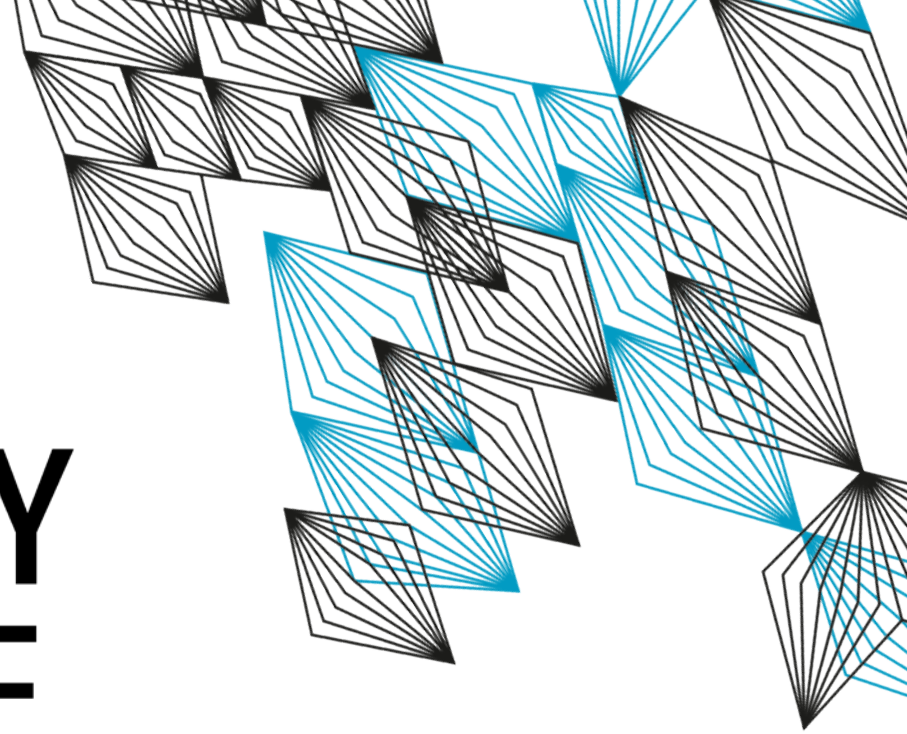


UNIVERSITY OF TWENTE.

THE STATE OF DNSSEC AUTOMATED PROVISIONING

RESEARCH PROJECT BSC TECHNICAL COMPUTER SCIENCE

WILCO VAN BEIJNUM – A.C.W.VANBEIJNUM@STUDENT.UTWENTE.NL

SOFTWARE SUPPORT

- Parent side
  - Authoritative software
  - Registry software
  - Scanners
- Child side
  - Authoritative software

Software	Parent side Auto update DS	Child side Auto update CDS/CDNSKEY
BIND 9	Using tool	Using tool
Knot DNS	No	Yes
MaraDNS	No	No
NSD	No	No
PowerDNS Authoritative Server	No	Using tool
YADIFA	No	No
BIG-IP DNS	No	Using UI
FRED	Yes	Not applicable
Nomulus	No	Not applicable
cdnskey-scanner	Not applicable	Not applicable
rcdss	Not applicable	Not applicable

TLD SUPPORT

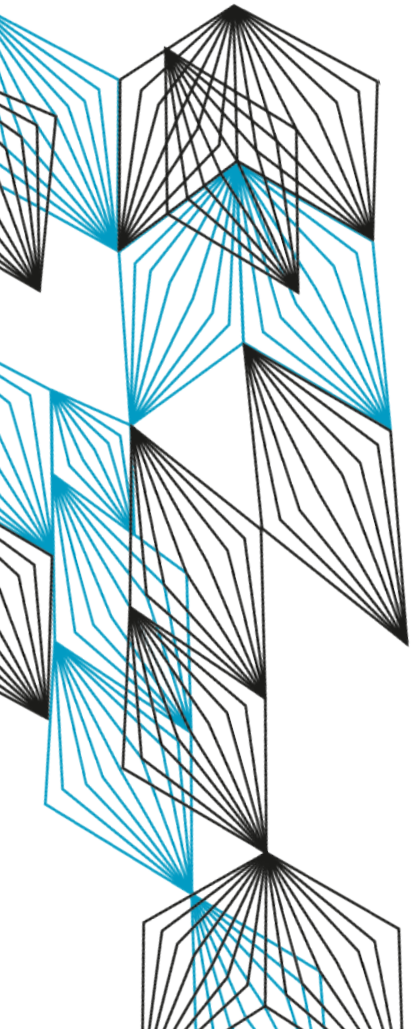
Registry	CDS	CDNSKEY	Bootstrap from insecure
.ch	Yes	No	3 days TCP-only
.cr	No	Yes	7 days TCP-only
.cz	No	Yes	7 days TCP-only
.li	Yes	No	3 days TCP-only
.sk	Yes	No	3 days

- Current support:
- Planned support: .ca, .cl, .dk, .fi, .nu, .pt, .se
- Lack of demand, priority and resources

DOMAIN SUPPORT

- Analysis of OpenINTEL dataset
  - .ch
    - 7.2% DNSSEC usage, 0.75% CDS record usage
    - CDS is actively used to enable and disable DNSSEC, but not much
    - Only some Swiss DNS providers seem to automatically publish CDS records
    - Malformed CDS records: ZSK; no corresponding DNSKEY
  - Alexa 1M
    - 2% DNSSEC usage, 2% CDS record usage, 1.7% CDNSKEY usage
    - .com largest number of domains with CDS/CDNSKEY
    - .dev largest percentage of domains with CDS/CDNSKEY

CONCLUSION



REFERENCES – SOFTWARE SUPPORT

Authoritative DNS software

BIND 9 (9.13.3) - https://www.isc.org/bind/

Knot DNS (3.0.5) - https://www.knot-dns.cz/

MaraDNS (3.5.0019) - https://maradns.samiam.org/

PowerDNS Authoritative Server (4.4.1) - https://www.powerdns.com/auth.html

YADIFA (2.4.2) - https://www.yadifa.eu/

BIG-IP DNS (16.0.1) - https://www.f5.com/products/big-ip-services

Registry management software

FRED (2.42) - https://fred.nic.cz/en/ | https://fred.nic.cz/documentation/html/Concepts/AKM.html

Nomulus (20210520-RC00) - https://github.com/google/nomulus/

Scanners

cdnskey-scanner (14-12-2020) - https://gitlab.nic.cz/fred/cdnskey-scanner/

rcdss (0.7) - https://github.com/RIPE-NCC/rcdss/

REFERENCES – TLD SUPPORT

.ch/.li - https://www.nic.ch/export/shared/.content/files/SWITCH_CDS_Manual_en.pdf

.cz - https://www.nic.cz/page/3909/automatizovana-sprava-keysetu/

.sk - https://sk-nic.sk/sk-nic-has-launched-a-technological-innovation-as-the-third-country-in-europe/

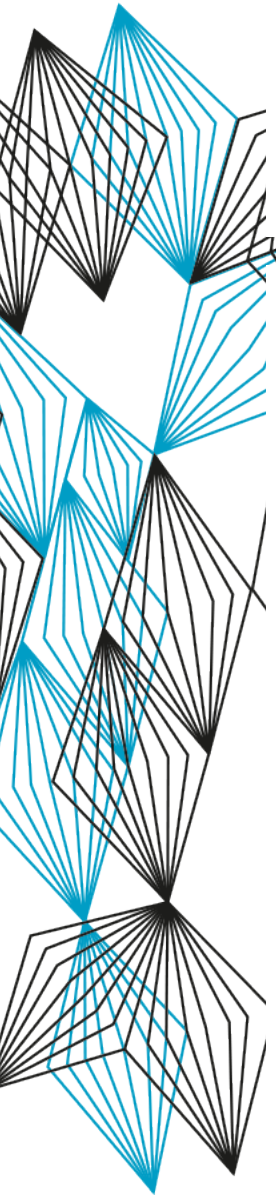
.pt - https://www.dns.pt/fotos/editor2/relatorios/pa_2021.pdf

.se/.nu - https://internetstiftelsen.se/dns-labs/projects/

REFERENCES – DOMAIN SUPPORT

OpenINTEL - https://openintel.nl/

REFERENCES – .CH DATASET



Total number of domains: ~2,100,000

Number of domains using automated provisioning
~7.2% using DNSSEC, ~0.75% have CDS record published

Using CDS to disable DNSSEC
Used by roughly ~5 domains per month. Found some development websites, most are ‘normal’ websites. In total ~250 domains found with a CDS DELETE record.

Using CDS to enable DNSSEC
~11% of new domains is using DNSSEC. ~0.2% of new domains (~2% of domains using DNSSEC) likely enabled DNSSEC using automated provisioning.

CDS and CDNSKEY publishing by nameserver
Pretty much all nameservers/DNS providers with a high number of domains with automated provisioning are Swiss. The largest 20 providers all have an automated provisioning usage of <= 2%, apart from Cloudflare, which has a usage of 7%. Another larger DNS provider outside the Swiss is Google’s Cloud DNS, which has a 12% automated provisioning usage.
In the time period of the obtained data, no significant changes have been found that indicate providers that started supporting CDS/CDNSKEY.

REFERENCES – .CH DATASET

Algorithm and digest usage
By far the most used algorithm is ECDSAP256SHA256, with ~95% usage at domains with a CDS record. This is followed by RSASHA256 with ~2% usage and RSASHA1-NSEC3-SHA1 with 1.7% usage. Finally, 1.1% of domains is using a DELETE record.

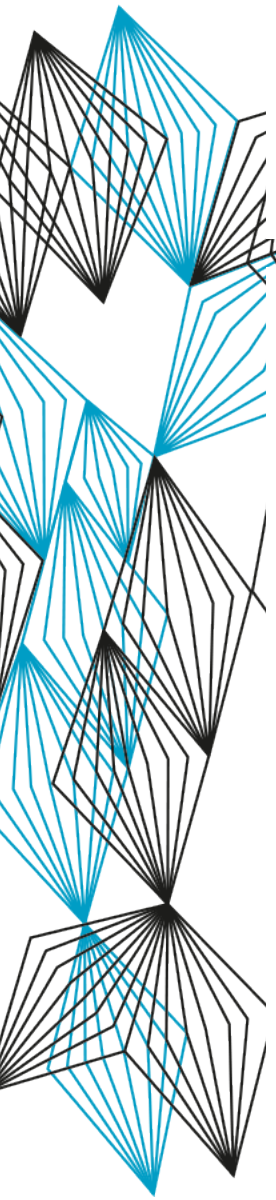
Digest usage is a bit more divided, with ~53.6% using SHA-256 and ~32.1% using SHA-384. This is followed by 13.2% SHA-1 and again 1.1% DELETE.

Key types
3 domains were found that had a ZSK in their automated provisioning records.

CDS without DNSKEY
~20 domains were found that have a CDS key without a corresponding DNSKEY. Most of these domains had a key tag value of 0 (without an algorithm value of 0, so no DELETE record). These domains were all managed with the DNS provider dnsimple.

Nameserver software usage
Nameservers that have domains with automated provisioning seem to be mostly using PowerDNS, which is running on 67% of the domains. It is noteworthy that for 31.2% of the nameservers, the used software could not be identified. For nameservers that have no domains with automated provisioning, 80.7% of nameservers is running unknown software. For 9.9% of the nameservers the PowerDNS software was identified and for 9.3% BIND 9.

REFERENCES – ALEXA 1M DATASET



Total number of domains: ~790,000

Number of domains using automated provisioning
~2.1% of domains using DNSSEC, ~2% of domains have a CDS record published, ~1.7% of domains have a CDNSKEY record published. About half of the domains that publish a CDS or CDNSKEY record does not currently have DNSSEC enabled.

CDS and CDNSKEY publishing by nameserver
Again, the most predominant CDS/CDNSKEY publishers are Cloudflare and Google Cloud DNS with respectively 8% and 24% of domains.

Algorithm and digest usage
Algorithm usage is a bit more divided than .ch. 59% of CDS and 72.6% of CDNSKEY records is using ECDSAP256SHA256. 20.5% of CDS and 3.1% of CDNSKEY records is using RSASHA256. Finally, there are a lot of domains with a DELETE algorithm, 19% of CDS records and 24.3% of CDNSKEY records.

Automated provisioning usage per TLD
By number of domains with a CDS and/or CDNSKEY record, the .com TLD has the largest number of domains, followed by .io, .ir and .in. However, in comparison with the total number of domains for these TLDs it is a negligible number of domains.
After filtering out TLDs with less than 10 domains in the dataset (which was not deemed representative), it was found that .dev is the most predominant TLD by means of percentage of domains using automated provisioning, namely 12.9% of 520 domains.

REFERENCES – ALEXA 1M DATASET

Nameserver software usage

The software for nameservers that have domains with automated provisioning is largely unknown. For 99.6% of the nameservers, no software could be identified. For nameservers that have no domains with automated provisioning, 72.9% of nameservers is running unknown software. For 14.2% of the nameservers the BIND 9 software was identified and for 12.7% PowerDNS.