

# DNSSEC in Switzerland

2<sup>nd</sup> DENIC Testbed Meeting



**SWITCH**  
Serving Swiss Universities

Samuel Benz  
samuel.benz@switch.ch

Frankfurt, 26. January 2010

# About SWITCH

- The SWITCH foundation operates the national research network since 1987
- SWITCH provides different services to universities like wireless roaming, AAI, PKI, video conferencing and lecture streaming
- SWITCH is the registry for the ccTLD .ch and .li

# DNSSEC in Switzerland

Why ?

- Currently the best solution to prevent cache poisoning
- „Normal“ evolution of the DNS protocol
- Provides low level infrastructure security
- Platform to integrate new services
- As a registry: DNSSEC has to be deployed by an top down approach.

Why now ?

- NSEC3 is available

Challenges ?

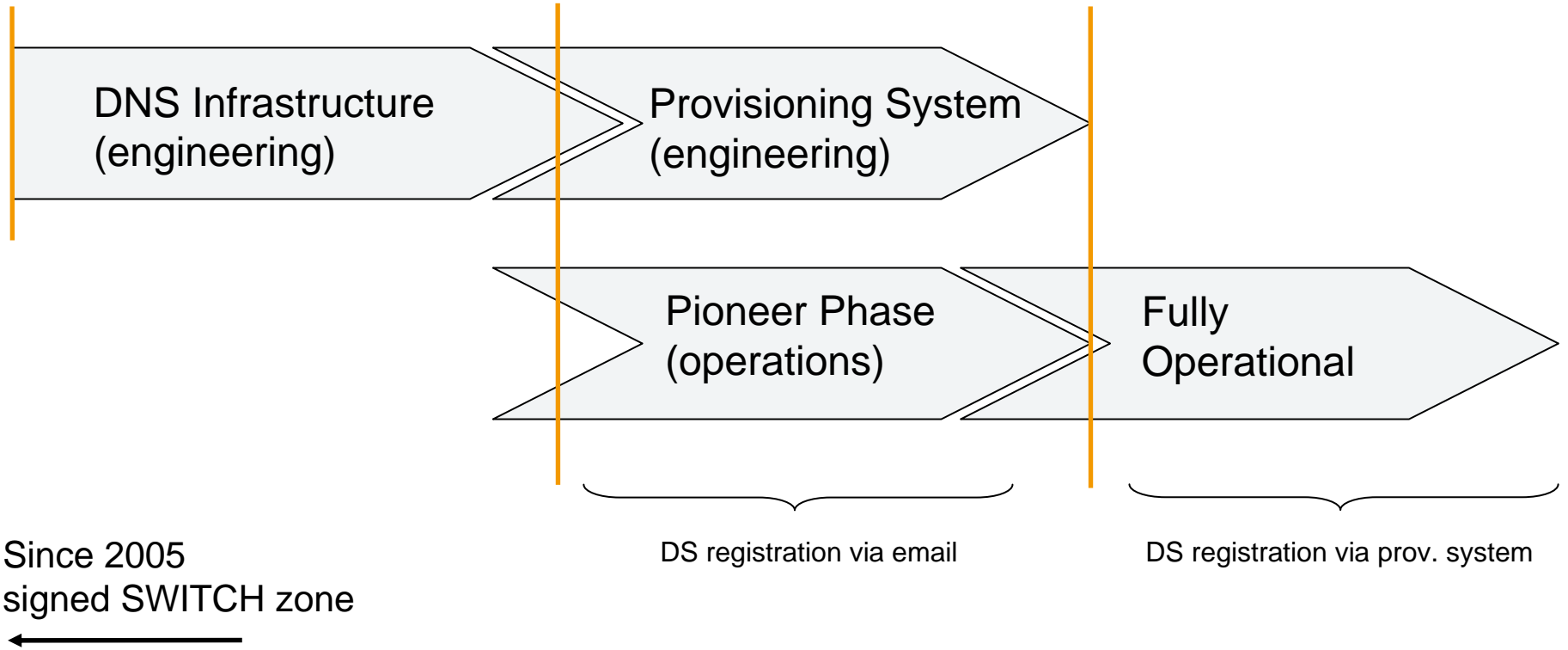
- Complex technology with a minimal amount of operational practice
- The implementation costs

# Project Schedule Overview

1. March 2009  
Start

21. Sept. 2009  
publish first signed zone

2. February 2010  
“Going Live” provisioning system



# Project Task Overview

## Phase 1: DNS

- Upgrade the DNS infrastructure
- Specify Key Management Practice Statement (KMPS)
- Implement the KMPS
- Develop signing tools
- Develop monitoring tools for registrants and our infrastructure

## Phase 2: Pioneer Phase

- Build a community
- Organize workshops
- Accept DS records from “friends & family” by email

## Phase 3: Provisioning Interfaces

- EPP interface for registrars
- Web interface for registrants

# Phase 1: DNS

- Replace those secondary name server without DNSSEC support
  - New secondary in Brazil / new 2<sup>nd</sup> anycast network
- Renaming all name server host names to {a-h}.nic.ch
  - Reduces DNS answer packet size
  - Example: domreg.nic.ch -> a.nic.ch
- No hardware upgrades (no significant increase of cpu usage detected)
- Problem:
  - NS need enough RAM (requirement for .ch ~1.5GB)
  - Time to copy the full zone (450MB) to Brazil (tcp window tuning)
  - Increase BIND journal space for IXFR

# Phase 1: KMPS

- Political questions
  - Who holds the pass phrase for the keys (shared between several persons?)
  - Where do we store the private keys (offline or online?)
  - Using HSM (hardware security module)
  - Using NSEC or NSEC3
- Technical questions
  - Key length
  - Signature and key life time
  - Key rollover scheme
  - NSEC3 opt-out
  - How we publish our keys
- Problem:
  - Ask the right questions
  - Less operational practice

# Phase 1: Key Generation

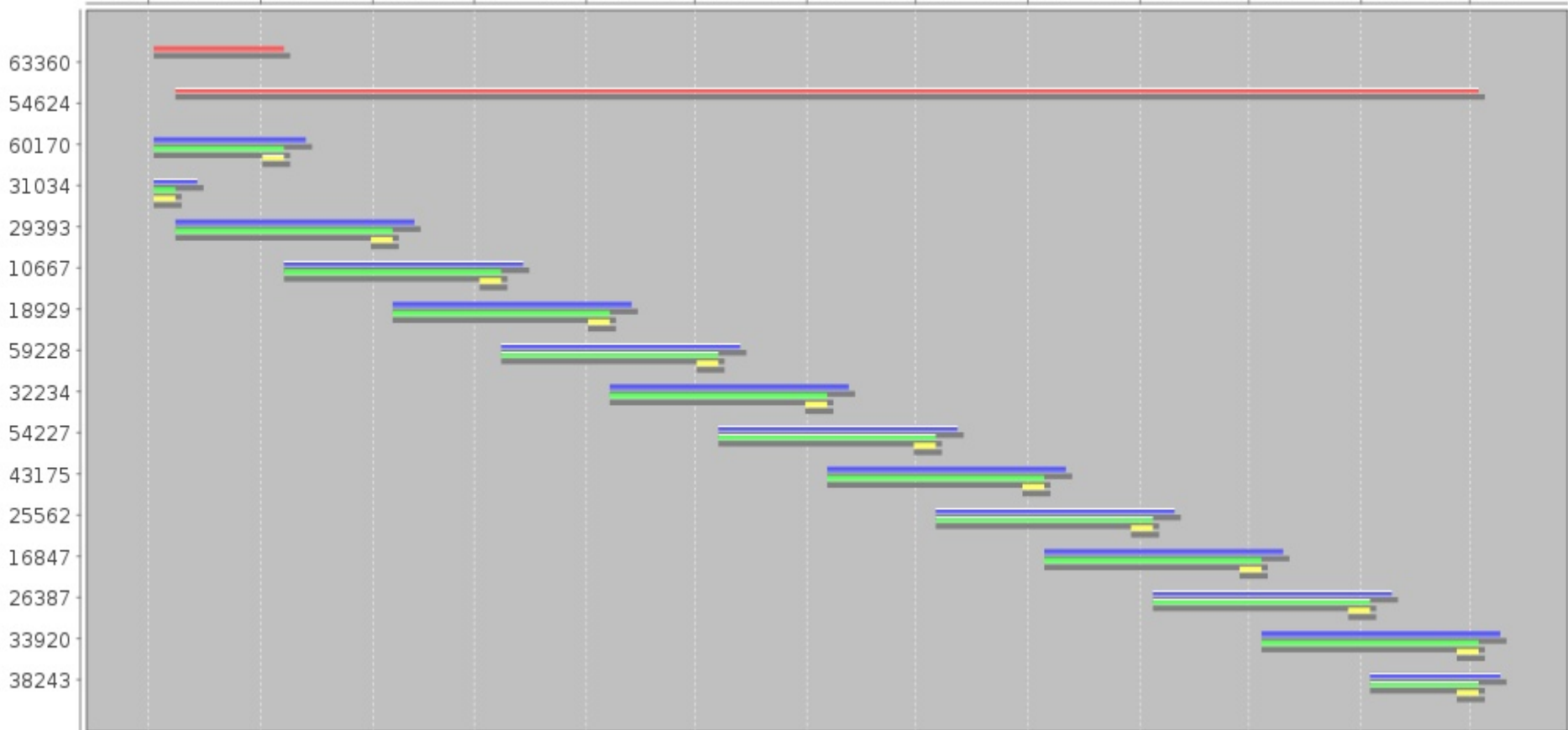
- Key generation platform
  - Offline system runs diskless
- Using TPM chip as hardware random seed for key generation
- Several people (2 of 3) are required to unlock the active KSK
- Pre generating 12 ZSK and sign all zone apex with the right combination and validity period of the KSK
- Problem:
  - PKCS11 / Crypto Know-How
  - Key validity period pre calculation



# Phase 1: Key Lifetime

ch. key schedule

Dec-2009 Jan-2010 Feb-2010 Mar-2010 Apr-2010 May-2010 Jun-2010 Jul-2010 Aug-2010 Sep-2010 Oct-2010 Nov-2010 Dec-2010



■ KSK ■ ZSK eff ■ ZSK list ■ rollover

# Phase 1: Signing Tools

- Build own tools for key rollover management
  - Configuration is done according to a schedule file which is generated during key generation
- Signing the zone every hour with standard BIND tools
  - took about ~20 min without incremental signing
  - incremental signing ~9000 sigs/h
- Signing is done on a new DNS hidden master server
- Problem:
  - Because the KSK private keys will never be available on the signer, it needs a special logic to include the correct DNSKEY RRSIGS
  - Bugs with NSEC3 signing from BIND
  - Signature expiration jitter (use initial  $\frac{3}{4}$  of sig. lifetime; then 1h)

# Phase 1: Monitoring

- Additional DNSSEC tests for our new delegation checker
  - Pre-delegation check with DNSKEY / DS records (integrated in the direct customer web application)
- Additional test for .ch / .li according to the “key schedule” file
  - Test if the key rollover logic is in the right state
  - Test DNSKEY / SOA signatures
  - Test correctness of all published keys in our zone
  - Test correctness of all published keys in the root zone / ITAR
- Test some validating resolver from ISP. Problem: We can't check all recursive name servers on the internet!

# Phase 2: Pioneer Phase

Pioneer phase != Testbed:

- We sign the real .ch / .li zone

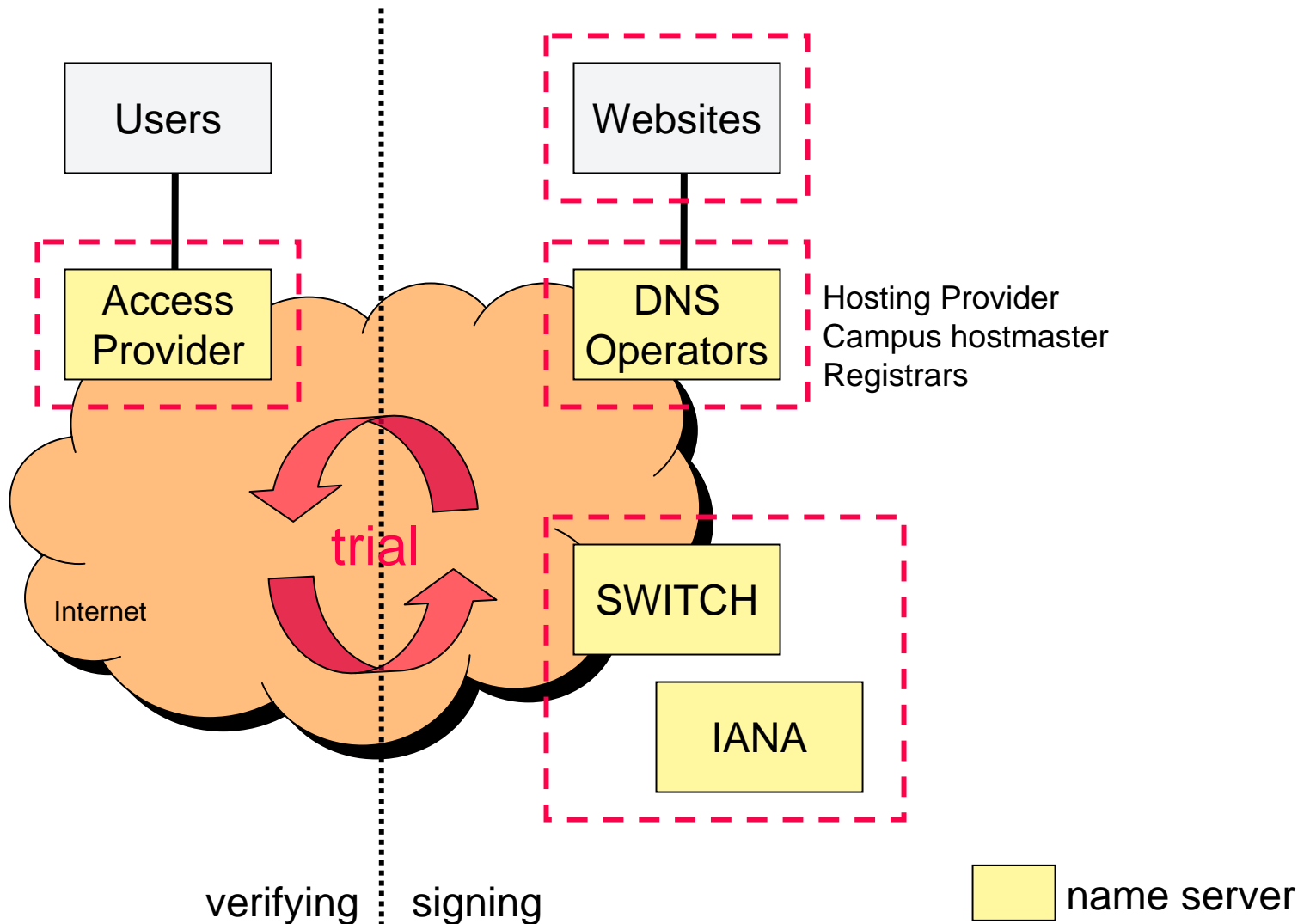
Why:

- Complex topics are hard to sandbox
- New operational processes need real life testing
- Many involved parties (chicken-egg problem)

Desired participants:

- Verifying: Access-Provider / ISP
- Signing: Web-Site operators (Bank/Media/Shops)
- Provisioning: Registrars

# Phase 2: Roles of Participants



# Phase 2: Community

Where we found the “friends & family”:

- Asking on mailing lists
- Talking to friends

What we provide to them:

- Mailing list
- Information meetings
- Bilateral support

What was their motivation of participation:

- Understanding of the new technology!
  - Most have only personal interests (no official company task)
  - In rare cases DNSSEC is a company mission

# Phase 2: Participants

- ~ 40 people (most Security or DNS Operators)
  - Government
  - Banks
  - Media
  - ISP (large public broadband isp) (only resolving)
  - ISP (specialized isp for financial institutes) (resolving and signing)
  - Web-Hosting provider
  - Universities

# Phase 2: Community Problems

- No time for this complex topic
  - Less time for learning -> Need external help
  - A reduced amount of time to implement own tools -> need better tools
- Hardware and DNS infrastructure problem -> same behavior as described in the cost study [1]
- We suspected that signing a zone is easier than enable signature validation. But in reality: No!
  - Signing is a new process (this is much more political)
  - Validation failure impacts more persons; but is also disabled really fast

[1] <http://www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts>



## Phase 2: Community Conclusions

- Most of the participants had no official company mandate
- 6 month is too short to get an official mandate
- Everything depends on few persons. You have to find the right ones!
- Most interested people: public ISP (resolving), ISP for financial customers and banks
- Lessons learned:
  - DNS is a critical but mostly forgotten system
  - We need to establish better communication channels to the large resolver operators in Switzerland

# Phase 2: Technical Results

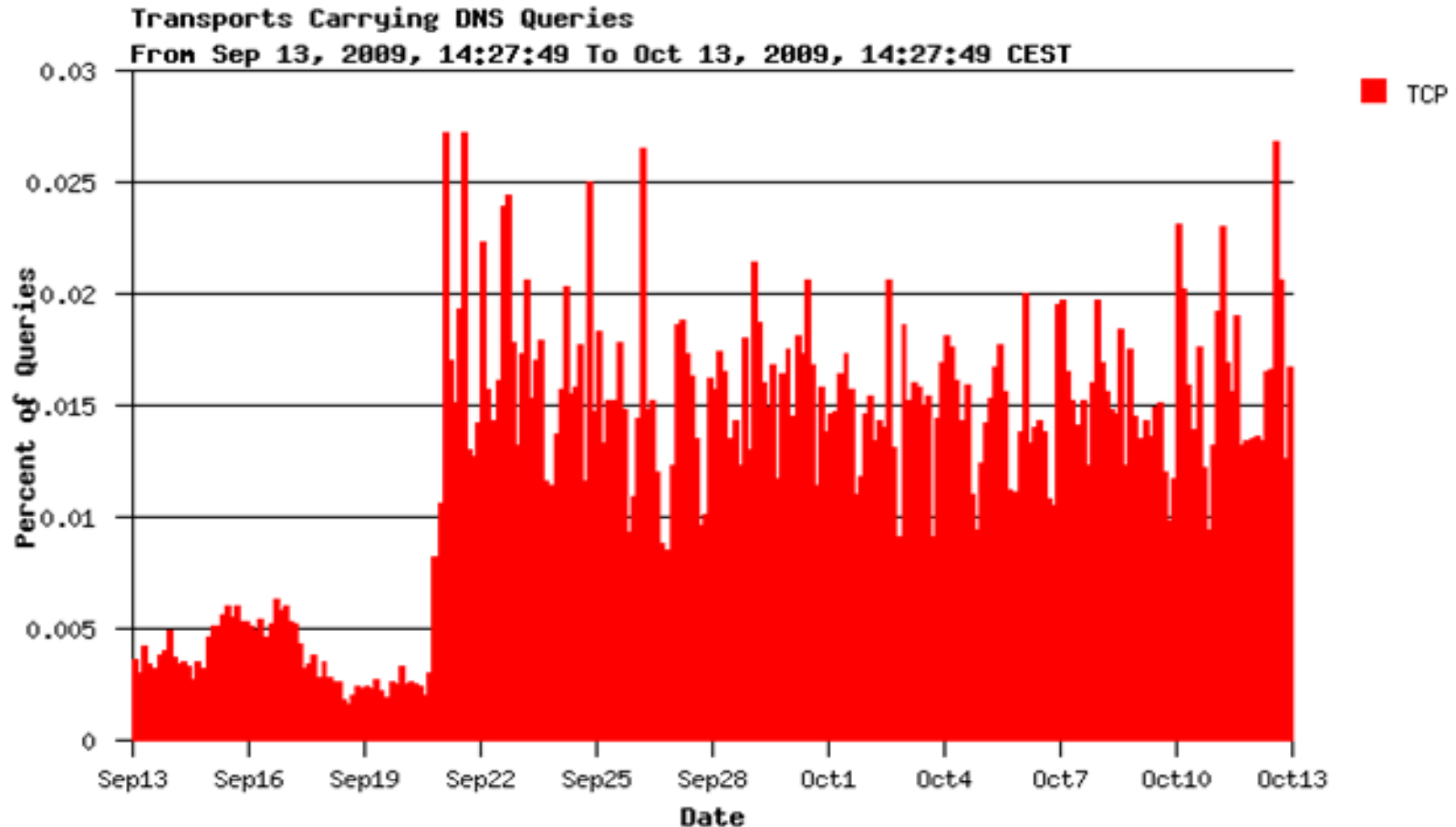
- Technical success:
  - Largest ISP validates DNSSEC signature (51% of all broadband users in Switzerland [1])
  - About 10 signed test domain names
- No grave technical problems recognized!
- Four examples of potential problems
  - Trust anchors update
  - TCP queries
  - Response packet size and home router
  - Fault tolerance with DNSSEC

[1] <http://www.bakom.admin.ch/dokumentation/zahlen/00744/00746/index.html?lang=en>

## Phase 2: Trust Anchors update

- Until the root zone is signed, this is a operational problem
  - Validating resolver operators have to install and update the correct keys
  - Keys from Website, ITAR or DLV ?
- Problem:
  - Install wrong keys; old keys; untrusted dev keys
  - Hard to detect failures; only a few people knows the problem
  - Impossible to monitor for a registry

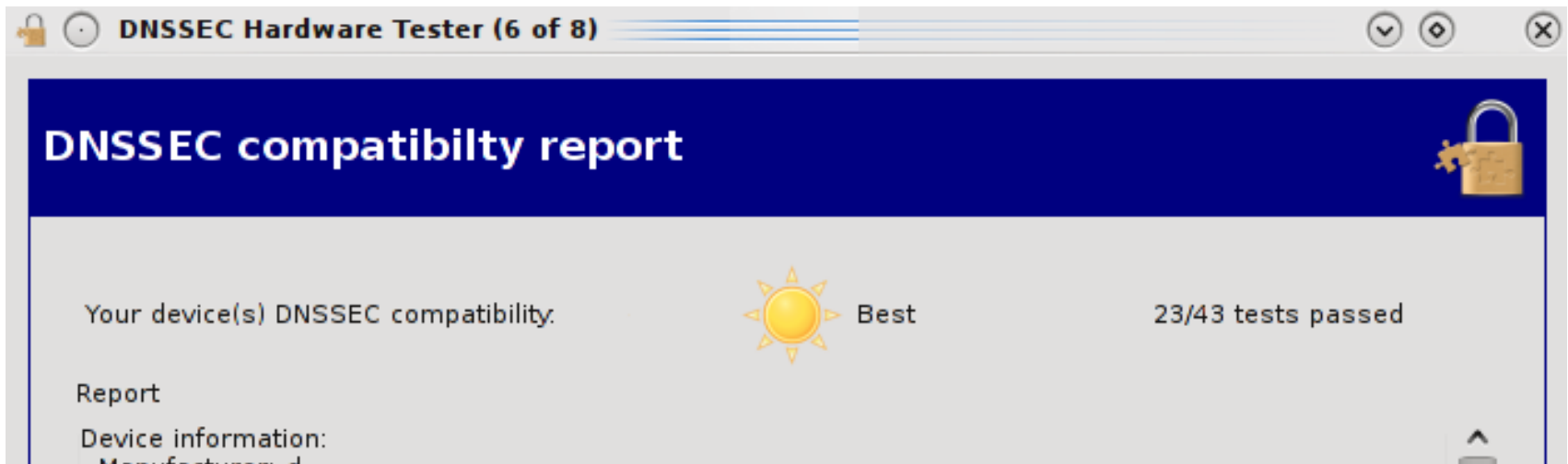
# Phase 2: TCP Queries



- Most of them are NXDOMAIN with EDNS0 (DO) and bufsize = 512

## Phase 2: Validating behind a home router

- We tested the behavior with the most common ADSL router from the participating ISP (SMC SMCA1T-A).
- Tested with hardware tester from <http://www.nic.cz/dnssectests>
- Result:



# Phase 2: Validating behind a home router 2

- Result detail:
  - Act as DNS proxy; announce himself in DHCP
  - Works with EDNS0 and DO/AD flag
  - No TCP
  - No IP fragmentation
- Means: No DNS responses > MTU (~1472 bytes) possible!
- Some response sizes under .ch
  - dig ch. SOA 405 -> dig ch. SOA +dnssec 2522
  - dig ch. NS 371 -> dig ch. NS +dnssec 2315
  - dig switch.ch. NS 173 -> dig switch.ch. NS +dnssec 430
  - dig dsdsdswitch.ch. NS 83 -> dig dsdsdswitch.ch. NS +dnssec 976

# Phase 2: Validating behind a home router 3

- Conclusion:

- No problem during daily usage!
- You will run into problems if you like to validate signatures on the client
- A browser plug-in like this will never work correctly (<http://labs.nic.cz>)



## Phase 2: DNS Fault Tolerance

- There is no DNS fault tolerance with DNSSEC!
- Example:  
sub.switch.ch on same authoritative server than switch.ch  
but without an NS record.

Standard DNS: This will work !

With DNSSEC: sub.switch.ch will be marked as insecure !

Is this really a DNSSEC problem? We learned: DNSSEC isn't complex, but it shows you all "old" failures.



# Phase 3: Provisioning Interface

- What does the provisioning system:
  - Currently: writes NS records to the DNS
  - With DNSSEC: it will also write DS records to the DNS
  - Responsible for NS / DNSKEY / DS exchange between the registrants, registrars and the registry
- Two ways to publish your keys:
  - Web interface on [www.nic.ch](http://www.nic.ch) (for direct customers)
  - EPP interface (extensible provisioning protocol) (for registrars)

# Phase 3: Web Interface

Planned workflow:

Für alle Internetbenutzer | Für Hochschulen | Über SWITCH | Suche:

Registrierungsstelle | Benutzerkonto von Samuel Benz [530949] | Abmelden

Registrierungsstelle > Domain-Namen > Verwalten

**Internet Domains**

- > Domain-Namen
- > Registrieren
- > Warenkorb (0)
- > **Verwalten**
- > Löschen
- > Transferieren
- > Benutzerkonto
- > Bezahlen
- > Mitteilungen
- > Name-Server
- > Domain-Namen-Suche

**Informationen**

1 ändern | 2 speichern | 3 Bestätigung

**Eintrag ändern** ⓘ

Domain-Name	Typ	Status
0x7e.ch	H, R	✓ 15.01.2010, <a href="#">Details</a>

Domain-Name:

Untenstehend finden Sie die Angaben vom Halter, Rechnungs- und technischen Kontakt zu den von Ihnen ausgewählten Domain-Namen. Bitte beachten Sie, dass für gewisse Änderungsanträge eine Bestätigung des Halters notwendig ist.

# Phase 3: Web Interface 2

Planned workflow:

The screenshot shows the SWITCH web interface for domain management. The top navigation bar includes buttons for "Für alle Internetbenutzer", "Für Hochschulen", and "Über SWITCH", along with a search field. The user is logged in as "Benutzerkonto von Samuel Benz [530949] | Abmelden". The breadcrumb trail is "Registrierungsstelle > Domain-Namen > Verwalten".

The left sidebar contains a menu for "Internet Domains" and "Informationen". The "Internet Domains" menu includes options like "Domain-Namen", "Registrieren", "Warenkorb (0)", "Verwalten", "Löschen", "Transferieren", "Benutzerkonto", "Bezahlen", "Mitteilungen", "Name-Server", and "Domain-Namen-Suche". The "Informationen" menu includes "Produkte", "Preise und Bedingungen", "Support/FAQ", "Partner", "Streitbeilegung", and "Statistiken".

The main content area shows a progress indicator with three steps: 1. ändern, 2. speichern, 3. Bestätigung. The current step is "ändern".

The main content area is titled "DNSSEC aktivieren oder verwalten". It contains the following text:

DNSSEC ist eine Erweiterung des Domain-Namen-Systems (DNS), die dazu dient, die Echtheit (Authentizität) und die Vollständigkeit (Integrität) der Daten von DNS-Antworten sicherzustellen. [Mehr über DNSSEC](#)

Wenn Sie DNSSEC für Ihren Domain-Namen nutzen möchten, muss dies zuerst auf den Name-Servern des Domain-Namens konfiguriert werden. Wenden Sie sich an Ihren Webhosting-Provider (Betreiber der Name-Server).

Falls DNSSEC bereits auf den Name-Servern Ihres Domain-Namens konfiguriert ist, können Sie hier DNSSEC aktivieren sowie die DNSSEC-Schlüssel verwalten.

The table below shows the configuration for the domain 0x7e.ch:

Domain-Name	keine Änderung	DNSSEC deaktivieren alle Schlüssel löschen	DNSSEC aktivieren Schlüssel ändern
▶ 0x7e.ch	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Navigation buttons: "<< zurück" and "weiter >>".

# Phase 3: Web Interface 3

- Planned workflow:

Eintrag ändern

Domain-Name		Typ	Status
0x7e.ch	H, R		✓ 15.01.2010, <a href="#">Details</a>

Schlüssel 33577

dnssec.dnskey 257 3 5 AwEAAe2NJ/AvHEK0SMDjOW5xLAljLI/j59lpYMe/mQRv9mP9/wptv9D1CM TB45nji4hEiPRDATyjL7Bn5cGLShGpwGqaCjbQSVpmOIVix5k02k/OYYR0whST5Lf605CbcI3TTBea40 8tQ871qiRfyRe6QWab+wDUmpSBquo82bvj/wkB

DS 5 1 D5B77BDA27B98BFAB9B900F9D9CBCE60125F2613  
DS 5 2 7C2952DF83F6D44EE6A8EBB9E267108A6EFDC9066344BFAAAB74D7D23B64FED6

Schlüssel 22221

dnssec.dnskey 256 3 5 AwEAAaN/6DzaG3nkd8knSg73s9p8DAINmW+g7/sxJyqiLSQh6wF0pSFnXf k84oRk466hxBQOTd10B1xng9IM0lueUonx/Sw1UQm181PYrQVayJdwB22PyOJcPP2VOsTi yYFYA0iUNxJgFOiy+EgZoeXvKOFekKtvjtQ9puiHq9du6Xwz

DS 5 1 89C887BFC15EED8FDF1D81F99347E33EE90D1B5A  
DS 5 2 E3A494A1D2A015077CB0768FAF5C2E90712D8B4151F5AC6DEE07DD3B8929397F8

Schlüssel 56067

dnssec.dnskey 256 3 5 AwEAAbS6sDuaffFsnduih+YWgkx3/01DRXXJ+njxf1vPXyDkKcXhxdqcc 4rA8o84C4oZE/xlmKoGI1edCdAzX/5F0TtL16EO5R8+x7O4A1ohG92ePMwNyB0s57UGqm9J3IehLtfAw 8dXIbS2eC5OKvxpak5VVU1DZ9lazXnAMfeB+cX

DS 5 1 6C6F0661D4DA56E7D028C0212ECAB8118E3EE850  
DS 5 2 F0E3B3D7C017A25D35E37B341487DCC71D64B28E13497F66C54DC6E395803C0B

<< zurück weiter >>

# Phase 3: EPP Interface

- RFC 4310
  - No SWITCH specific extensions
  - RFC 4310 extends the domain object
  - DS record must, DNSKEY record optional
  - We neither validate the submitted DS nor the DNSKEY records, we will write them unchanged to the zone
- Problem:
  - What about a transfer ?

# Phase 3: How to transfer a domain with DNSSEC

3 Options:

1. All registrars must implement DNSSEC (or at least the disable DNSSEC command)
2. The registry silently disables DNSSEC during a transfer to a registrar without DNSSEC support
3. The registry prohibits a transfer to a registrar who does not support DNSSEC (losing registrar had to switch off DNSSEC first)

We decide to implement option 3.

**<http://www.nic.ch/dnssec>**