DNSSEC

Swinog #19

SWITCH

Serving Swiss Universities

Simon Leinen
simon.leinen@switch.ch

Bern, 29. September 2009

What DNSSEC does …

DNSSEC is an **extension** of the Domain Name System (DNS), that ensures the **authenticity** and **integrity** of the data in DNS replies.

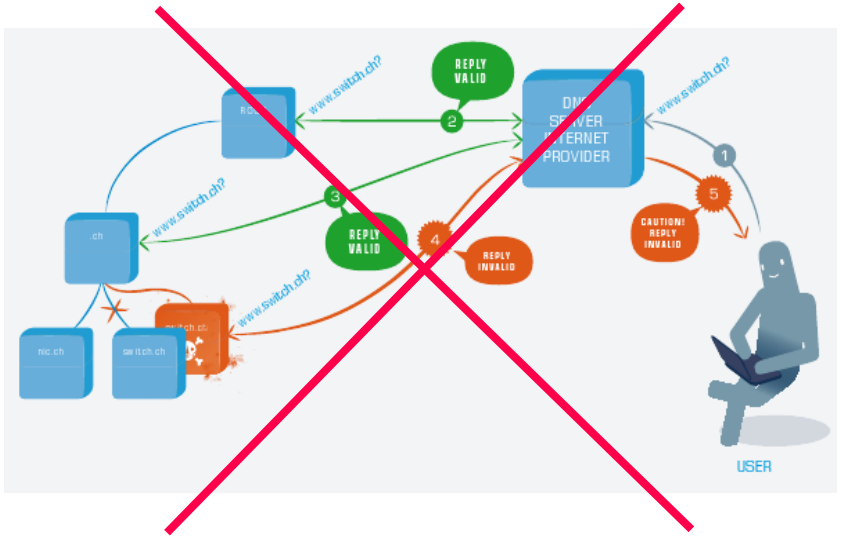
So it allows a resolver to verify that:

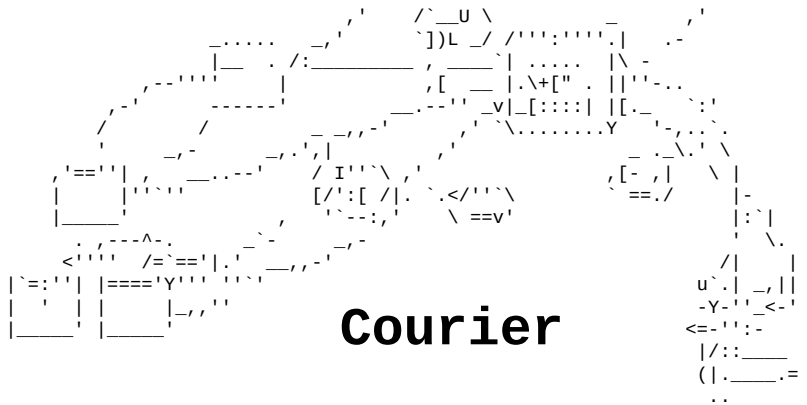
- Data comes from the maintainer of the zone
- Data has not been altered in transit

… and what it doesn‘t

- Does not protect DNS data packets in transit
- Does not authenticate hosts
- Does not encrypt anything (DNS data is public by nature)

How DNSSEC works …





Warning: The next slides contains only ASCII characters!
For a management friendly introduction to DNSSEC please go to
http://www.nic.ch/dnssec

The signatures (RRSIG)

```
$ dig switch.ch. SOA +dnssec

; <<>> DiG 9.6.1-P1 <<>> switch.ch. SOA +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37489
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;switch.ch.                     IN      SOA

;; ANSWER SECTION:
switch.ch.              86046   IN      SOA     scsnms.switch.ch. hostmaster.switch.ch. 2009092800 28800
    7200 604800 180
switch.ch.              86046   IN      RRSIG   SOA 5 2 86400 20091027221036 20090927221036 4500 switch.ch.
    SrVw6WsDxBU5WYZraQDyY4Tozb+pJ63uizH34ksDMhSNBx6+4RfHsbP9
    Q2F6pvx+BfAdJdtT14i6pkb9eKp9HrxH/ZZBFNd3DF7q2x03tArzV9nL ud6T1J8wRt1Y25tM

;; AUTHORITY SECTION:
switch.ch.              172446  IN      NS      scsnms.switch.ch.
switch.ch.              172446  IN      NS      merapi.switch.ch.
switch.ch.              172446  IN      RRSIG   NS 5 2 172800 20091027221036 20090927221036 4500 switch.ch.
    EaaiEqpyu36flpWB42LmYkOj4LpwREZXi5woYtu/jfcoBM79+J9+c/kl
    qmPBKAf8XC9SsTnnwyFiZmWR64nuI6ylw8NTVyDQyJ0VNFdS87fx3pAJ g0DkpTkpTztuFYhT
```

The keys (DNSKEY)

```
$ dig switch.ch. DNSKEY +dnssec


;; ANSWER SECTION:
switch.ch.              86343   IN      DNSKEY  256 3 5
     AwEAAaafSevqyDuMGFMhgVBe0kaWzfIZRa78dPXhvruL+e/QxD18p/Ij
     uNJg9y8F/YdwpY2yu8rFOsHdMiMD3vi3LKnTYEfzILBgctcSMjywh9zA goN+JCdngQ0yd+gCShpFAw==
switch.ch.              86343   IN      DNSKEY  256 3 5
     AwEAAa8JZ0f9i615Ypurdfew5wxQ53+c2ll2G49HmRXkUWR7Eh1wWNyh
     yEueX376BGkCzmJH8IOgh7mM2q7ZT0LlfY+0Mpm+OEotfnqYqFMKni/G UbjhXs8sekDz8BP4eCLb/w==
switch.ch.              86343   IN      DNSKEY  257 3 5
     AwEAAbwGNEAFB3vME/TcCU8VfC5Joz6e04NeMkAaC+jbNiFGAebYSM75
     oqNHiAkAgelT3K0QqKm5jlrL3wtprQ8Qb8M4XDKTJT4KFLeLrRvXzPhr
     liCerRLf7fAs9be+tST1dTJItDVMVFEneviBzVpOFxDDtprbT91cWgmy
     DzMk5litKdXhvUoaF4U975z78cgHGIUO4XmkSGymz8pXfpzagNNaxzLS
     deZnj9oPEEKICn9LyvSfdM35SNfnFYaxD52QjcPFyBIy3Ew2IY11guXN
     mWAnLt/ZXLYTNSxJOTz8B8lL+HEpK4iVSTcx64lC0OWI20m/pJea9afZ ANzuIP6A1vM=
switch.ch.              86343   IN      RRSIG   DNSKEY 5 2 86400 20091027221036 20090927221036 4500
     switch.ch. nSmTwHjipqaSSE5ZNSSbJ/hOtzXpnu47rSC7GqwCNWD2XU8gMy+eP24f
     JlBVc2zKMNY8MaS8F1emEneqY2h060mBzacNMbm0uc9DTqxHEWS+3+Uz ALEeqjHJVLjjGUzW
switch.ch.              86343   IN      RRSIG   DNSKEY 5 2 86400 20091027221036 20090927221036 43837
     switch.ch. MMnmienxZ5guhzyU33vAfvfz/B9g4f8qXhsGO6EhtjH8hdFlCyfUZtLp
     MlqHcjsIeRhYtgXMZ8OrrOtVWhlLbbnKzA8nef4AemvskcUp+oKrzxzc
     ngzhTc34YGNHw2UEIzNPPDp4i++Y2zWLGBmc+qpX3Lvs2MczzMxdGgNH
     CVoj5C2hbd37QiGCX1AIYT7UiqV2vNTTrq6Umng4pOXMp4kisIWmRyjk
     RYjwk+jhwm8NVS9wnT+vJBGr81cvawfml5bLREtSy7SH+TMwsMBHGoEg
     h6lZgyaMCjCkhXvaBVh4bI6Y+irjRtOYMCqZQYP1ZqKwKj2V4xvVCySH XUWKtg==
```

The delegations (DS)

```
$ dig switch.ch. DS +dnssec @a.nic.ch.


;; ANSWER SECTION:
switch.ch.              3600    IN      DS      43837 5 1 91DCFCA519CF8B038441869878CC361060200534
switch.ch.              3600    IN      DS      43837 5 2
    838CEF7635952DF83311A92B48AE7F191AE29484534E38B1AB7B3D09 66B9EE55
switch.ch.              3600    IN      RRSIG   DS 7 2 3600 20090930103603 20090923132131 8060 ch.
    YjfOWqWY2qT0Y4A0cP2QbO+o/kL48nYgDu6pD0wd7WL/m1NHHiKrmGFW
    I6/Ia47h5F41dUAZWs16hrnueW6TE9SGge77H56vBER1yRzZomU2Wmdw
    2xLteN3HqEntC2FfZb8VPGhn0HZJMbPU/OkxAA03XjyDQY+xOsZ/UCcR 7c4=
```

Signing “non-existence” (NSEC/NSEC3)

```
$ dig non-exists.switch.ch. A +dnssec


;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 39649
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1


;; AUTHORITY SECTION:
nms.switch.ch.          180     IN      RRSIG   NSEC 5 3 180 20091027221036 20090927221036 4500 switch.ch.
     Npx36lHBgKcHjscO8axB5bw4nt6kl/EQzHdYu93NVp165niL1u07vAwv
     13kkIFNI4MhivYmckv0F2Y6RvTZQJoYByYqGpYGSQfU6nRbH4EAPmeg7 1z2/cw0LHIvnO4wr
nms.switch.ch.          180     IN      NSEC    nona.switch.ch. CNAME RRSIG NSEC
switch.ch.              180     IN      SOA     scsnms.switch.ch. hostmaster.switch.ch. 2009092800 28800
     7200 604800 180
switch.ch.              180     IN      RRSIG   SOA 5 2 86400 20091027221036 20090927221036 4500 switch.ch.
     SrVw6WsDxBU5WYZraQDyY4Tozb+pJ63uizH34ksDMhSNBx6+4RfHsbP9
     Q2F6pvx+BfAdJdtT14i6pkb9eKp9HrxH/ZZBFNd3DF7q2x03tArzV9nL ud6T1J8wRt1Y25tM
switch.ch.              180     IN      RRSIG   NSEC 5 2 180 20091027221036 20090927221036 4500 switch.ch.
     Ocwswk6HtYM1tFyfseNpWeNzIW7b3Du1haBDIgQmpcjkLOvAIpb1HswQ
     qX3QQxCofQwsSakMY16mjhXb5TeItDSU6xqw6/VB/Kfx38cBfaXEAHfq eqiDDoK9uzpqZ5cm
switch.ch.              180     IN      NSEC    res102.102.switch.ch. A NS SOA MX AAAA LOC NAPTR RRSIG NSEC
     DNSKEY
```

Operational issues

```
$ dig switch.ch. ANY

;; Truncated, retrying in TCP mode.

;; Query time: 2 msec
;; SERVER: 130.59.31.248#53(130.59.31.248)
;; WHEN: Mon Sep 28 10:32:01 2009
;; MSG SIZE  rcvd: 2639
```

```
$dig switch.ch. ANY +dnssec @scsnms.switch.ch.

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;switch.ch.                     IN      ANY

;; Query time: 2 msec
;; SERVER: 2001:620::1#53(2001:620::1)
;; WHEN: Mon Sep 28 10:36:43 2009
;; MSG SIZE  rcvd: 4045
```

DNSSEC @ SWITCH

Project to introduce DNSSEC to .ch / .li

- Phase 1: DNS
  - Includes: key generation, signing, secondary infrastructure

done

- Phase 1+: Trial period

- Phase 2: Provisioning System
  - Includes: www.nic.ch, EPP interface

- Public start: **Feb. 2010**

Phase 1+: Trial period

What can you do?

- Enable validation of signatures on your cache

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

include "/etc/bind/itar-keys";   //from itar.iana.org

trusted-keys {
    “test-zone.ch.” 257 3 5 “AwEAAbyciviZB ….. pRgnLGO542”;
};
```

- Sign your zones

```
dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE your-domain.ch.

dnssec-signzone -o your-domain.ch. your-domain.zonefile
```

http://www.nic.ch/dnssec