn+JqfVCaUcADLlnSULGGrw1NDqqS
                D86XrXExlkS0dfhGh2B47gE9WfZ3fB36O99GJO/KpQIi
                Khw7pg+S3e6DK8xTFXFujTD/CTi/YNHJoBeN/iYNL+zA
                GNAbyZKyhRhMV1wQkVgE5FeeGOwsD83nEZDolrew1Mvw
                SeC4qJBfD4ctUBB51kDnMM2/NPDvQNhtynLi/WW+gcI3
                1KgLAb+whhjitXBNSaGYUPAms0gU7MYIGxv7dNrkLUex
                qARSNjh91Lz17ADwDpcKyZavE7VB7Kg0o2z7f0QpWCEg
                NoLVz+9ZzkgTNGxzlhy4awYN7XF+jGdZM5/ccp2LK/Og
                3vvsnuTmKwneaWfnEtm5c+d5BNVuk6rRLIM2b11ZmSOa
                as3+CmEoXwvBIVBIHdHDnToo7Gj/uRNEgGndnvYWQKbr
                ESfSUgIw2l3kNlD1RHl5EBytU0c3wvu3WyasLIp5Yr0v
                fjQw7UWjrboPtd9vwqTArLHplSoioAb+GUmzb0Gnilvq
                adtZtdYoF/tutEKYqgG3Le5s+DpBITFPG/6xXWsRPOO/
                tlzFfUqh7MBto/H2RQIf7T0= )

;; Query time: 5 msec
;; SERVER: 193.59.201.189#53(193.59.201.189)
;; WHEN: Tue Jan 18 10:23:14 2011
;; MSG SIZE  rcvd: 1696
```

NASK

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 ze strefy nadrzędnej jeśli jest podpisany przez klucz KSK z tej strefy, itd.
- Jeśli trafimy na klucz SEP (Secure Entry Point), któremu ufamy (jest zapisany w pliku konfiguracyjnym) to oznacza, że zbudowaliśmy łańcuch zaufania i dane są zweryfikowane poprawnie.

DNSSEC - wprowadzenie



ZSK - Zone Signig Key

KSK - Key Signing Key

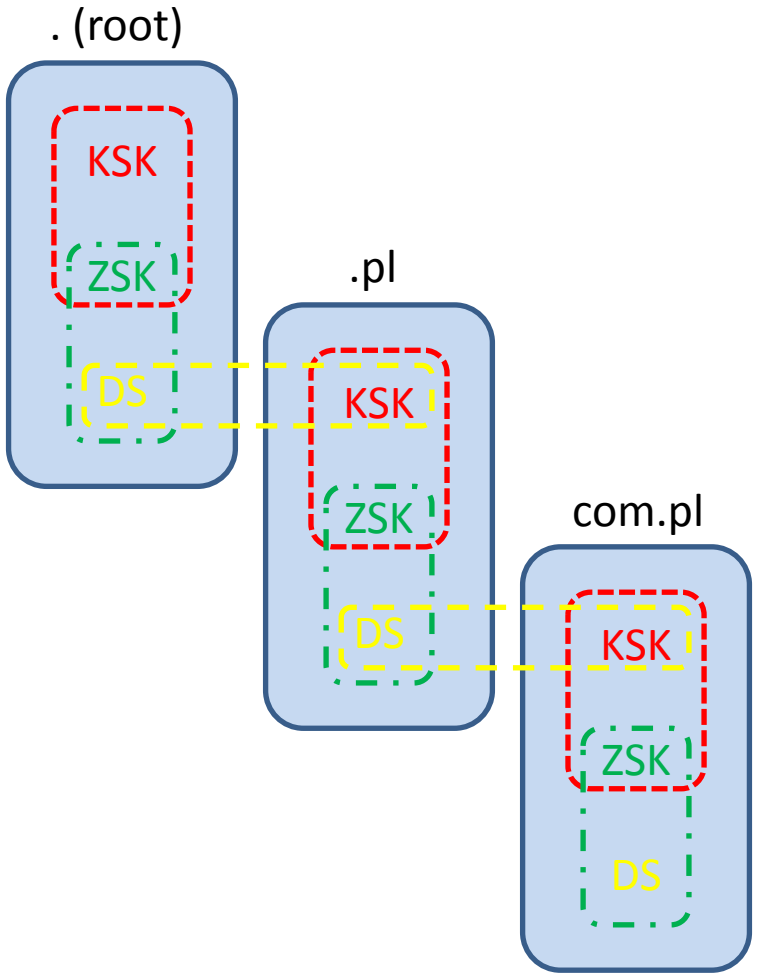
kierunek podpisywania rekordów DNS

wskazania rekordów DS na klucz w strefie podrzędnej

kierunek weryfikacji

NASK

Łańcuch zaufania



NASK

DNSSEC – problemy techniczne

- Zwiększony rozmiar odpowiedzi
- Większy plik strefy
- Weryfikowanie podpisów (obciążenie resolverów)
- Przechowywanie materiału kryptograficznego w bezpieczny sposób
- Oprogramowanie wspierające DNSSEC’a
- Narzędzia do zarządzania kluczami
- Monitorowanie podpisanej strefy

NASK

DNSSEC – problemy administracyjne

- Role (oficer bezpieczeństwa, operator)
- Ujednolicony model między Registrarami
- Implementacja DNSSEC’a u ISP
- Specjalistyczna wiedza wymagająca szkoleń

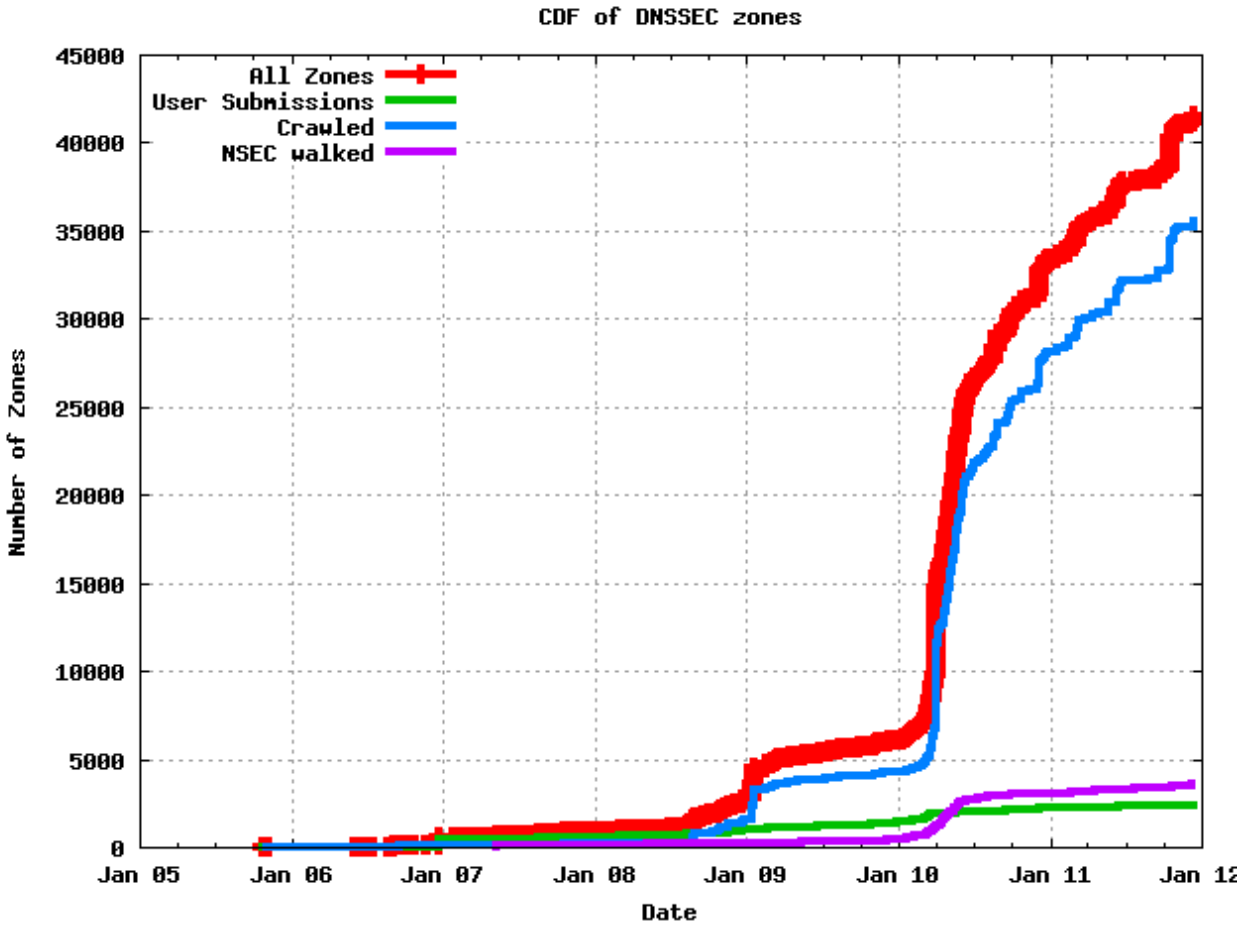
NASK

Wdrożenie na świecie

W chwili obecnej 73 rekordów DS znajduje się w strefie root: **.ac** (Ascension Island), **.ag** (Antigua and Barbuda), **.am** (Armenia), **.arpa**, **.asia**, **.at** (Austria), **.be** (Belgium), **.bg** (Bulgaria), **.biz**, **.br** (Brazil), **.bz** (Belize), **.cat** (Catalan community), **.ch** (Switzerland), **.cl** (Chile), **.co** (Colombia), **.com**, **.cr** (Costa Rica), **.cz** (Czech Republic), **.de** (Germany), **.dk** (Denmark), **.edu**, **.eu** (European Union), **.fi** (Finland), **.fr** (France), **.gi** (Gibraltar), **.gl** (Greenland), **.gov**, **.gr** (Greece), **.hn** (Honduras), **.in** (India), **.info**, **.io** (British Indian Ocean Territory), **.jp** (Japan), **.kg** (Kyrgyzstan), **.kr** (Korea, Republic Of), **.la** (Lao People's Democratic Republic), **.lc** (Saint Lucia), **.li** (Liechtenstein), **.lk** (Sri Lanka), **.lu** (Luxemburg), **.me** (Montenegro), **.mm** (Myanmar), **.mn** (Mongolia), **.museum**, .**my** (Malaysia), **.na** (Namibia), **.nc** (New Caledonia), **.net**, **.nl** (Netherlands), **.nu** (Niue), **.nz** (New Zealand), **.org**, **.pl** (Poland), **.pm** (Saint Pierre and Miquelon), **.pr** (Puerto Rico), **.pt** (Portugal), **.re** (Reunion), **.sc** (Seychelles), **.se** (Sweden), **.sh** (Saint Helena), **.si** (Slovenia), **.su** (Russian Federation), **.sx** (Sint Maarten, dutch Part), **.tf** (French Southern Territories), **.th** (Thailand), **.tm** (Turkmenistan), **.tw** (Taiwan), **.ua** (Ukraine), **.ug** (Uganda), **.uk** (United Kingdom), **.us** (United States), **.wf** (Wallis and Futuna), **.yt** (Mayotte)

NASK

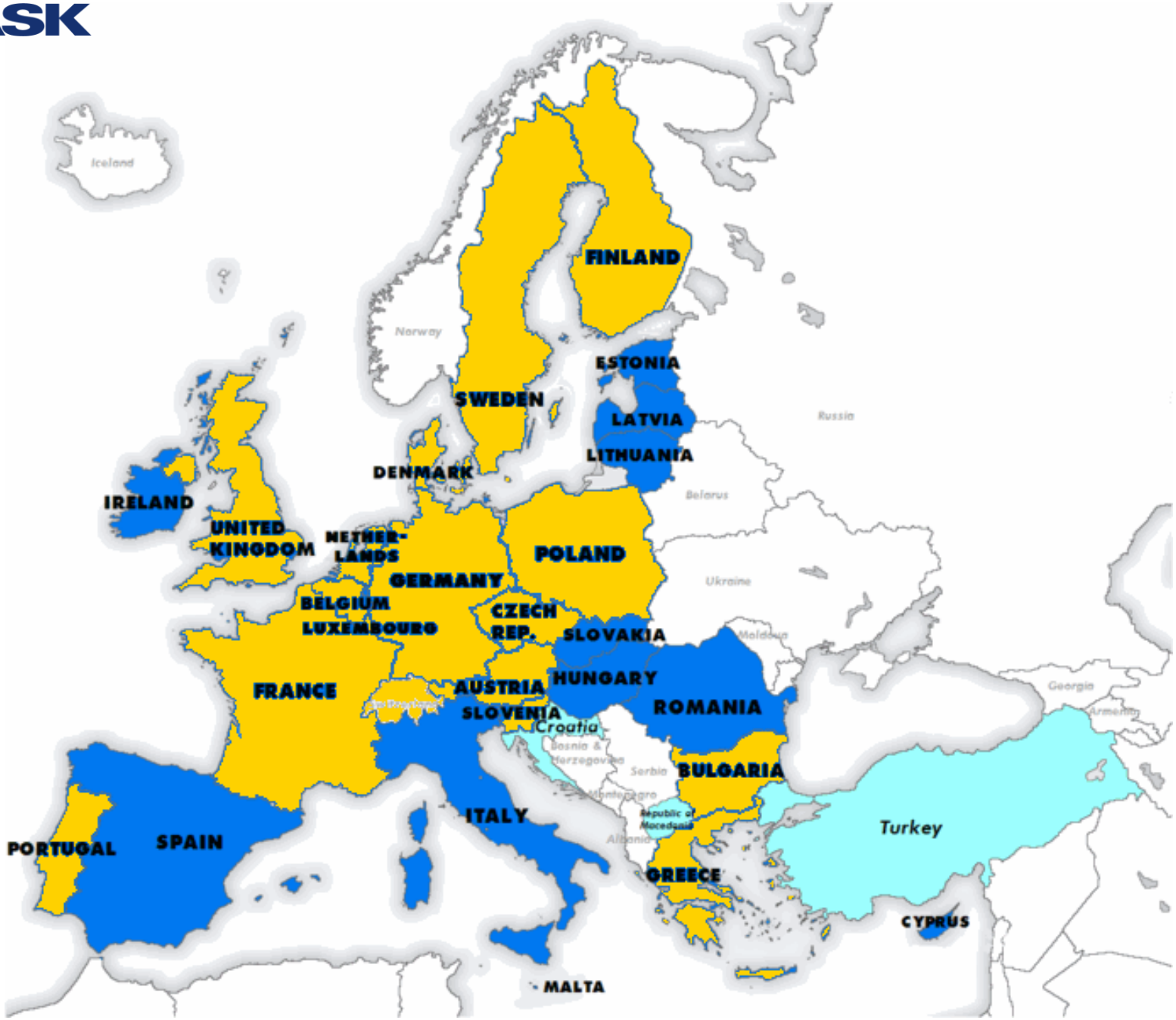
Wdrożenie na świecie



http://secspider.cs.ucla.edu/

SecSpider the DNSSEC Monitoring Project

NASK

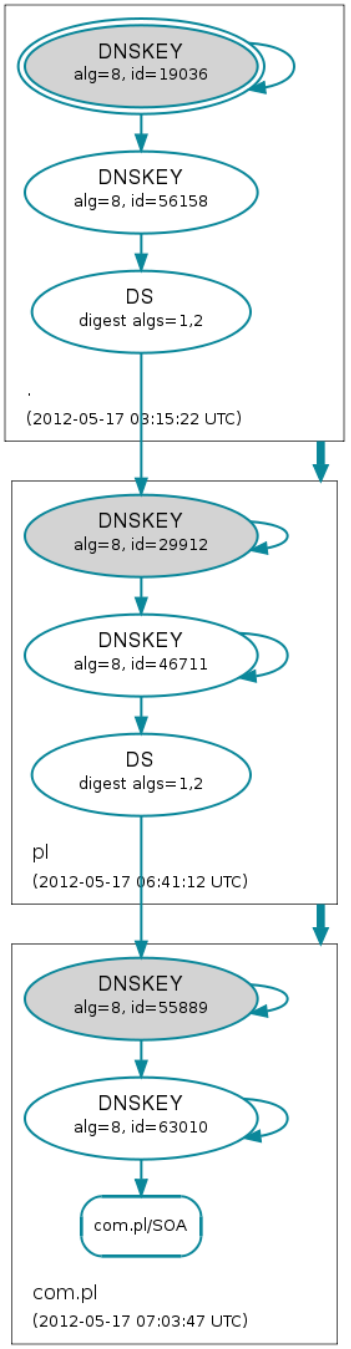

Iceland
Norway
FINLAND
ESTONIA
SWEDEN
LATVIA
Russia
LITHUANIA
DENMARK
Belarus
IRELAND
UNITED KINGDOM
NETHER-LANDS
POLAND
GERMANY
Ukraine
BELGIUM
LUXEMBOURG
CZECH REP.
SLOVAKIA
Moldova
FRANCE
AUSTRIA
HUNGARY
Georgia
SLOVENIA
ROMANIA
Croatia
Bosnia & Herzegovina
Serbia
BULGARIA
Montenegro
Republic of Macedonia
ITALY
Turkey
Albania
PORTUGAL
SPAIN
GREECE
CYPRUS
MALTA

NASK

Narzędzia

- DNSViz (http://dnsviz.net/)

Sandia National Laboratories



NASK

Narzędzia

- ZoneCheck (http://www.zonecheck.fr/), wersja command line oraz CGI/WEB, licencja GPL przygotowana przez Rejestr .fr
- DNSCheck (http://dnscheck.iis.se/), wersja comman line orac CGI/WEB, licencja GPL przygotowana przez Rejestr .se
- DNSSEC Validator (http://www.dnssec-validator.cz/), plugin do FireFox'a przygotowana przez Rejestr .cz

NASK

Uruchomienie DNSSEC (BIND)

- Włączenie DNSSEC na serwerach autorytatywnych

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

- Wymagane: BIND skompilowany z obsługą OpenSSL

NASK

Uruchomienie DNSSEC (BIND)

- Włączenie walidacji DNSSEC na resolverach

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

- Walidacja odbywa się na serwerach rekursywnych, a nie autorytatywnych

NASK

Generowanie kluczy

- Generowanie klucza ZSK

```
dnssec-keygen -r /dev/urandom -a RSASHA512 -b 1024
 -n ZONE zonename
```

- Używamy algorytmu RSASHA512
- Długość klucza 1024

NASK

Generowanie kluczy

- Generowanie klucza ZSK

```
dnssec-keygen -r /dev/urandom -a RSASHA512 -b 1024
 -n ZONE zonename
```

- Tworzy 2 pliki
  - Kzonename+<alg>+<ID>.key
  - Kzonename+<alg>+<ID>.private

NASK

Generowanie kluczy

- Generowanie klucza KSK

```
dnssec-keygen -r /dev/urandom -a RSASHA512 -b 4096
 -n ZONE –f KSK zonename
```

- Używamy algorytmu RSASHA512
- Długość klucza 4096
- Klucz KSK z ustawionym bitem SEP

NASK

Podpisanie strefy

- Dodanie rekordó w RRSIG, NSEC3

```
dnssec-signzone -r /dev/urandom –A -n 4 -g -a -H 10
    -3 baababcd -K eee/ -d dssets/ -S pl
```

- Opcje:
  - -A NSEC3 optout
  - -n CPU num
  - -g update rekordów DS.
  - -a weryfikacja sygnatur
  - -H iteracje NSEC3
  - -3 NSEC salt
  - -K katalog zawierający klucze
  - -d katalog zawierajacy rekordy DS.
  - -S smart signing

NASK

Pytania?

szopen@nask.pl