

Automating the DNSSEC trust anchors using CDS



SWITCH

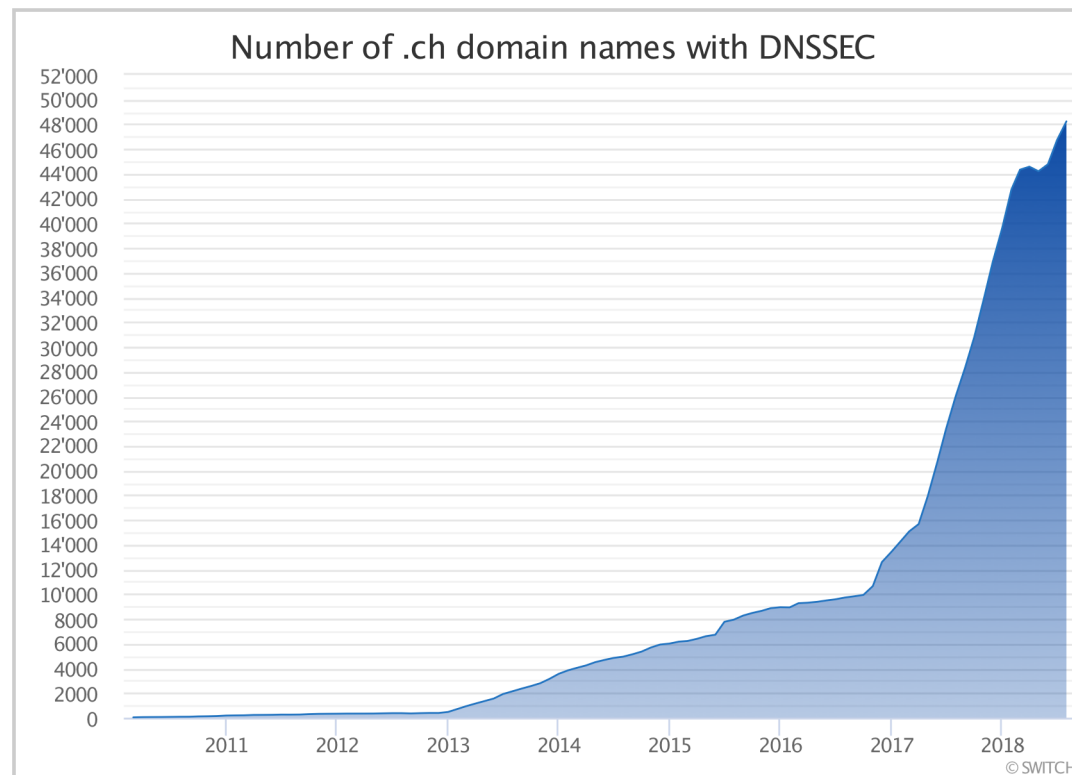
Oli Schacher

oli.Schacher@switch.ch

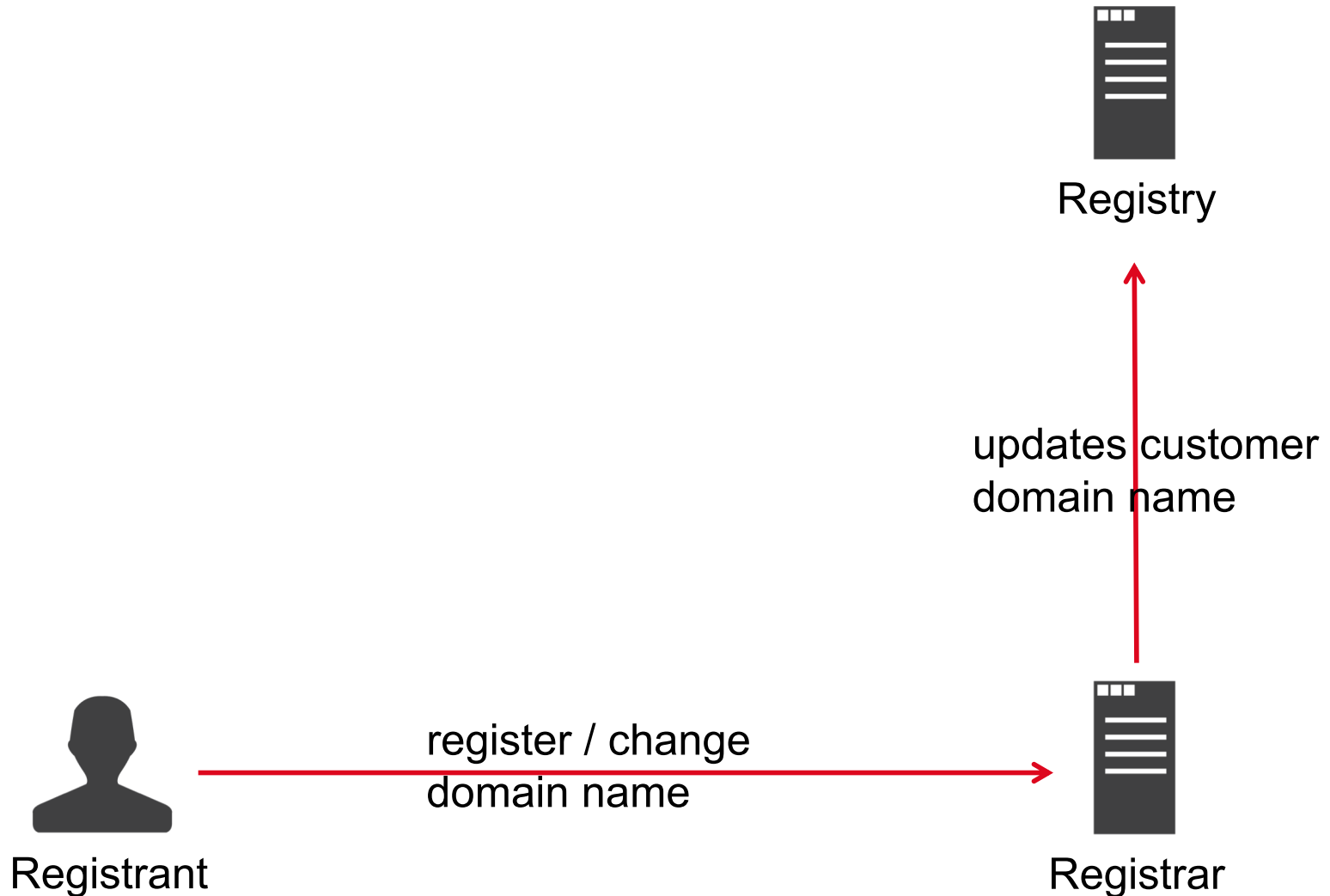
Bern, 18. October 2018

DNSSEC quick recap

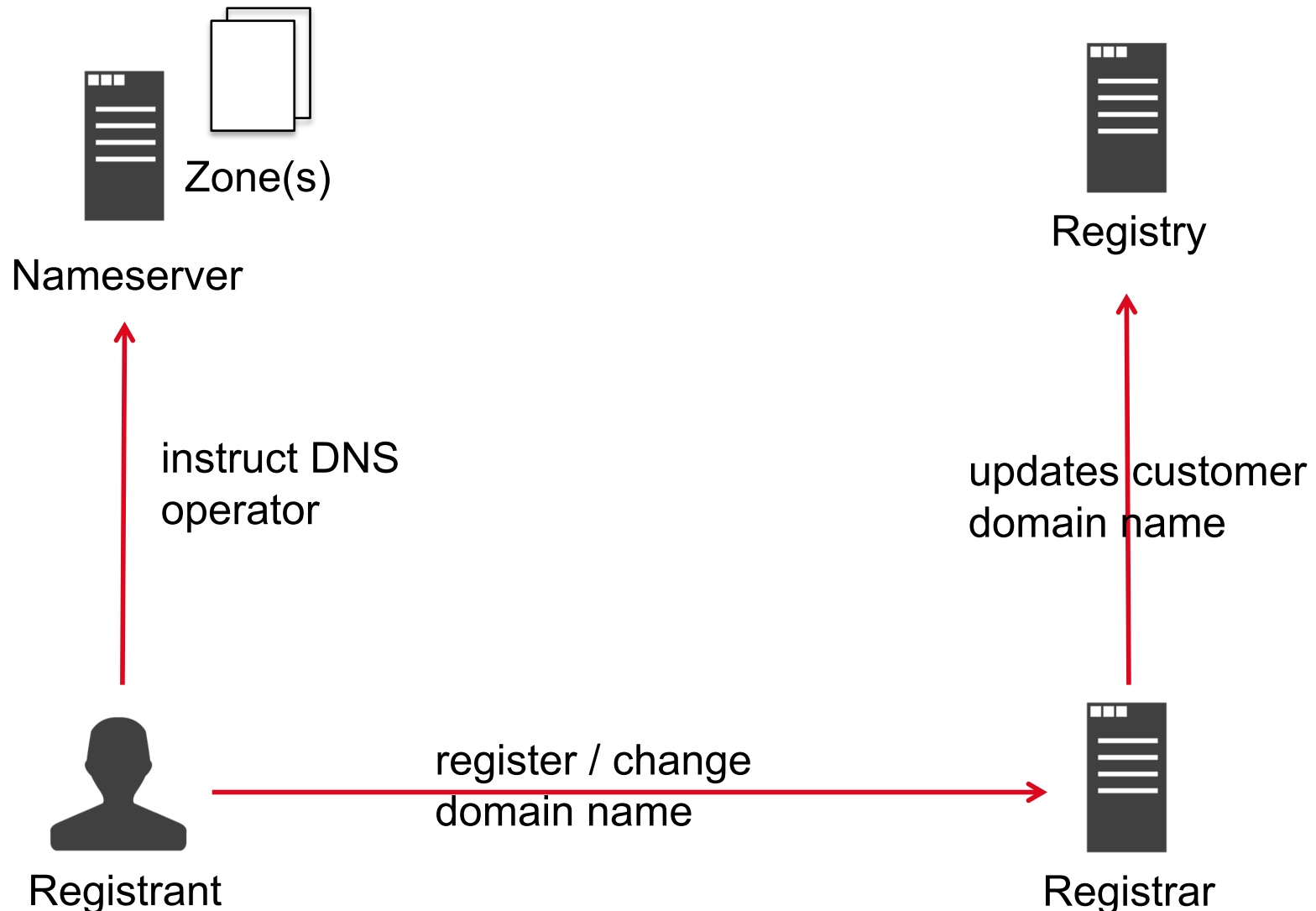
- Detects spoofed DNS answers – they happen !
- Foundation for various other security controls (HTTPS, Secure Email, ...)
- Some hosting companies started to enable by default



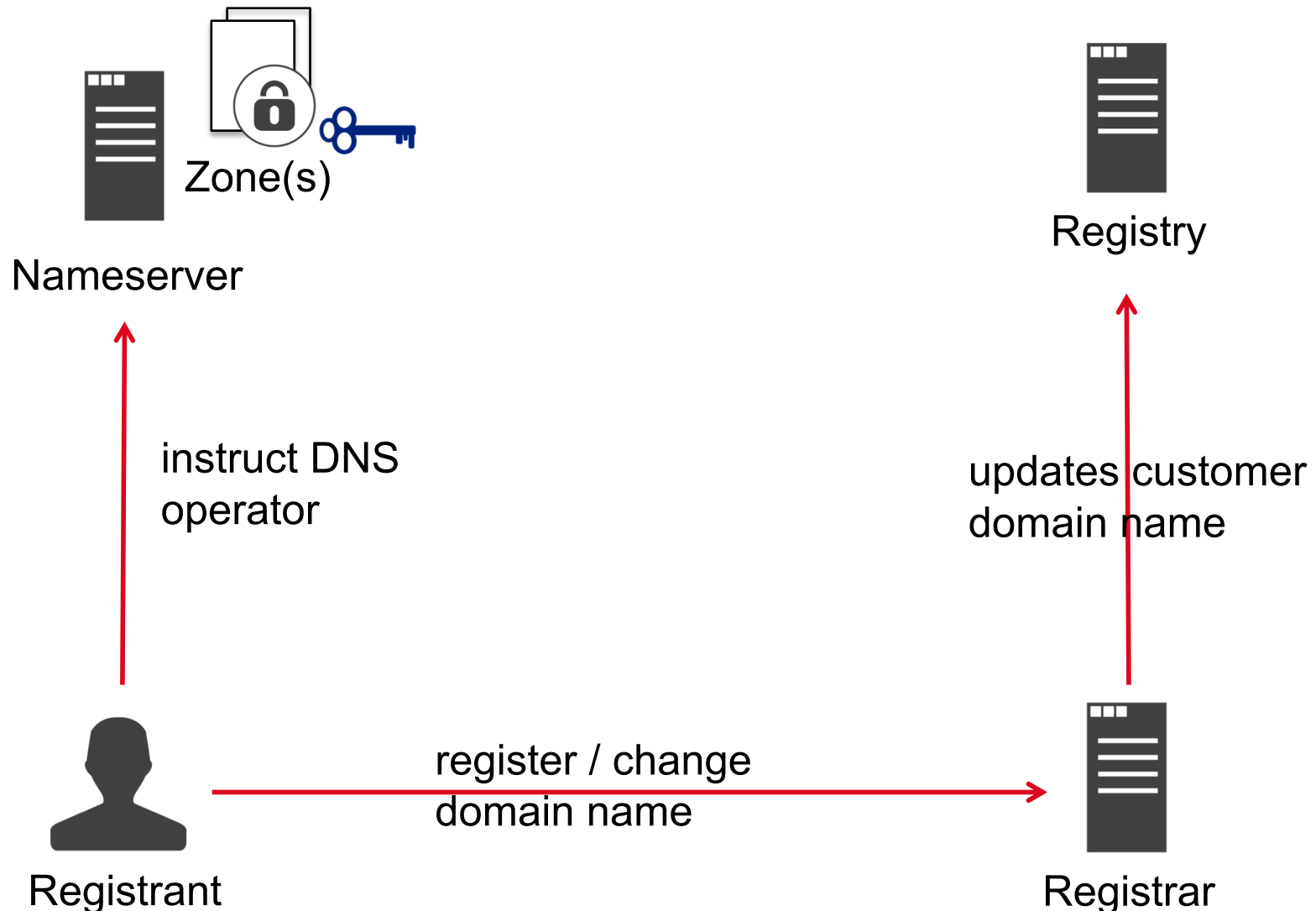
Domain Registration Process



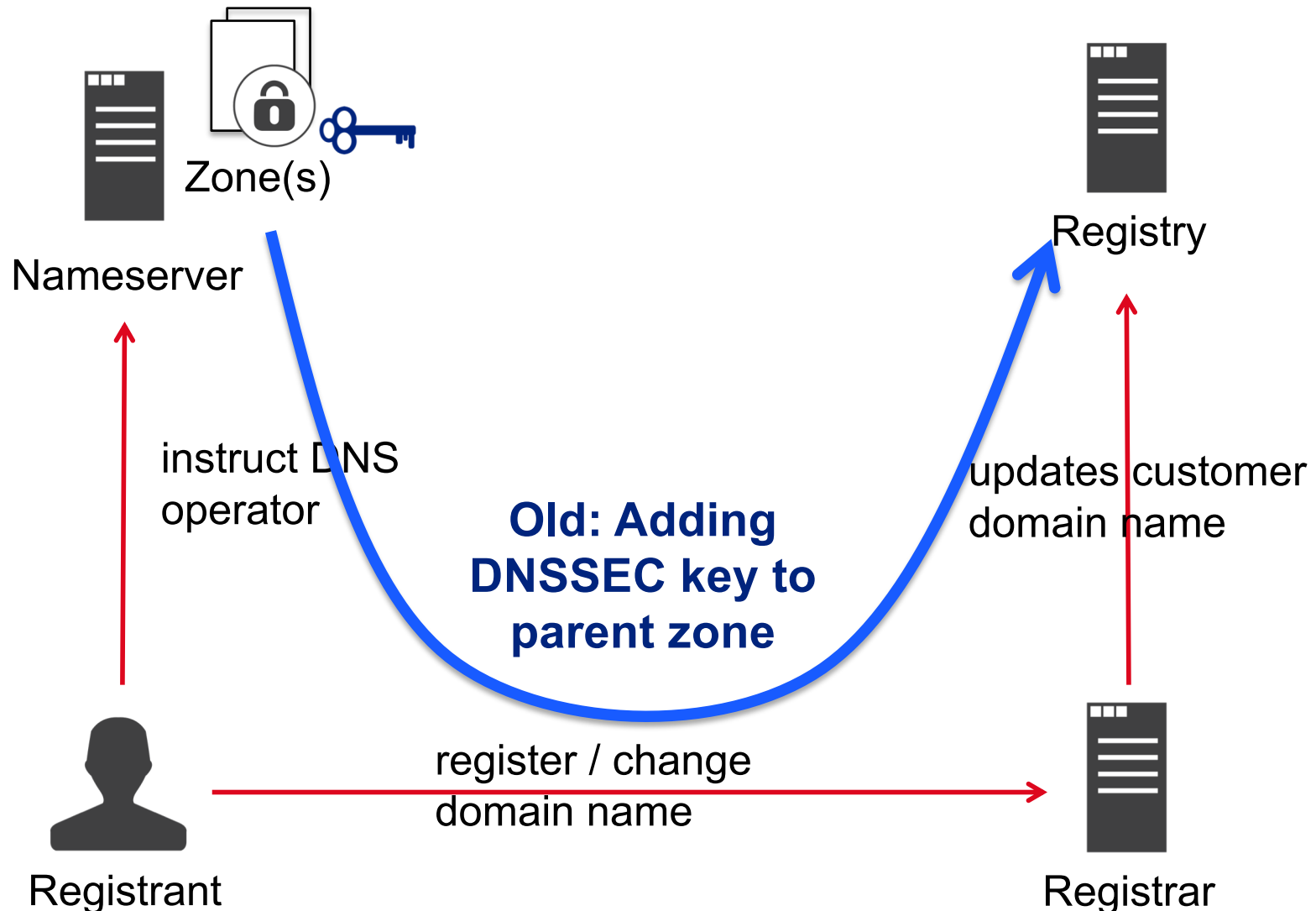
Domain Registration Process



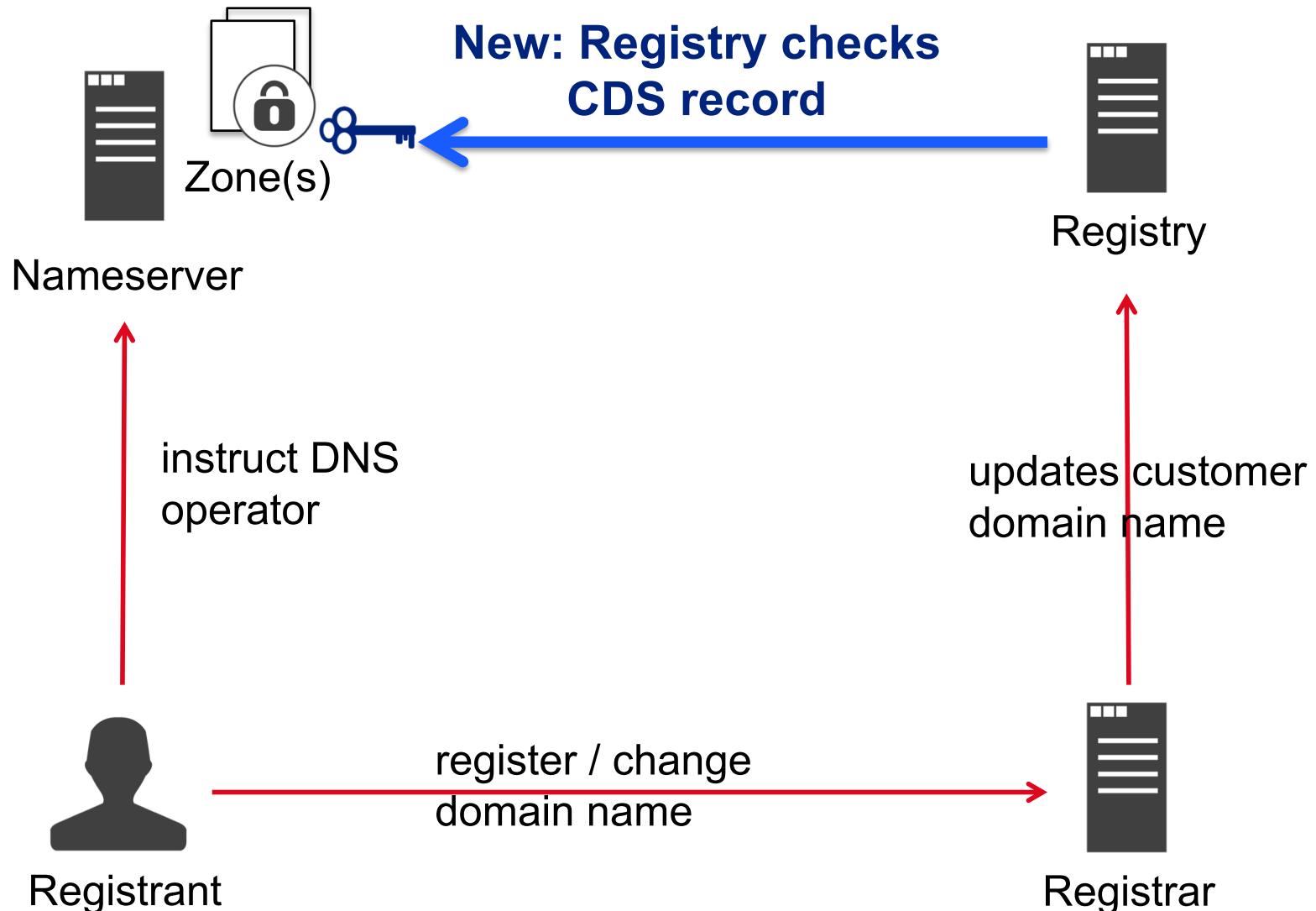
Domain Registration Process



Domain Registration Process



Domain Registration Process



Motivation

- Allow domain operators to automate DNSSEC
- Provide simple method to enable DNSSEC
- Prevent manual key rollover errors by automation
- Show that DNSSEC is easy to use

Note: Automated DNSSEC provisioning is not intended to enable DNSSEC in case your registrar does not support it. For emergency you want an interface from your registrar to edit DNSSEC information instantly.

How to sign a zone?

Example configuration for knot [1] name server software :

...

template:

- id: default
- storage: /var/lib/knot

zone:

- domain: example.ch

[1] <https://www.knot-dns.cz/>

How to sign a zone?

Example configuration for knot name server software :

...

template:

- id: default
- storage: /var/lib/knot
- dnssec-signing: on**

zone:

- domain: example.ch

How to sign a zone?

Example configuration for knot name server software :

...

template:

- id: default
- storage: /var/lib/knot
- dnssec-signing: on**

zone:

- domain: example.ch

Default DNSSEC Policy

algorithm: ecdsap256sha256
single-type-signing: off
ksk-lifetime: 0
zsk-lifetime: 30
cds-cdnskey-publish: always

How to sign a zone

Example for PowerDNS authoritative server

```
pdnsutil secure-zone einbeispiel.ch  
pdnsutil set-publish-cds einbeispiel.ch 2
```

Automatic DNSSEC via CDS processing

What we implemented

- **RFC 7344** - Automating DNSSEC Delegation Trust Maintenance, September 2014
- **RFC 8078** - Managing DS Records from the Parent via CDS/CDNSKEY, March 2017

How we implemented it

Step 1: Getting the CDS data

Zone is already secure:

1. CDS checked via validating resolver
2. CDS must not change for 3 days

Zone is not secure (no DS in parent):

1. Auth. servers as provided in registry are checked on all their IP addresses
2. These name server must respond with a consistent result
3. DNS query sent over TCP only
4. Name server checked from multiple vantage points
5. CDS must not change for 3 days

How we implemented it

Step 2: Verifying the CDS data

1. CDS only accepted if it does not break trust chain
2. DNSSEC algorithm supported: 5, 7, 8, 10, 13, 14, 15, 16 and 0 for deletion
 - <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml>
3. Digest Type supported: 1, 2, 4 or 0 for deletion
 - <https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml>

How we implemented it

Additional information

- DS record via EPP from registrar overwrites registry data, CDS record re-evaluated if newer than last EPP update
- Accepted CDS signaling changes are also sent to registrar using EPP poll messages
- No communication by email to registrant or technical contact. However, we provide a status portal:
<https://www.nic.ch/de/faqs/dnssec/cds/>

Status Portal

CDS Status Check

Status of CDS Publication

Enter a .ch or .li domain name here to check whether the DNSSEC related changes signaled via CDS are valid and will be published.

Please note: Until early 2019 we are in a pilot phase to give our registrars time to adapt to the recently implemented Automated DNSSEC Provisioning process. This means that the process isn't activated for all registrars yet and so the verification of the change could fail.

<https://www.nic.ch/de/faqs/dnssec/cds/>

Status Portal

✔ Success! A CDS record for the domain name **dnssectests.ch** has been found.

Domain name	dnssectests.ch
State	PENDING
Expected processing	12 October 2018
Type of change	BOOTSTRAP
Last scan run	09 October 2018 10:30
Unchanged since	09 October 2018
Scan runs	1 (at least 3 scan runs and 3 days since first "Unchanged since" date are required for the change to be activated)
Checked name servers	cds-auth-test.servername.ch / 2001:620:5ca1:1f0:f816:3eff:fed6:b706 cds-auth-test.servername.ch / 86.119.39.55

Valid Record Set

CDS 9508 13 2 70CB27735E6B115920C43AE3E9F3217C5E210A6260C7606498FA290315BA16C7

Who is using it already?

- Over 900 .ch domain names publish a CDS record set as of end of Sept 2018
- Top 10 by registrars

Registrar	#
Gandi SAS	219
Infomaniak Network SA	113
switchplus AG	96
Hostpoint AG	63
1API GmbH	52
OVH	48
METANET AG	41
cyon GmbH	28
NetZone AG	25
united-domains AG	23

Top 3 by DNS operator

Registrar	#
cloudflare.com	574
googledomains.com	113
internezzohosting.ch	24

DNSSEC sign your zone

- DNSSEC sign your zones
- Turn on DNSSEC validation on your resolver
- Don't be on Team Telnet

Team Telnet

noun

1. a member of a computer user community which continues to use insecure communication protocols

Questions

More information about
Automated DNSSEC provisioning at
<https://www.nic.ch/faqs/dnssec/cds/>

Appendix

How to sign a zone?

Example configuration for knot name server software :

remote:

- **id: google**
address: ["8.8.8.8"]

submission:

- **id: validating-resolver**
parent: google

policy:

- **id: default**
ksk-submission: validating-resolver
ksk-lifetime: 365d

template:

- **id: default**
storage: /var/lib/knot
dnssec-signing: on

Needed for KSK key rollover

Allows name server to detect whether parent is ready