Network Infrastructure Security
Network Security
DNSSec

Boldizsár Bencsáth PhD

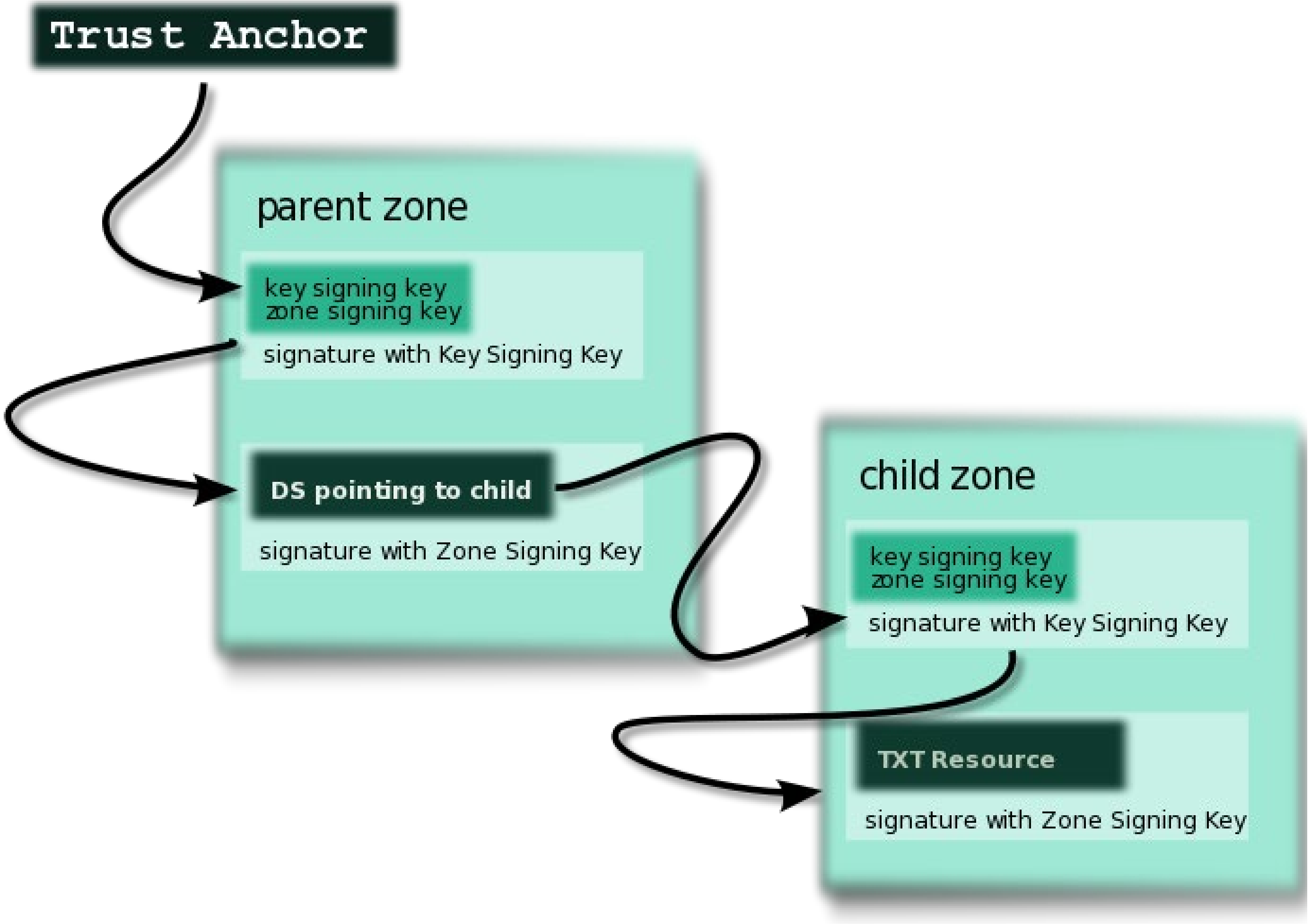
Securing DNS: DNSSEC

- add security, while maintaining backwards compatibility
- All answers in DNSSEC are digitally signed
- By checking the digital signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server
- new DNS record types: RRSIG, DNSKEY, DS, and NSEC
- When DNSSEC is used, each answer to a DNS lookup will contain an RRSIG DNS record
- The RRSIG record is a digital signature of the answer DNS resource record set
- The digital signature can be verified by locating the correct public key found in a DNSKEY record

The trust system of DNSSEC

- To be able to prove that a DNS answer is correct, you need to know at least one key that is correct from sources other than the DNS. These starting points are known as **trust anchors** and are typically obtained with the OS or via some other trusted source.
- The trust anchors will be the root servers
- An *authentication chain* is a series of **linked DS** and **DNSKEY** records, starting with a trust anchor to the authorative name server for the domain in question.
- Without a complete authentication chain, an answer to a DNS lookup cannot be securely authenticated.

The crypto trust tree



DURZ records are available on root servers!(2010)

```
boldi@shamir:~/crysys/courses/hbgyak/slides $  dig dc.hu @k.root-servers.net +dnssec

; <<>> DiG 9.5.1-P3 <<>> dc.hu @k.root-servers.net +dnssec
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24053
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dc.hu.                    IN      A

;; AUTHORITY SECTION:
hu.                 172800  IN     NS     ns.nic.hu.
hu.                 172800  IN     NS     ns1.nic.hu.
hu.                 172800  IN     NS     ns2.nic.fr.
hu.                 172800  IN     NS     ns2.nic.hu.
hu.                 172800  IN     NS     ns3.nic.hu.
hu.                 172800  IN     NS     ns-se.nic.hu.
hu.                 172800  IN     NS     ns-com.nic.hu.
hu.                 86400   IN     NSEC   id. NS RRSIG NSEC
hu.                 86400   IN     RRSIG  NSEC 8 1 86400 20100512070000 20100505060000 55138 .
      P+vSlYRY+dxqOucKYxVhaSfKlUaniHekz1hPjCCa8D1gDuUkskKen3WU
      iTFhwS6Eg0j2506JMsIC7JYpIOKuG7eS16SbipjJ+8sBm/EU4o90LnwP
      HLihYIzAwJoAAPUGyjP/4j77dIt5yIx5yFjKc5NVE2F1IU8vpkiUTLKm dpg=
```

.id is the next domain in the root

The same in 04/2011

```
▪ $ dig dc.hu @k.root-servers.net +dnssec

▪ ; <<>> DiG 9.7.3 <<>> dc.hu @k.root-servers.net +dnssec
▪ ;; global options: +cmd
▪ ;; Got answer:
▪ ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63288
▪ ;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 12
▪ ;; WARNING: recursion requested but not available

▪ ;; OPT PSEUDOSECTION:
▪ ; EDNS: version: 0, flags:; udp: 4096
▪ ;; QUESTION SECTION:
▪ ;dc.hu.              IN    A

▪ ;; AUTHORITY SECTION:
▪ hu.           172800  IN    NS    ns.nic.hu.
▪ hu.           172800  IN    NS    ns1.nic.hu.
▪ hu.           172800  IN    NS    ns2.nic.fr.
▪ hu.           172800  IN    NS    ns2.nic.hu.
▪ hu.           172800  IN    NS    ns3.nic.hu.
▪ hu.           172800  IN    NS    ns-se.nic.hu.
▪ hu.           172800  IN    NS    ns-com.nic.hu.
▪ hu.           86400   IN    NSEC   id. NS RRSIG NSEC
▪ hu.           86400   IN    RRSIG  NSEC 8 1 86400 20110417000000 20110409230000 34525 .
  LXy3Yn7fNVvvzuVeQ++f9eSNCVImb9BcHbrFNSc/WktU+tvNY7o1S+zS
  Kkss9xclLA/hnMvEmPNldf+tRoGGel+7HRWuE8geUCZ9fT0z1dxTmhMV
  a8UoN1h6mAzGsQv1zyW7f5NkUVbqBQcBoBg1xtZBmb+ostNjpDnoFjVc XvY=
```

Nsec is used to have a linked list of entries and to prove that something is NOT in that

```
aggregator.crysys.hu.  3000    IN A     195.228.45.178
                3000    RRSIG   A 8 3 3000 20110222195654 (
                            20100509103014 741 crysys.hu.
                            r/6Ee2GYBoBIyYlckRhl6c0IcN2tixj12H2g
                            m7aAJ5SPNfPS9tTFgVu+ygs+Atom9gLtwRzv
                            AT1sRi18agJ5jq09k/noBsz6vaqS72DyseJw
                            Kqv93AvQxkaGxaLWlWyQSjhVMVAfKMJ1tfFU
                            h3PuJrotHFAbcNphdbQRso7qJicJz8TooByr
                            XeXp9tE1GIntmUtvM1OoCMy8xlya8F1O4wyU
                            8i/cmtWCYz9M4Kq/4be9EkPVbbLqKYbUThGK
                            +W+1jCakCqaNJ+iqbIHyUZvn8qD1QW6YKi5C
                            dZ/dFMMck76LmgLFrCriRFaTgm2KgLIXoJ0j
                            XQFWyKY/Ib0UdCTDmw== )
                3000    NSEC    albifrons.crysys.hu. A RRSIG NSEC
                3000    RRSIG   NSEC 8 3 3000 20110222195654 (
                            20100509103014 741 crysys.hu.
                            hsYJefGXJn31Dae6s8k6N5yDkFacOwl6kGF3
                            5I1QK975htqvIn8OgmSqIpjnCXXmzr7Wt3KN
                            aBzc6r/ZrDkwbJ+JMg3m/IjjRTYLVpbqfhOH
                            AdMVLp3aCkHPWkoagiljR92OdDt1BJeq2mxs
                            ujcBtMn0ssUI0VCAEOYl+tDn8fbTF8E2AIsh
                            Bd+gY+N8K8Pos940ovOQSu2Qt45pWCvWQ2Ih
                            cOxlnlekkWuuT41NTfSKBJ1eJF8f6bR1T6Bx
                            Mzzz19nDpphFjVMi+/TrqQp0ocRMax5uGWiC
                            ZikXi9iLG1hepnUTf+fv7aauLDY9w5996xsl
                            4g0BBCLbXgICdkvwOQ== )
```

„linked list” of
DNS info by NSEC

Security problem of NSEC record

- NSEC is a „linked list” in the domain zone
- NSEC record is good to proove that a record is not defined
- NSEC information makes it possible to map, discover the whole zone (just like in zone transfer)

Countermeasure: NSEC3

- After deliberation, an extension was developed: "DNSSEC **Hashed Authenticated Denial of Existence**" (informally called "NSEC3").
- In this approach, DNSSEC-aware servers can choose to send an "NSEC3" record instead of an NSEC record when a record is not found.
- The NSEC3 record is signed, but instead of including the name directly (which would enable zone enumeration), the NSEC3 record includes a cryptographically hashed value of the name.
- The NSEC3 record includes both a hash after a number of iterations and an optional salt. Salt, where used, increases the number of pre-computed dictionaries that an attacker using a pre-computed dictionary attack would need to create, increasing iteration values raise the computational cost of computing a dictionary.
- In March 2008, NSEC3 was formally defined in RFC 5155.

Implementation of NSEC3

- **New features in BIND 9.6**
- Since BIND 9.5 was released in May 2008, many new features and improvements have been added to BIND. Over 125 changes have been made. The following are the highlights for the 9.6 release.
- **Full NSEC3 support**
- BIND 9.6 includes support for the NSEC3 record generation as defined in RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. As an alternative to NSEC, it can prevent walking DNSSEC zones (zone enumeration). It also permits gradual expansion of delegation-centric zones. (NSEC3 has an opt-out bit which lets the zone owner save overhead by skipping over signing delegations to unsigned children zones.)
- **NSEC3 is not recommended unless there is a pressing need** for the features NSEC3 provides**. It is expensive for both the server and the client.** Most zones do not need the addition expense incured by the use of NSEC3.

CrySyS NSEC3

```
; <<>> DiG 9.7.3 <<>> www5.crysys.hu @localhost in a +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16579
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www5.crysys.hu.                   IN      A

;; AUTHORITY SECTION:
crysys.hu.            3000    IN      SOA     ns1.crysys.dc.hu. netadmin.ns1.crysys.dc.hu. 2012050611 43200 14400 2592000 3000
crysys.hu.            3000    IN      RRSIG   SOA 8 2 3000 20130510062720 20130425181400 741 crysys.hu. ZyUNM0xoq22uXilINEmRiL6WH2x+CCqdGFyMiCV/cD61cpytMc5MG2o8
00e7kuiEAnHy6xPzWfMcnkJRnakkp6/fi/bfCxb3hwJoFKv5CEH19f3O ETyRXjP3QFnkWoQ2MQ0VQsKg//HbwdL0GJV8q3dEgw6uFBiMnTMHdeq3
qZsjTnD4RvDGvDr0DX0mexKJWGBQSp1QpSwQaSqW7smAVeprK8zVSHvN Uu2/sC8Snx9SJwwngjGSVvk1Ix/5zH7AFsiuSS4RzHtHY76Vh8WhuFic
J7aN2RIEUOae66G38U3Xly60SAbLwfXSU2f10Qd2clucwW8hzzgYDN6n a0VYmQ==
5K1Q2M95IB1T87SQE78E15I44OOOU8GM.crysys.hu. 3000 IN NSEC3 1 0 100 C3732ADDA6748D8DC56208B1A19AC014 64SFPVSL8B2TP3E5TA179QNOPSUBPHIP A NS SOA MX TXT
RRSIG DNSKEY NSEC3PARAM
5K1Q2M95IB1T87SQE78E15I44OOOU8GM.crysys.hu. 3000 IN RRSIG NSEC3 8 3 3000 20130510062720 20130425181400 741 crysys.hu.
eKdTBcC4vDxNtOlR7msc1+PhyHk5r7CoFH9fP26eL5UzeJObX8xO9Q8R MFoe3Alm03+q7l0pFI74aOdqjMS5M4m6cFqhgwyPeJOpU25RO/9kI2mH
Nv+pvjThTGRDnGhj8pSQfcJopV1vPe7b9i1RsTL47rcvso3L13qKnOu1 UFUbtuT10nINDC3EmdXfN1ClsCmFH7T+49E5YPVU7Nxz/wythMLdmowa
5j/Ij9WOcim58ClWjLOAUDLAejEeWi5m0GhvgiKF7tadufKxecHbBPBQ w9STI0FI8tDb1E6bQU/vl+pf+bdml5YN9jbnUUgnnv9yq669gHb1meNd sPIOjw==
1MT46GU7MTVLILB3EBVKEN170UQARV12.crysys.hu. 3000 IN NSEC3 1 0 100 C3732ADDA6748D8DC56208B1A19AC014 1SFT4CLIN4OKKT04L6KF3VME4PBSIQT0 A RRSIG
1MT46GU7MTVLILB3EBVKEN170UQARV12.crysys.hu. 3000 IN RRSIG NSEC3 8 3 3000 20130510062720 20130425181400 741 crysys.hu.
Aeo8AQIIAn6LCVqNaouZRYtgaELMnxLMPajenp3t8u7frVCDoixJTJXj pevJkonzxncrc/EqDLXU4lKzFe8hcIIxKYPZ35Sl7olseQVdO8jeGJpy
pd/2Y3TYAZISzeGxOpolx8cZS7b/TElHSQj4hEIa7J6YQ8RhWqktpiSk 2vLlmESXX9rDZT2ApvXaZFmcDRu79rDFnHoZZidPsUO1GuJPe+7KC1YN
Ly2+0eIltyyyuHDaJmcnaJ/kPm63bg2yPQf2gepzJGB4MGcNVqKEvUWx 9c1i7Q+GGOB8tSNR9z0djy2XiCQNwPFFSlBQA0dsZYEzJjNpNcN2myQ+ TXBhJg==
HCBROVD1MRN2HNFR4JQ9MT157Q033G91.crysys.hu. 3000 IN NSEC3 1 0 100 C3732ADDA6748D8DC56208B1A19AC014 I08D83JCP956CJ5A0GMA3S267JFO5CTV A RRSIG
HCBROVD1MRN2HNFR4JQ9MT157Q033G91.crysys.hu. 3000 IN RRSIG NSEC3 8 3 3000 20130510062720 20130425181400 741 crysys.hu.
czp/QyComdh/tjms+p82oV+RTuaOzQPobSSxsrPQGDE/5H/Jwr7x6146 NhC/N+h5OfuZdMO3QIBHdEcQs5sluVnfNGETwBt9ezvLPUCaYcLQzsP/
WymkoHYVC8aDCtTM38YQDDGSZC8ZoFzCnnS1QL+bdj0Dw318RtPtakt2 Sq1yRpUEagAMgQewFeTrlFgP/COUJ7XXsfSN4cg0hh3DWd7vTAvA72WO
Ka4dH4m2uU2swo5nX4MZjCLzNSNROmOzR9ovyC858pWSndiwVENI8wvq 9aVq9lN2haEiSCz+uBLhO3Iah6WQWhFVF+emWdXqDmFqa37cP53J5NxX KT4muA==
```

NSEC3 critiques

- NSEC3 can be attacked to make zone enumeration
- https://tools.ietf.org/html/draft-gieben-nsec4-01
- NSEC4 was proposed around 2013
- NSEC5 was proposed for further enhancements
- https://datatracker.ietf.org/doc/draft-vcelak-nsec5/
- Dazed and confused: NSEC usage leaves a gap in practice
- https://tools.cisco.com/security/center/resources/dnssec_best_practices
- Easiest thing is to don’t care and use normal NSEC, but that leaves trivial zone enumeration possible

crysys.hu. 0 IN NSEC3PARAM 1 0 100 C5A5A66BE840E95738660AE445101D53

- “1” –algorithm -> SHA-1
- “0” – flags
- “100” – iterations
- “C5…” – salt

Calculation:

- IH(salt, x, 0) = H(x || salt), and
- IH(salt, x, k) = H(IH(salt, x, k-1) || salt), if k > 0
- then IH(salt, owner name, iterations)
- With my example.com domain, the hash algorithm will be :
- IH(fromHexStringToByte(“C5A5..."), toCanonicalWireFormat(“crysys.hu"), 100)
- fromHexStringToByte is a base 16 decoder : fromHexStringToByte("aabbccdd") = [0xaa, 0xbb, 0xcc, 0xdd]. See RFC4648
- toCanonicalWireFormat convert the domain in wire format using its canonical form : toCanonicalWireFormat("example.com") = [0x07, 0x65, 0x78, 0x61, 0x6d, 0x70, 0x6c, 0x65, 0x03, 0x63, 0x6f, 0x6d, 0x00]. See RFC4034 (canonical form), RFC3845 (wire format)
- And that's it, you are now able to compute the NSEC3 hash of your favourite domain. You just need to wait for NSEC3PARAM to be published in the respective zone to got all the necessary parameters :) (http://benoitperroud.blogspot.hu/2010/12/dnssec-nsec3-domain-hash-computation.html)

DNSSEC keys

- DNSSEC involves many different keys, stored both in DNSKEY records, and from other sources to form trust anchors.
- In order to allow for replacement keys, a **key rollover** scheme is required. Typically, this involves first rolling out new keys in new DNSKEY records, in addition to the existing old keys. Then, when it is safe to assume that the TTL values have caused the caching of old keys to have passed, these new keys can be used. Finally, when it is safe to assume that the caching of records using the old keys have expired, the old DNSKEY records can be deleted. This process is more complicated for things such as the keys to trust anchors, such as at the root, which may require an update of the operating system. (??)
- Keys in DNSKEY records can be used for two different things and typically different DNSKEY records are used for each. First, there are **Key Signing Keys** (KSK) which are used to sign other DNSKEY records and the DS records. Second, there are **Zone Signing Keys** (ZSK) which are used to sign RRSIG and NSEC/NSEC3 records. Since the ZSKs are under complete control and use by one particular DNS zone, they can be switched more easily and more often. As a result, ZSKs can be much shorter than KSKs and still offer the same level of protection, but reducing the size of the RRSIG/NSEC/NSEC3 records.

Key rollover

- In order to help with key rollover, there are not only the normal DNS TTL values for caching purposes, but additional timestamps in RRSIG records to make sure they don't get used past the expiration of the corresponding DNSKEY records. Unlike TTL values which are relative to when the records were sent, the timestamps are absolute. This means that all security-aware DNS resolvers must have clocks that are fairly closely in sync, say to within a few minutes.
- The DS records in a zone's parent domain require the use of the zone's private keys and can only be created by the zone. They must then be transferred to the parent zone and published there. The DS records use a message digest of the KSK instead of the complete key in order to keep the size of the records small. This is critical for zones such as the .com domain, which are very large. The procedure to update DS keys in the parent zone is also simpler than earlier DNSSEC versions that required DNSKEY records to be in the parent zone, also very important for large zones, such as the .com TLD.

DNSSec transition at root servers

- **December 1, 2009:** Root zone signed for internal use by VeriSign and ICANN. ICANN and VeriSign exercise interaction protocols for signing the ZSK with the KSK.
- **January, 2010:** The first root server begins serving the signed root in the form of the DURZ (deliberately unvalidatable root zone). The DURZ contains unusable keys in place of the root KSK and ZSK to prevent these keys being used for validation.
- **Early May, 2010:** All root servers are now serving the DURZ. The effects of the larger responses from the signed root, if any, would now be encountered.
- **May and June, 2010:** The deployment results are studied and a final decision to deploy DNSSEC in the root zone is made.
- **July 1, 2010:** ICANN publishes the root zone trust anchor and root operators begin to serve the signed root zone with actual keys
  – **The signed root zone is available**.

Transitions 2

- Week of 2010-01-25: L starts to serve DURZ
- Week of 2010-02-08: A starts to serve DURZ
- Week of 2010-03-01: M, I start to serve DURZ
- Week of 2010-03-22: D, K, E start to serve DURZ
- Week of 2010-04-12: B, H, C, G, F start to serve DURZ
- Week of 2010-05-03: J starts to serve DURZ
- 2010-07-01: Distribution of validatable, production, signed root zone; publication of root zone trust anchor

04/2011 What happened?

- Root zones are singed
- Next step is to do something that really works in-life
- E.g. set DS records for the .com zone
- Summary of the last 11 month: nothing happened…

Setting up DNSSEC

- Implementing DNSSec
- Check http://www.nlnetlabs.nl/publications/dnssec_howto/index.html
- Insert dnssec-enable yes; into named.conf options part.

```
#dnssec-keygen -r/dev/random -a RSASHA256 -b 2048 -n ZONE crysys.hu
Kcrysys.hu.+008+00741
```

RSASHA256 is not available in bind ~9.5.1.

```
#dnssec-keygen -r/dev/random -f KSK -a RSASHA256 -b 2048 -n ZONE crysys.hu
Kcrysys.hu.+008+17707
```

```
# ls -la Kcrysys.hu.+008+*
-rw-r--r-- 1 root root  549 máj  9 13.24 Kcrysys.hu.+008+00741.key
-rw------- 1 root root 1776 máj  9 13.24 Kcrysys.hu.+008+00741.private
-rw-r--r-- 1 root root  550 máj  9 13.25 Kcrysys.hu.+008+17707.key
-rw------- 1 root root 1776 máj  9 13.25 Kcrysys.hu.+008+17707.private
```

- Add to Crysys.hu zone file:
- $include /var/named/Kcrysys.hu.+008+00741.key
- $include /var/named/Kcrysys.hu.+008+17707.key

- A=Kcrysys.hu.+008+17707
- B=Kcrysys.hu.+008+00741
- dnssec-signzone -e now+25000000 -o crysys.hu -k $A crysys.hu.zone $B.keyChange
- zone definition:

```
zone "crysys.hu" {
      type master;
      file "crysys.hu.zone.signed";
 };
```

Key expiry issues

- Depends on the key length
- The idea is to have some <1024 bits key for zone singing
- And some >1024 (2048) for KEK
- Hard to guess what is appropriate
- Easy solution: have all keys >2048 bits RSA

NSEC3

- B=Kcrysys.hu.+008+00741
- A=Kcrysys.hu.+008+17707
- Z=`dd if=/dev/random bs=16 count=1 2>/dev/null | hexdump -e \"%08x\"`
- echo "random salt for NSEC3:$Z "
- dnssec-signzone -e now+25000000 -o crysys.hu -3 $Z -k $A crysys.hu.zone $B.key
- NSEC3 solves the problem with NSEC, not zone walk possible
- http://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt

Sig with NSEC3

```
3000    RRSIG   DNSKEY 8 2 3000 20120125075519 (
                  20110410222839 741 crysys.hu.
                  pEK443nsRDWBtjBTYQ74SB/hKXtTBd/bArnj
                  kK0iu4g7oyrMK7T8hrgXtnw7daz3Sp9Aizn1
                  DYz70ztCgPCIUjOrxtha+cqoJOipnNWX4M9X
                  ME9LbxKjn0bPrzl7MWohBrj7kJtSlRBuOE8Y
                  OJnQtdrL6EOvgeqFBuT/dCVxpyaYzYZvHhwO
                  pXVRyuzGytpYIK6qYzsIdWIWOACCk9EpPODo
                  RmKvfc96OcSCNv/UtFTiDLIMGo1PUyXngswB
                  +oxrfSRBDD168QsdnjHyzBrU6IeJ08BC1its
                  dsbxX0siG2aiPXReeDOpIuOAV9TsZjqR4W+x
                  aXZh6AAazdsS0Zfr6g== )
           3000    RRSIG   DNSKEY 8 2 3000 20120125075519 (
                  20110410222839 17707 crysys.hu.
                  mgO85fpzlMgzdcZw7KPphH1xB8RERpjAd0HM
                  TN5fV4zCvIC2QZROjGIhH+MffwO7NsWw81TC
                  +1IA2/cJ71vaVftV3g+Fb3QiFAAR7ZW1HMgg
                  s5/2VCXEFwFwuTHzhE/DO8M/oRMvFTC8peNO
                  YdvZ6wnH/IT/4tDYk5hhmNNBB9VpFkbe9ffj
                  a+Gcu1xyYxAzjItYJUfsZ/g7uj31tpsbD7Qa
                  AxqgnpWxwzuM0YTWE9On4HlWcXpvHvBwegQ/
                  VRdg73wwKXamgifcwvZz8xtJF/T4COXDEDwd
                  w5C4W5nS44BTWa7wz9VLpU/20kX3zYAu7PnY
                  NNxmPe0SC3NlVJIhKg== )
           0      NSEC3PARAM 1 0 10 0F2C122A0C920E942F8CD43EB37F5AA6
           0      RRSIG   NSEC3PARAM 8 2 0 20120125075519 (
                  20110410222839 741 crysys.hu.
                  QThP0QJMq6cMvZt43tDZBMlkNjcAO52gNf/7
                  ZPMJuBjPlSzr7HxEOKpbKiHkXlsoN+xG2z1i
                  zwNBPmfULvh4bNAFQaxbbFTfFdPcAhGl0owG
                  T0Zrw/E7eJBlYiMglZwjJc8eYvcDOSH46pPA
                  kQqRGkg3KIAR/3WYICpXHakn0WjKc2AaXx52
                  G3N91VL9tLSeTl0TQNcuQ3IBZ1tGiTpXQkN9
                  Nf/JehQW4m5PqQpd62s7G7MdfvBUCv3OpMx0
                  yijNNVF/WLQHuj7BpAgQkBqG4wxrqHvKNeaO
                  F24Ku1iMVeEv/yk70p783CwWCmovs5ixTeeV
                  8F/LFEOaI2SsaOzL4w== )
```

NSEC3 …

```
eternal._domainkey.crysys.hu. 3000 IN TXT "v=DKIM1\; t=s\; k=rsa\;
        p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkI1xqg49bAvPSB2QiEDRenlcPSxp3O53JqLOEzorTOMUU/8b6kuWSWvF
bToMw8kA3QDHE2c+No+OIJG3Ru7vaQkKJd08tlOe/jtGO23G0ajPQR7vVnnE3uIEVoqJNa6e4KPJR4MfoOQY3XDZWj/dhY6CUXwSKYY257l3
        f7ZvYqQIDAQAB"
                    3000    RRSIG   TXT 8 4 3000 20120125075519 (
                                20110410222839 741 crysys.hu.
                                a1nyZxirKR/v+AuPElzvNAXyPXQx+hdQdatt
                                6u1vFWKKOKQhmQnKyDucYgN3+pvltOEC3D6E
                                iiAS2Iev7wVa4j/gzXGxonEdf3vNMfnj3WLH
                                qd/X28Vb1wtACYWtytgKtdd1hrch4Nkdh9qS
                                M1e2BJdB5qtLVlHzstKQr/GTSuj49mS37Vll
                                2LwK7O+IFdGIjIB2bcJLpNx1QMHvxJ8e5E9p
                                MKFXzQvq5Qmg0rbGAVamTVm32dJuJlk/mpiN
                                WcnWUoLnCsUTsKSuqug8Dn3LT4BymPoq5DX5
                                jXD7J8RBzCOQgobCfbOmqeStEY80Q7fIdydo
                                +awiAHp0Q7Tz2/yCQw== )
shamir._domainkey.crysys.hu. 3000 IN TXT "v=DKIM1\; t=s\; k=rsa\;
        p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPiAQp5v2WLboPeciMd5b4G+jr+88/hykseyyOY0Y26jhVNJOJOWtlKrpT
MdPjX5cvhv0yWdhMIXY3ZkGoNkcxCVUawup53IOJwI3tEBlg0IDZfmjNx3BkPdlSdXN7ezTYEBddrAKnjzUJf0qlo4cleoCAAra3UUARe4fwvGNl
        /QIDAQAB"
                    3000    RRSIG   TXT 8 4 3000 20120125075519 (
                                20110410222839 741 crysys.hu.
                                UY68d+adn6+/ngVD95JIAKm04TtW6GKiJI+w
                                tMuDOureJQZ2LbF7uQTUbbEYGqYAUFT82yGm
                                GO64NNoX09JinGGGtMDrOdopbxTJdWdEYF9b
                                6F4hyZck5EBi8VIyN+J+9UB3jlsuXPzNRkjh
                                +KnzIM37VUjfTXmuVxrD1Lysp3jOvN+wcLZ1
                                iWqW/xygknBkKEZabYCZ/s/gQp4UtZrFW9R5
                                nRmG2eQDxHDfT5AZggRisW20GWADTQAAQi9R
                                jvLz85zxTwc3AUcMmFWokwSv9GtxY7E2pVah
                                OU9QEopZsES8twpSQRCGBS8+azVRVNydO6DJ
                                OdGohK9H8lCvd5YLDA== )
```

```
aggregator.crysys.hu.   3000    IN A    195.228.45.178
                        3000    RRSIG   A 8 3 3000 20120125075519 (
                                20110410222839 741 crysys.hu.
                                bErF9GJ/DfJEl0NvR0QUx6BqugN3GU3Xfh9U
                                c+iLxjrhryCeYQVF+6kvGPfTW9PexgySIH51
                                98JaqW1TRQ2OGvxbmwgqE0drcpdtitrR1BSU
                                Yu/m8yMkoDQI1UfbUQq0AgV3qjsbRJyX3bRn
                                Vun5ZNEN08YjJw83h5MOk7h/hXS0nQID3dQe
                                72le4gyeM/2Mxv+k6unBRgkPYRFS4ZoeGDLV
                                VGyINKpi4hxBjZO6RYs5nKLwdWDVDAtETPzn
                                SVQkCKTkOZd7hz93NmiJf5zNER5xqRGujs0e
                                ApR49G79YP78MlTeORh3gS6GpdQBm+ziFKnG
                                ZJoHBEDA2ttWw6EVug== )
albifrons.crysys.hu.    3000    IN A    10.105.1.95
                        3000    RRSIG   A 8 3 3000 20120125075519 (
                                20110410222839 741 crysys.hu.
                                YXnE810Nrk9OLZmGvfiRxYnDv69PQkHVLn0N
                                6i6rUvZp35O4JT4FHU68S6q1VCstv0vnYjMS
                                exRU/ck0p0JvdgCX+fmykeTZoNdob5dx/Uip
                                qhiMhgDqk/Uws24v3wr1zQCflptmZWZR1osx
                                LggDufLC8MiHT/Be6gDVDHqnBDMaXD+4QUN1
                                cBApUyJiTdiZFvrPBSmaTTQzfYiXUvoih5VN
                                PDgwG33NwCueGr0Wl0aoopJK/rgFgQdNP9MJ
                                z3sS6/TlHTNB5cIz2jAjoX0P9QpsL+pSSVzd
                                h7/tLt4vkz/MP2ya9Qp3lM4qSvuuR+tf2V+q
                                JGa0QTryXJtzwZsqSQ== )
```