Switch_

Report 2024

of the registry for the ccTLDs .ch and .li

Table of contents

The cost of critical DNS infrastructure can no longer be covered by volume growth alone.

Urs Eppenberger
Head of Registry, Switch

Editorial

Urs Eppenberger, Head of Registry

The world of domain names is currently in a consolidation phase, and the registries in particular are hoping for a boost from the next round of top-level domain names, which are due to be introduced in 2026. However, this is unlikely to have any impact on the quantity structure of .ch domain names.

During the pandemic, we saw a huge increase in digitization. But now that this period is well and truly over, private holders are starting to consolidate the domain names they hoarded at that time, resulting in lower overall growth and lower revenues for registrars. Possible marketing strategies by web hosts and registrars could raise awareness among businesses of how an individual web presence with their own domain name can strengthen their brand and give them control over their offering. However, if companies choose to offer their products or services through the major sales platforms, they do not need their own website or domain name. The advantage of these sales platforms is their size and global reach, so it is hard to predict which sales channel will win.

The discussion of growth or stagnation is relevant for registrars and registries because of the need to cover costs caused by inflation, increasing demands on infrastructure resilience and compliance requirements. Costs can no longer be covered by volume growth alone.

The 2.6 million registered domain names, the name servers and the resolvers of the Internet service providers form a key infrastructure for the Swiss economy and population. They must therefore be maintained and protected. The requirements for this are laid down in the National Cyber Strategy and the Swiss Telecommunications Act. The registry and the registrars are fully capable to take care of the technical aspects. In consultation with the relevant authorities, we will identify and implement the most efficient measures to secure and further develop this infrastructure.

1.

Activity report – operations

Combating cybercrime

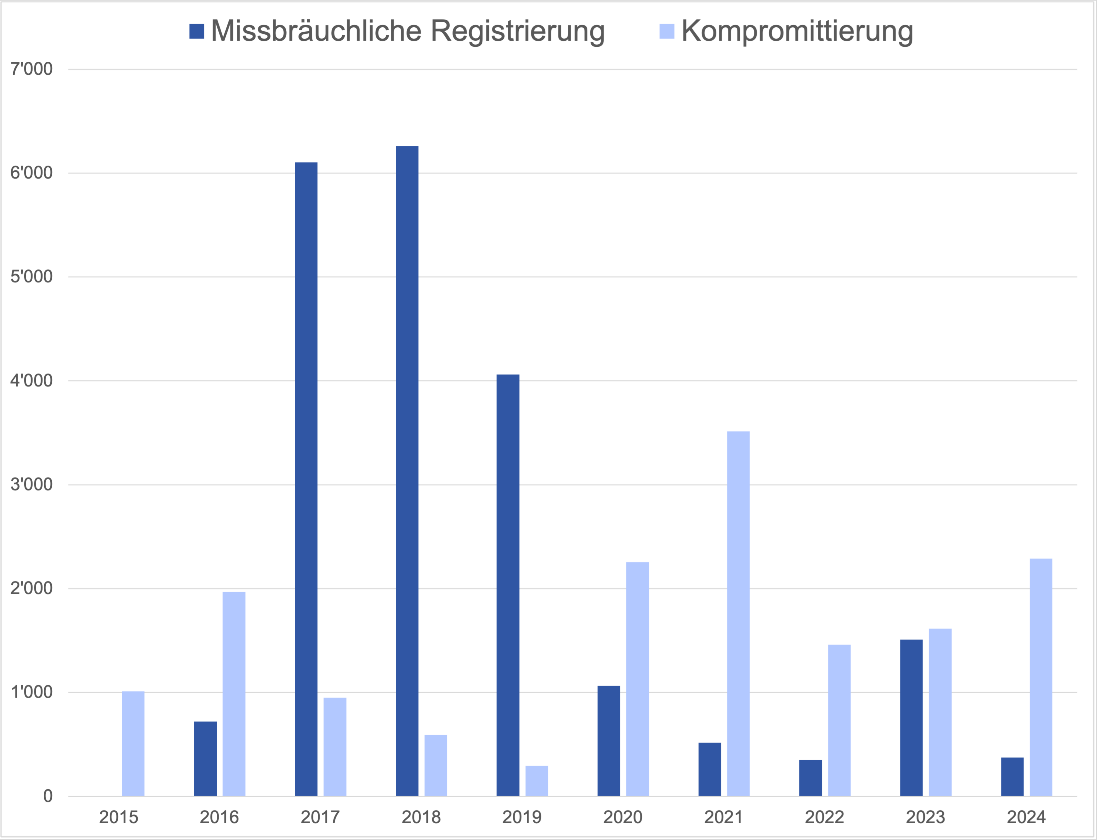
Compromised websites

The number of compromised websites used for phishing and malware has increased compared to last year. The majority of these websites were detected by the Web crawler developed specifically for the .ch zone.

Improper registration

The number of domain names reported as suspected improper registrations has decreased. One reason for this is that Fedpol has sent fewer requests under Art. 15 OID as part of its SWITCHoff project. The number of requests under Art. 16 OID has also decreased.

Website: https://www.saferinternet.ch/



Measures in the event of suspected abuse

Requests from recognised authorities – OID Art. 15.1

In 2024, accredited authorities submitted a total of 66 requests under OID Art. 15.1 for immediate blocking (technical/administrative) of domain names related to phishing. There were no requests related to malware.

Requests	Consequences	2024
Not answered	Domain name deleted	65
Answered	Domain name reactivated	1
Total		**66**

All authorities recognised by OFCOM are listed on the following website: Recognised authorities

Administrative assistance – OID Art. 16.3

At the request of an intervening Swiss authority acting within its jurisdiction, 310 requests were submitted for Swiss correspondence addresses under OID Art. 16.3.

Requests	Consequences	2024
Not answered	Domain name deleted	246
Answered	Domain name reactivated	64
Total		**310**

Security awareness – iBarry and SISA

In collaboration with SISA, Switch continues to help raise awareness among the Swiss population. With its three new information campaigns (passkeys, the new Swiss Data Protection Act, deepfakes), iBarry.ch provides information, guidance and support for anyone who is uncertain or has questions about Internet security.

https://checkawebsite.ibarry.ch

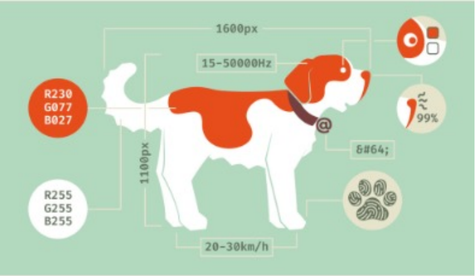
https://ibarry.ch

To optimise the services offered to the Swiss population and to better position the iBarry platform, SISA once again took part in this year's survey of Swiss Internet users.

https://cyberstudie.ch

A new iBarry newsletter will be launched this year to provide its community with all the latest information.

→ Sign up here



Security awareness – SISA anniversary

This year, the Swiss Internet Security Alliance (SISA) has once again set itself the goal of bringing together the key players in Swiss Internet security and keeping the Swiss population safe.

Since mid-2024, members have also been able to obtain crypto-fraud URLs via the existing SISA phishing feed. NEDIK collects and shares this data together with Mute Group.

New members and partners in 2024:

NEDIK

CLUSIS 1989

Zürcher Hochschule
für Angewandte Wissenschaften
zh aw

SBB CFF FFS

cyon

ISC2 CHAPTER

SISA celebrates its 10th anniversary

The Swiss Internet Security Alliance was launched in 2014 by a group of leading industry figures with a shared vision of making Switzerland the most secure Internet country in the world.

Members of the SISA board (from left): Simon Seebeck (Die Mobiliar), SISA President Katja Dörlemann (Switch), Rita Frei (Sunrise), Marcus Beyer (Swisscom). Not pictured: Fabian Ilg (Swiss Crime Prevention).
Photo: Netzmedien

Security Awareness Day

On 24 October 2024, Switch hosted the seventh Swiss Security Awareness Day. This year, iBarry.ch was once again a partner of the conference, which is growing every year. Around 130 attendees were able to network with other experts during various networking breaks between the exciting presentations.

For the first time, attendees were also able to participate in hands-on workshops.

Once again, the aim of this year’s programme was to increase awareness of security-related issues within the Switch community, while also sharing ideas and encouraging communication and interaction.

All presentations are available online.

Security Awareness Adventures

The Switch Security Awareness Adventures

‘Hack the Hacker – the escape room’ was the first of three Switch security awareness adventures, followed by ‘Track the Hacker – the scavenger hunt’ and ‘Piece of Cake – the role play’. The adventures continue to be very popular.

In 2024, Switch hosted a total of 77 of these interactive security training sessions, almost twice as many as in 2023 (40 sessions), and shared its training game expertise at numerous conferences.

Website: https://swit.ch/security-awareness-adventures

Security awareness – Podcast

Podcast: Security Awareness Insider

In December 2024, the 50th episode of the ‘Security Awareness Insider’ podcast (in German) was released.

In this podcast, Katja Dörlemann (Switch) and Marcus Beyer (Swisscom) talk about raising employee awareness of security issues, new and creative methods, tools and training approaches, provide insights into security awareness programmes of companies and organisations, and much more.

Since its launch, the podcast has been downloaded almost 25,000 times, with an average of 450 downloads per episode.

You can find it on any podcast platform, or here: https://www.securityawarenessinsider.ch

Swiss Web Security Day

On 29 October 2024, Switch, together with SISA and Swico, organised the Swiss Web Security Day in Bern, which ran alongside the LEO event with Swiss Law Enforcement authorities. With 79 participants from Switzerland and abroad, the event was a great success and received very positive feedback.

In the morning, there was a presentation on crypto investment fraud by the Central Office for Cybercrime Bavaria. Another presentation was on 'Internet-wide deployment of post-quantum cryptography for security protocols'.

In the afternoon, there were talks on DNS abuse and a presentation of a legal dispute that confirmed the self-regulation of the Swiss hosting industry (Swico Domain Names Code of Conduct).

Like last year, the event took place in person in Bern.

Katja Dörlemann, SISA President, Urs Eppenberger, Head of Registry Switch, Claudius Röllin, Swico IG Hosting. Photo: Netzmedien

LEO event
Cooperation with Law Enforcement authorities

Target group

To continue its support of the authorities in the fight against cybercrime, Switch held its fourth LEO event this year. LEO stands for 'Law Enforcement Organisations'.

On 29 October 2024, the Law Enforcement community met in Bern, with the goal of strengthening the community and promoting the development of partnerships with private sector CERTs. This cooperation is crucial in the fight against cybercrime.

Therefore, in addition to 59 members of the LEO community, 40 representatives of Swiss CERTs (CH-CERT) attended the event. Many of the participants attended last year's event and brought along interested colleagues with them.

The distribution between the regions was very balanced. The participants came from police forces, public prosecutor's offices and the Liechtenstein National Police. Authorities such as Swissmedic, Seco, Finma and OFCOM were also represented.

Topics

Various topics were covered. Participants discussed current developments and projects related to domain abuse and cybercrime. Processes and interfaces to simplify cooperation were also covered.

The focus was on cooperation with relevant stakeholders beyond the community to prevent cybercrime. Several cases were presented that have been successfully and efficiently solved through this cooperation.

Feedback

The event was a superb success. The exchange between both sides has increased significantly. The event is gaining more and more interest every year and participants are already looking forward to next year. We will focus increasingly on concrete examples to promote this interdisciplinary cooperation.

Registry operations

Interruption of the registration system

The registration system experienced an interruption on 19 January 2024. Between 7:50 a.m. and 8:39 a.m., the registrars were not able to access the EPP interface. The interruption was resolved by switching to the standby system.

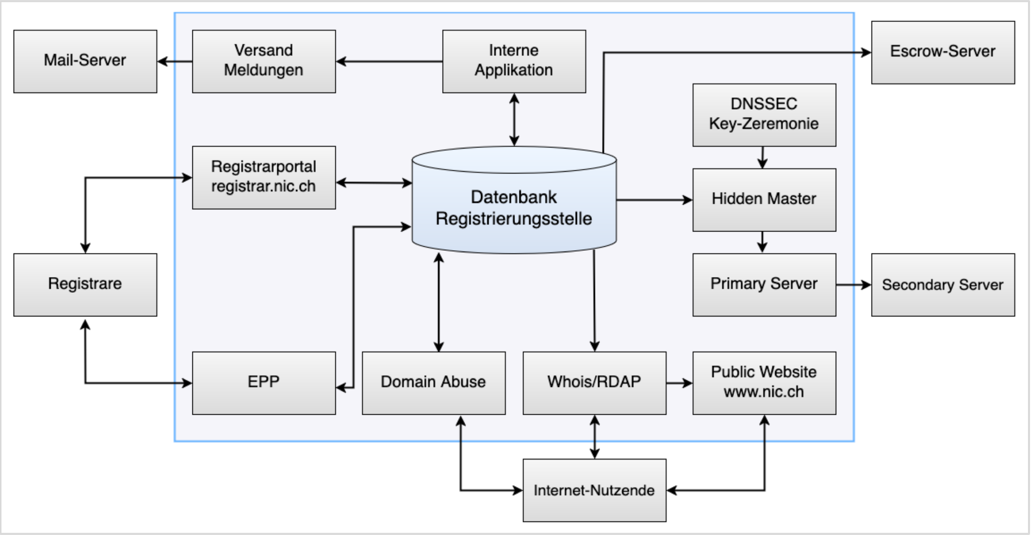
The fault was caused by a manipulation error during scheduled standard maintenance on the underlying server platform in Lausanne. Because this error affected the central database, automatic switchover to the standby system in Zurich could not take place.

After a 49-minute downtime, the registration application was up and running again in Zurich without any loss of data. The name servers were not affected by the outage and the zone file was always up to date.

Registration Data Directory Service (RDDS) outage

A software error on the Whois server led to excessively large log entries due to faulty connections/clients, resulting in the hard disk becoming full. This in turn led to the downtime of the server that provides the services whois.nic.ch and rdap.nic.ch. The administration and allocation of domain names was possible at all times and was not affected by this disruption.

System overview and scope of the registry



European TLD ISAC

The European TLD Information Sharing and Analysis Centre (ISAC) was established in 2023 under the umbrella of CENTR.

The European Top Level Domain Information Sharing and Analysis Centre (TLD ISAC) aims to promote the security and resilience of top-level domain registries in Europe through information sharing, cooperation and exchange of best practices.

It brings together operators, security experts and other stakeholders to share threat information, identify emerging trends and develop proactive measures to prevent and respond to cyber attacks.

Switch, together with other European ccTLD operators, is a founding member and active participant in the steering committee, the working group and the threat intelligence sharing group.

Website: https://www.tld-isac.eu

All CENTR members were asked to give their assessment of risks, risk management and possible consequences. Switch also participated. The results were consolidated and summarised in a report (Threat Landscape Analysis). Switch compared the resulting top ten risks against its own risk map. Two new and plausible risks were added to Switch's own risk management system.

EUROPEAN
TLD ISAC

The global landscape of abuse

Suspension of DAAR reports from ICANN

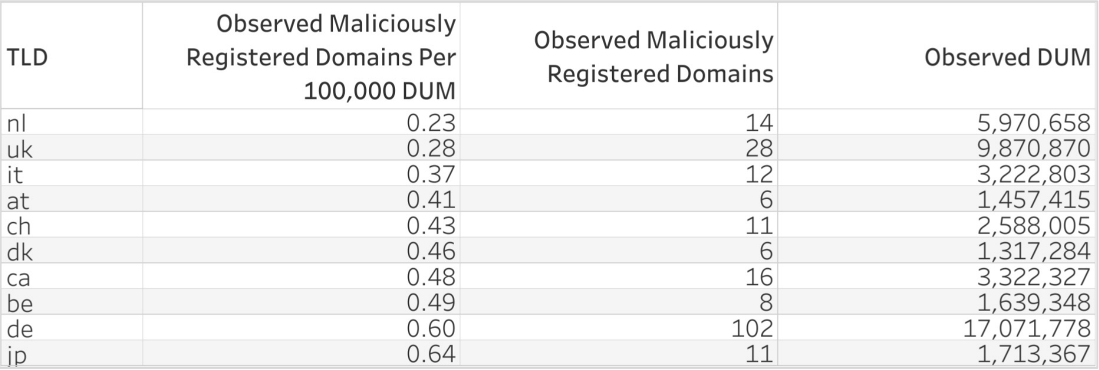
Switch voluntarily participated in ICANN’s DAAR project and received a tailored report on domain abuse for .ch and .li. ICANN suspended reporting in Q1 2024.

ICANN has launched a follow-up project called Domain Metrica, which will initially be for gTLDs only. ccTLDs are not currently being included, but we are following developments closely.

Public NetBeacon reports

Switch contributes to measurements by the NetBeacon Institute.

In October 2024, the .ch zone ranked fifth amongst the most secure ccTLDs with more than 1 million domain names.



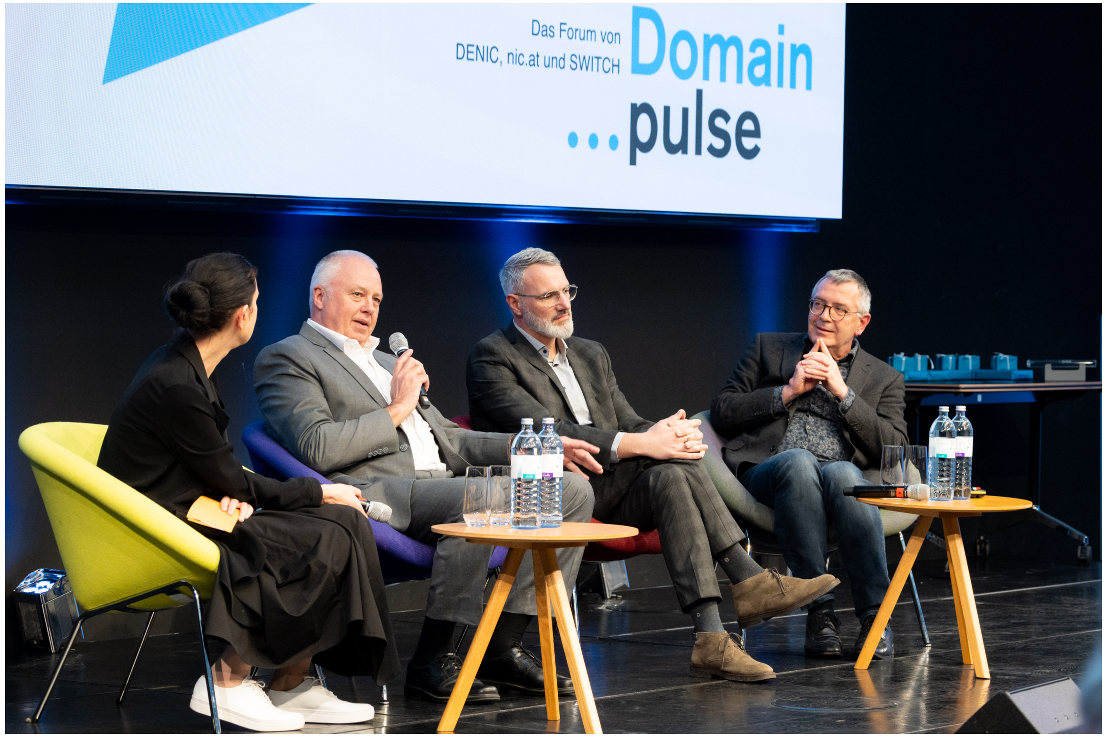
TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
nl	0.23	14	5,970,658
uk	0.28	28	9,870,870
it	0.37	12	3,222,803
at	0.41	6	1,457,415
ch	0.43	11	2,588,005
dk	0.46	6	1,317,284
ca	0.48	16	3,322,327
be	0.49	8	1,639,348
de	0.60	102	17,071,778
jp	0.64	11	1,713,367

Source: https://netbeacon.org/wp-content/uploads/2024/12/MAP-Report-December-2024-.pdf

Domain Pulse 2024

Domain Pulse was held in Vienna on 23 and 24 February 2024.

Under the motto ‘Vienna Calling: Domain Pulse 2024’, the event explored the opportunities, limitations and impact of technical advances, along with the associated regulations (NIS2) and challenges. Another focus was security and updates from the domain industry.



Panel with Richard Wein (Managing Director, nic.at), Andreas Musielak (Executive Board, DENIC) and Urs Eppenberger (Head of Registry, Switch).

DNS resilience programme

50.4%

As of 1 January 2025, 50.4% of all .ch domain names have been signed.

DNS resilience programme

Resilience for .ch domain names

Switch’s DNS resilience programme promotes the adoption and dissemination of open security standards for .ch and .li domain names. These standards play a key role in increasing resilience to cyber threats. The programme, which is based on financial incentives, runs from 2022 to 2026.

The main objective is to promote the signing of domain names with DNSSEC. For the entire duration of the programme, domain names that are not signed or are signed incorrectly are subject to a surcharge.

The DNSSEC Advisory Board decides which security standards to promote. The board is made up of representatives from OFCOM, the registrars and Switch.

For 2024, the programme has been extended to include the email security standards DMARC and SPF. This means: In 2024, the reimbursement of the additional revenue is based not only on DNSSEC, but also on the successful implementation of DMARC and SPF.

The Advisory Board has already agreed that (in addition to DNSSEC) DANE will be promoted in 2025, and IPv6 in 2026.

Quality control measurements

The correct implementation of the security standards is verified in cooperation with the external service provider OpenIntel. All .ch and .li domain names with name servers are checked daily to determine whether the criteria defined by the programme are met. The results of these checks are reported to Switch. Registrars with incorrect configurations receive error reports in order to fix the issues.

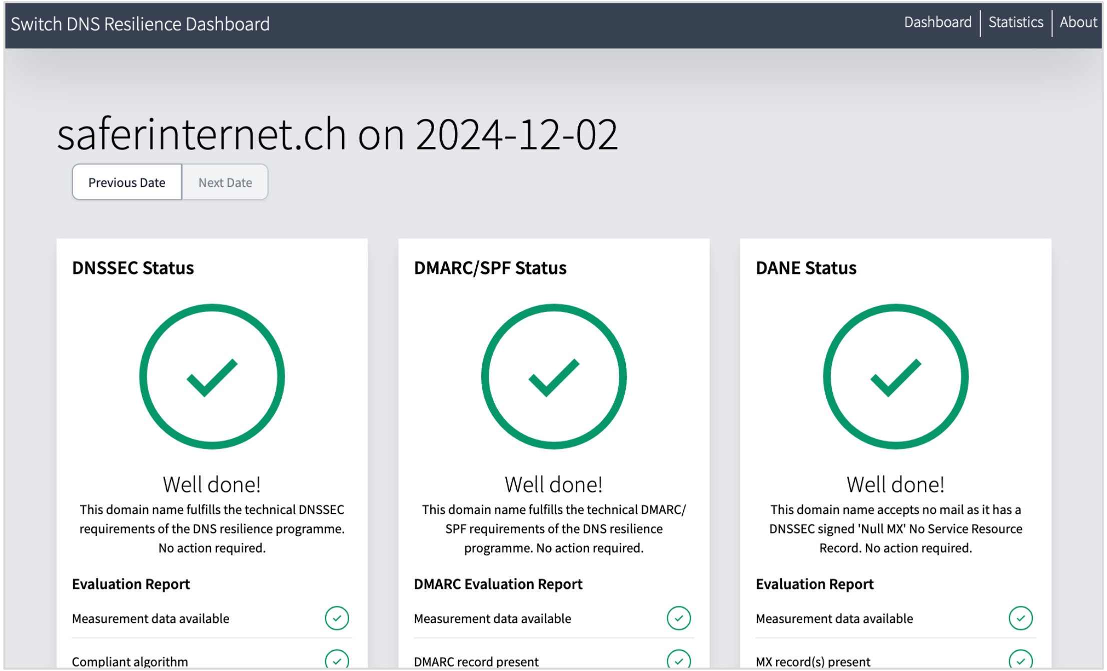
DNS resilience programme

In its third year of operation, we continued to focus on the development of the resilience programme in addition to operations.

Developments 2024

- Increased implementation of DMARC/SPF.
- Ongoing DMARC/SPF measurements, dispatch of the corresponding error reports.
- Reimbursements for 2023 to eligible registrars in the form of credit entries (end of February 2024).
- Implementation of DANE measurements; this criterion will be relevant in 2025.
- Since September 2024, error reports for DANE have been sent to the registrars. This allowed them to prepare for 2025.
- Extension of the dashboard provided by the external measurement service provider OpenIntel to include DANE (see screenshot with result for the domain name saferinternet.ch).
- Continuously providing information to the registrars, answering their questions, providing support.

Figures on the resilience programme can be found on page 40.



saferinternet.ch on 2024-12-02

DNSSEC Status

Well done!

This domain name fulfills the technical DNSSEC requirements of the DNS resilience programme. No action required.

Evaluation Report

Measurement data available ✓

Compliant algorithm ✓

DMARC/SPF Status

Well done!

This domain name fulfills the technical DMARC/SPF requirements of the DNS resilience programme. No action required.

DMARC Evaluation Report

Measurement data available ✓

DMARC record present ✓

DANE Status

Well done!

This domain name accepts no mail as it has a DNSSEC signed 'Null MX' No Service Resource Record. No action required.

Evaluation Report

Measurement data available ✓

MX record(s) present ✓

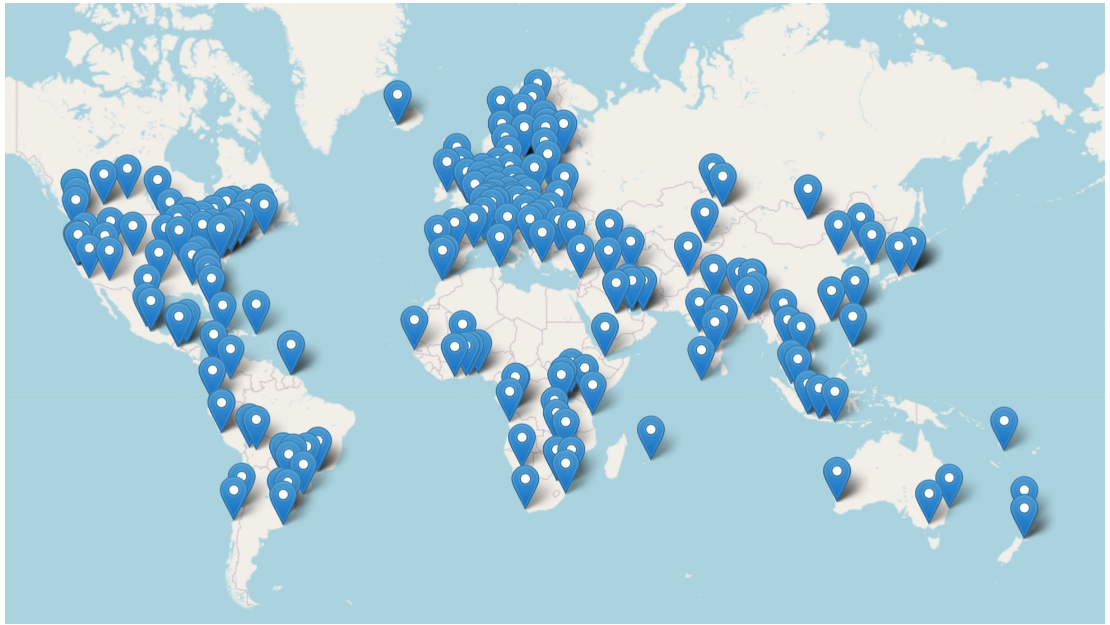
DNS – Anycast locations and zone generation

Anycast locations

Thanks to our Anycast hosting partners, the DNS zone is distributed across more than 100 locations worldwide, which are continuously updated in line with current circumstances. For example, a new hub was opened in Klagenfurt at the end of 2024.

Zone generation

Since the DNSSEC configuration was changed from NSEC3 to NSEC in 2023, no further changes have been made to the type of zone generation.



Switch_

ISO 27001 audit with neighbouring registries

The DACH audit takes place three times a year – one audit for each of the three participating registries (DENIC, nic.at and Switch) – under a rotating audit leadership. Each audit is followed by an exchange of best practices.

The first meeting was held at the end of April in Frankfurt at DENIC (denic.de). DENIC and its subsidiary Denic Services were audited over three days under the leadership of nic.at.

The audit group met again at Switch in early July. Switch was audited under the direction of DENIC's CISO and with the support of ISOs from Germany and the Austrian nic.at.

The audit results will be incorporated into the continuous improvement process and are reviewed by the auditors in one of the next DACH audits.

Under Switch's leadership, an internal audit according to ISO 27001:2022 took place at the Austrian registry nic.at from 24 to 26 September 2024. Representatives from the German registry DENIC were also present.

Although it was a 'friendly' internal audit, the same rigorous approach was applied as in a regular external audit. nic.at's high level of maturity over the past years was proven, and through continuous improvement they have shown that they can meet their high standards regarding compliance.

After the audit, the group discussed the requirements of the standard and the possibilities to implement them as efficiently as possible and in accordance with technical and organisational measures.

DACH stands for Germany (D), Austria (A), Switzerland (CH).

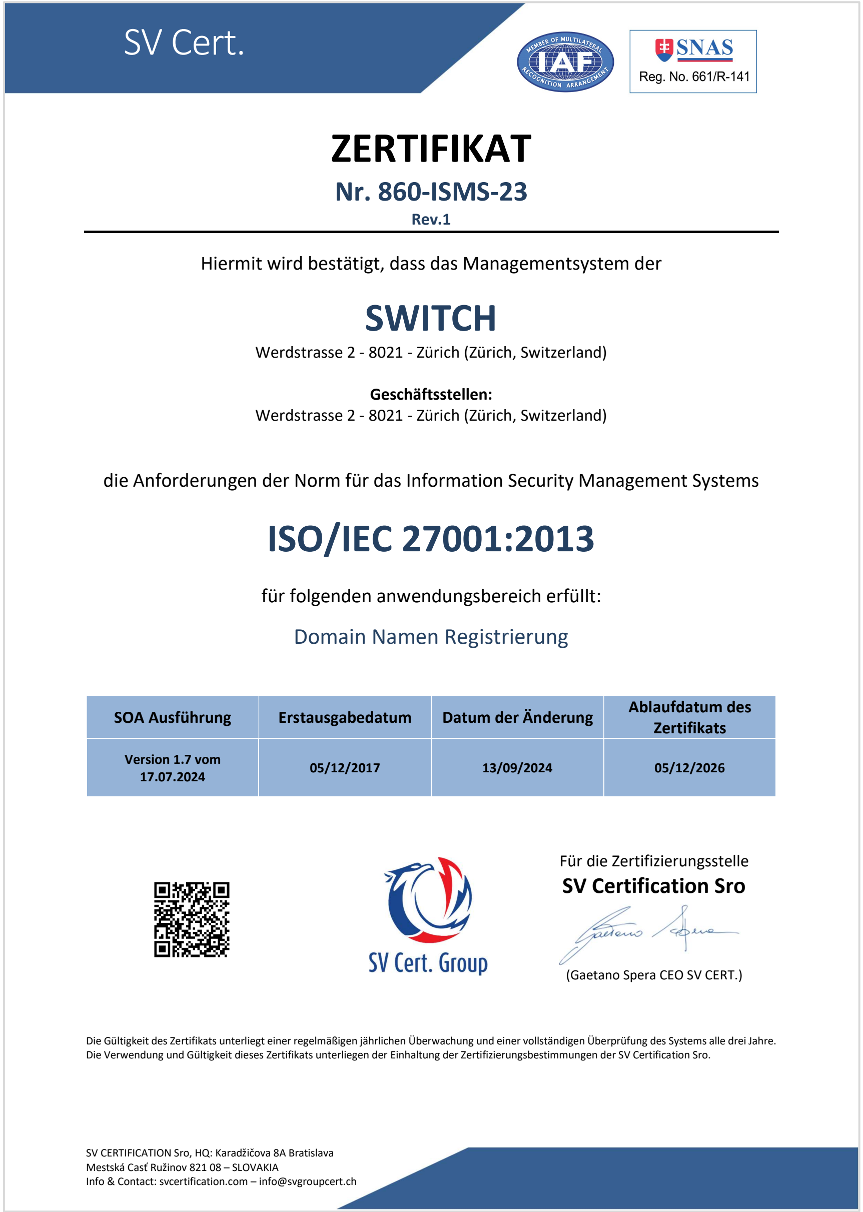
ISMS – ISO 27001 surveillance audit

The formal ISO 27001 Surveillance Audit took place on 5 September at the CSCS (Swiss National Supercomputing Centre) in Lugano.

Various controls from the new ISO 27001:2022 standard have already been tested, including threat intelligence. Switch impressed the auditor with its many years of experience in operating a CERT. Other areas covered were security architecture governance and procurement.

The certificate was issued in accordance with the 2013 standard.

Auditor's conclusion: "Information security is an important asset for Switch. What is striking is the high level of specialist knowledge and awareness of information security amongst all employees interviewed."



SV Cert.

SNAS
Reg. No. 661/R-141

ZERTIFIKAT

Nr. 860-ISMS-23

Rev.1

Hiermit wird bestätigt, dass das Managementsystem der

SWITCH

Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

Geschäftsstellen:
Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

die Anforderungen der Norm für das Information Security Management Systems

ISO/IEC 27001:2013

für folgenden anwendungsbereich erfüllt:

Domain Namen Registrierung

SOA Ausführung	Erstausgabedatum	Datum der Änderung	Ablaufdatum des Zertifikats
Version 1.7 vom 17.07.2024	05/12/2017	13/09/2024	05/12/2026

SV Cert. Group

Für die Zertifizierungsstelle
SV Certification Sro
(Gaetano Spera CEO SV CERT.)

Die Gültigkeit des Zertifikats unterliegt einer regelmäßigen jährlichen Überwachung und einer vollständigen Überprüfung des Systems alle drei Jahre.
Die Verwendung und Gültigkeit dieses Zertifikats unterliegen der Einhaltung der Zertifizierungsbestimmungen der SV Certification Sro.

SV CERTIFICATION Sro, HQ: Karadžičova 8A Bratislava
Mestská Casť Ružinov 821 08 – SLOVAKIA
Info & Contact: svcertification.com – info@svgroupcert.ch

“Information security is an important asset for Switch. What is striking is the high level of specialist knowledge and awareness of information security amongst all employees interviewed.”

ISO 27001 audit report

2.
Activity report – innovations

Domain Abuse 4.0

Modern and future-oriented anti-abuse measures

As mentioned in the 2023 Annual Report, the current software solution for combating cybercrime is no longer adequate for the ever-increasing challenges in combating domain name abuse.

A new forward-looking software solution based on state-of-the-art technology is therefore being developed as part of the Domain Abuse 4.0 project. The project team is developing a fast, low-maintenance and highly scalable solution. The processes are also being revised, adapted to the new circumstances and our experts are being trained in them. With these measures, Switch continues to be a global leader in the fight against cybercrime.

A major milestone

In 2024, CERT and the registry worked together to implement the key components of the new software solution, including implementing and testing initial workflows (processes against abuse).

The first production version of the new software solution was launched at the end of the year. Since January 2025, we have been using the new software to send identification requests to the holder of a domain name in accordance with Art. 29 and 30 of the OID if we have reasonable grounds to suspect that the holder’s details are incorrect.

Domain Abuse 4.0

Outlook for 2025

Thanks to our success in 2024, we are well positioned to implement the remaining workflows by the end of 2025 and put our old software solution into well-deserved retirement.

The most important workflows and software components planned for implementation in each quarter of 2025 are listed on the right-hand side. These will then be gradually incorporated into operations.

Outlook for 2026

Any additional workflows and features will be implemented on an ongoing basis. One feature could be a technical interface for the authorities, which will allow them to connect our software solution to their systems and send us requests automatically.

Workflows and components to be implemented in 2025

Q1 2025

- Registrations purely for abuse
- Feed reader (receiving reports of abuse)

Q2 2025

- Compromised websites (phishing and malware)
- Connection to saferinternet.ch

Q3 2025

- Blocking requests from authorities in accordance with Art. 15 OID
- Automatic reporting

Q4 2025

- Correspondence address requests from authorities in accordance with Art. 16 OID

Q1 2026 Ongoing development

Reliability engineering

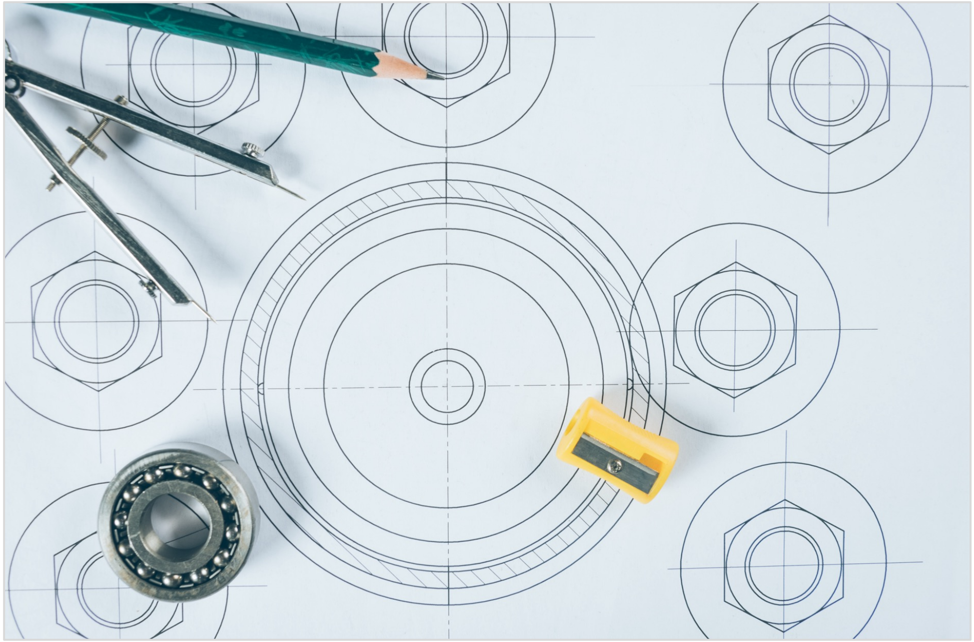
As IT systems become increasingly more complex and integrated into our lives, operations also need to change.

To improve information security, Switch is introducing the concept of ‘reliability engineering’, along with a dedicated ITSM and Reliability Coach role, to help teams deliver stable and reliable services.

We are focusing on automated and scalable methods for managing availability, capacity performance as well as incident and change management.

New processes and policies for incident management, change management and monitoring have been developed, and 15 specialist training sessions were held, including for members of the Infrastructure and Senior Management teams.

“Hope is not a strategy. Luck is not a factor. Fear is not an option.” James Cameron



Integrating ISMS and DPMS

There is considerable overlap between ISMS (ISO 27001) and DPMS (ISO 27701).

While both use the same ISO management system, DPMS is merely a supplement to ISMS. The two boards at Switch responsible for this have therefore decided to merge the two concepts.

The new system is now known as ‘Integrated Management System’, or IMS for short. Switch is not currently seeking certification in accordance with ISO 27701.

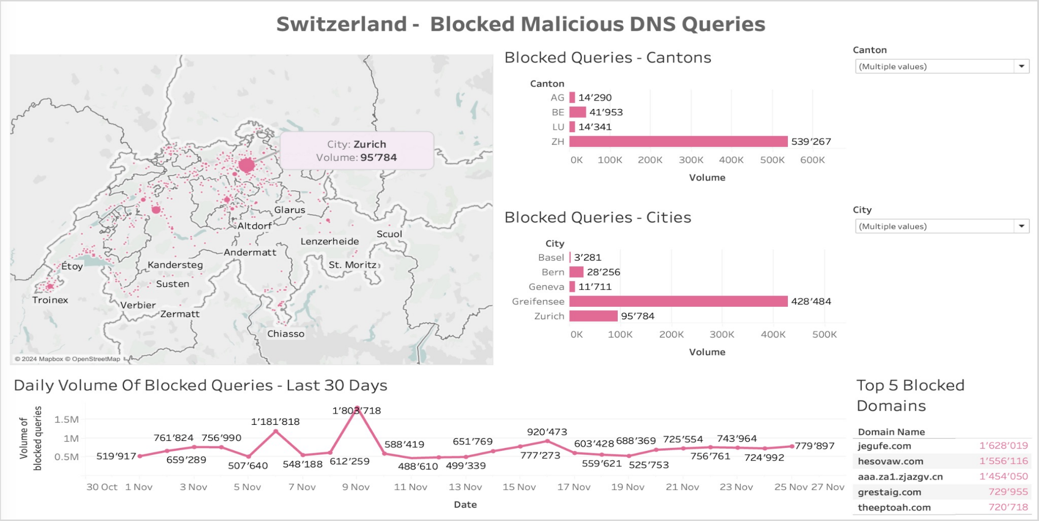
However, merging them helps to avoid duplication in the documentation. It also simplifies employee training since all the necessary information is now available in one place.

ISMS:	Information Security Management System
DPMS:	Data Protection Management System

Quad9: The role of threat intelligence

Quad9 and Switch are working together to analyse threats to the Swiss Internet. This includes:

- Developing and implementing a threat intelligence strategy for Quad9 and for combating domain abuse at Switch.
- Analysing the top threats blocked by Quad9 around the world each month and producing regular reports that are shared with interested parties within the security community and with local government cybersecurity organisations. Example reports: Security awareness blogpost for Christmas shopping season, Trends H1 2024: cyber insights and a blog article for AFRINIC
- Acquiring new threat intelligence partnerships for Quad9. In 2024, Quad9 signed 12 new partnerships, including a new partner in Switzerland, ThreatCat.
  A list of partners is available here.
- Creating a ‘Quad9 Threat Intelligence Product for Switch CERT’. The aim of this project is to develop a solution for Switch CERT for collecting, aggregating and analysing threat data from Quad9 DNS.
- Creation of a proof-of-concept dashboard for the Swiss government. The dashboard shows the most important threats that have been blocked by Quad9 at national level:



Switzerland - Blocked Malicious DNS Queries

Canton: (Multiple values)

City: (Multiple values)

Top 5 Blocked Domains

Domain Name	
jegufe.com	1’628’019
hesovaw.com	1’556’116
aaa.za1.zjazgv.cn	1’454’050
grestaig.com	729’955
theeptoah.com	720’718

- According to the Federal Department of Foreign Affairs (FDFA), Quad9 has become the protective DNS resolver for NGOs and IGOs based in Switzerland.

Top threats to the Swiss web

According to data collected by Quad9, the following campaigns were active in 2024 and posed a threat to Swiss Internet users:

SocGolish campaigns

A widespread, years-long malware campaign aimed at distributing fake browser updates to unsuspecting Internet users. Once installed, the fake browser updates infect the victim's computer with various types of malware, including Remote Access Trojans (RATs).

For this campaign, blacksaltys.com was used. Quad9 blocked more than 123,000 requests in Switzerland and more than 7 million worldwide.

SBB phishing

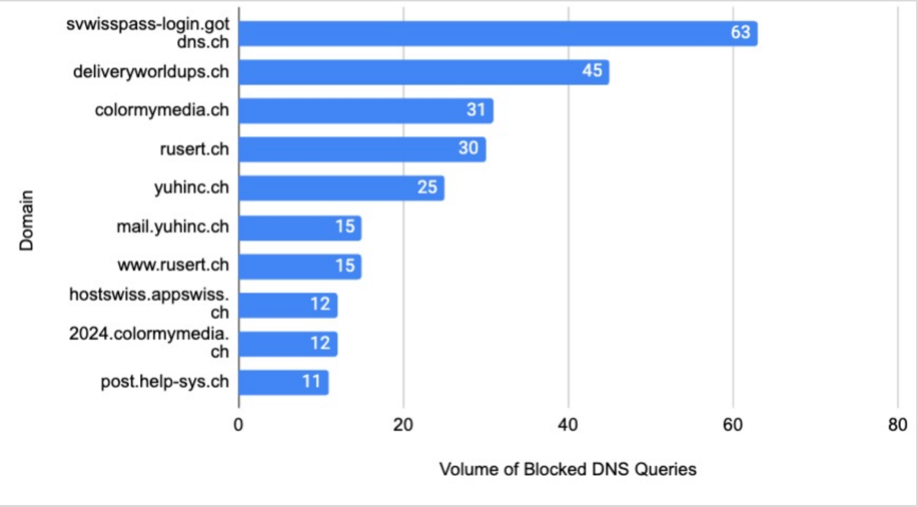
A phishing campaign that tricked victims into entering their SwissPass information.

The domain name divinedownload.com was used. Quad9 blocked more than 2,280 DNS requests from Swiss users.

Swiss Post phishing

A phishing campaign against Swiss Post in which victims were asked to provide their login details. The domain name espace-login.net was used for this campaign. Quad9 blocked more than 2,340 DNS requests from Swiss users.

The most frequently blocked compromised .ch domain names reported to Quad9 by Switch CERT were related to the campaign against SwissPass users, campaigns against delivery services (UPS, Deutsche Post) and webmail services.



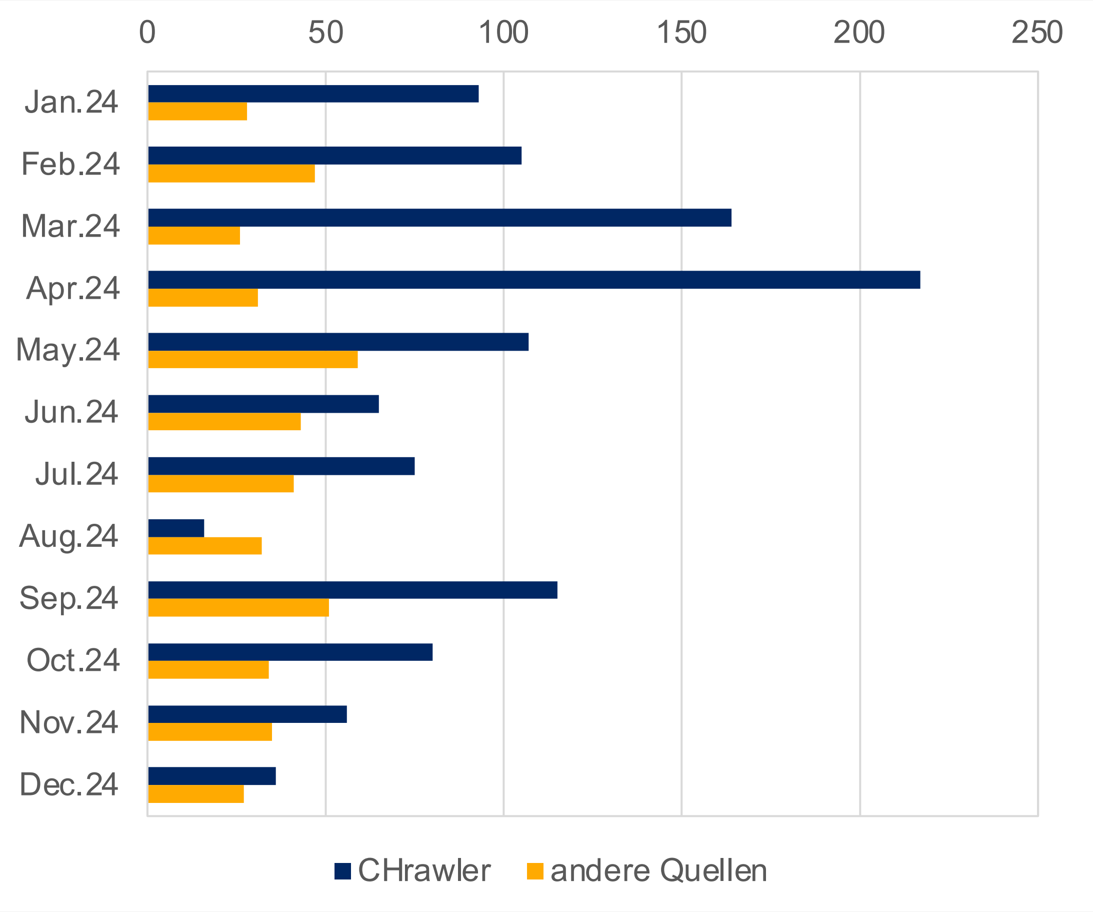
Web crawler

We use our Web crawler (CHrawler), which went live in early 2024, to regularly and systematically examine publicly available resources in the .ch and .li zones to detect compromised or malicious domain names at an early stage and thus reduce the risk for Internet users. If our crawler detects domain names that are phishing or spreading malware, we can block the domain name after notifying the holder and waiting for a period of time.

After almost a year of operation, we have been able to find a significant number of compromised domain names on a regular basis, especially in comparison to the figures otherwise reported to us (see the statistics on the right). In total, we discovered around 1,200 compromised domain names in 2024.

This way, Switch can make an important contribution to further increasing the security of the .ch and .li zones not only reactively, but also proactively through independent searches. We are also collecting important insights into what campaigns and threats are currently active on the Swiss web. See also ‘Top threats to the Swiss web’ on page 32.

Processed .ch malware domains in 2024



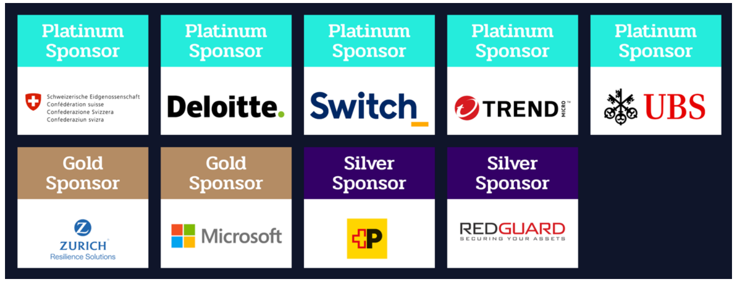
Women in Cyber Switzerland

Despite the growth in the field of cyber security in recent years, a closer look shows that women are still underrepresented in the global workforce. This is in the midst of a growing shortage of skilled workers in the cyber sector. To help companies close this gap, it is important to get more women excited about the cyber sector and ensure they have the same opportunities as their male counterparts.

Women in Cyber Switzerland is committed to increasing diversity by organising the annual Women in Cyber Day, local networking events and a mentoring programme.

Switch has been supporting the initiative since 2019 and is an active board member. In March, the first local networking event took place at Switch in Zurich.

https://women-in-cyber.ch



Platinum Sponsor	Platinum Sponsor	Platinum Sponsor	Platinum Sponsor	Platinum Sponsor
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Deloitte.	Switch	TREND MICRO	UBS
Gold Sponsor	Gold Sponsor	Silver Sponsor	Silver Sponsor	
ZURICH Resilience Solutions	Microsoft	P	REDGUARD SECURING YOUR ASSETS	

NextGen Hero

NextGen Hero award recognises young talent

At the Digital Economy Awards ceremony, held on 14 November 2024 at Zurich's Hallenstadion, companies, organisations and individuals received awards in various categories for their unique contributions to Switzerland's digital transformation.

In the 'NextGen Hero' category (in partnership with Switch), the attendees nominated two young talents for their outstanding creativity and innovative strength: Selina Pfyffer and David Cleres.

Who are these future stars and what are their goals? In this interview, they talk about their visions for the future and how they are helping to shape digital progress in Switzerland.

The fifth annual Digital Economy Awards brought together hundreds of experts from the Swiss ICT scene to celebrate the most outstanding talents and their innovations. Awards were presented to the top achievers in six categories.

Presenting the 'NextGen Hero' category at the 2024 Digital Economy Awards. From left to right: Tom Kleiber, Switch; Claudia Lienert, Switch; David Cleres, GirlsCodeToo; Selina Pfyffer, SeasonCell; Monika Schär, presenter.
Photo: Switch

3.

Activity report – statistical indicators

Switch

Domain name inventory – 2024 developments

Development of .ch

The inventory of .ch domain names increased by around 6,000 in the last year.

	2023	2024
New registrations	294,195	279,916
Deletions	282,649	303,361
Reactivations*	29,958	29,948
Domain inventory as at 31/12	**2,562,914**	**2,568,952**

* Deleted domain names that were reactivated by the registrar within the 40-day transition period.

Development of .li

The number of .li domain names decreased by around 1,000 in the last year.

	2023	2024
New registrations	10,658	9,495
Deletions	12,218	11,608
Reactivations*	1,699	1,285
Domain inventory as at 31/12	**70,607**	**69,774**

Information service – statistics 2024

Information service figures

Switch grants anyone who can credibly demonstrate an overriding legitimate interest free access to the domain name holder’s personal data contained in the RDDS database (Whois). These statistics record all requests that were made in the reporting year using the information service’s forms. The number of requests from private persons remained at the same level compared to the previous year.

	Private	Authorities
Information provided	309	73
Information not provided	54	5
General requests *	6	0
Total requests	**369**	**78**

* These are requests about processes, procedures and legal bases.

Simplified access via RDAP for .ch and .li

If an authority or organisation has the appropriate permissions, it can query domain names including personal data via RDAP (Registration Data Access Protocol). The number of authorities continued to increase in 2024, which is also thanks to our improved networking with Law Enforcement authorities. At the end of 2022, only 5 authorities were using RDAP, compared to 17 at the end of 2024. The cantonal police forces make up the largest proportion.

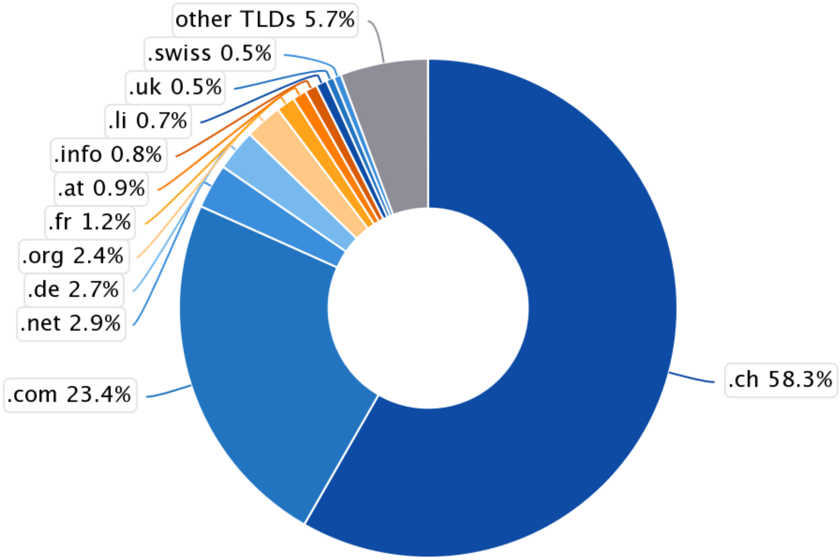
	Requests
Information provided	4,203
Information not provided	368
Total requests	**4,571**

Market share of .ch and .li with Swiss domain name holders

The market share of the TLD (top-level domain) **.ch** among holders in Switzerland remained nearly unchanged from October 2023 to October 2024.

October 2023

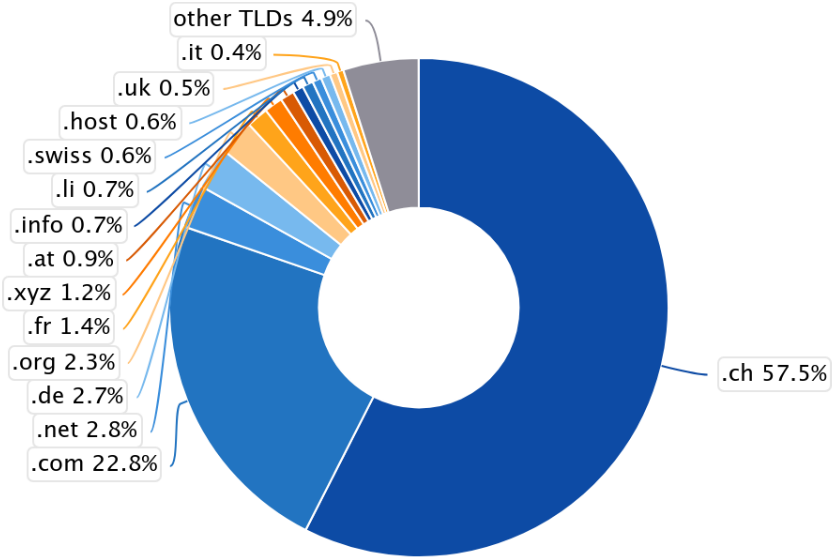
Market share of different TLDs among domain name holders in Switzerland. Source: CENTR



There was little change in the market share for the generic TLDs **.com/.net/.org**, or for **.li** domain names.

October 2024

Market share of different TLDs among domain name holders in Switzerland. Source: CENTR



DNS resilience programme – development in figures

DNSSEC

- Percentage of .ch domain names with DNSSEC, as of 1 January 2025: 50.4% (1 January 2024: 49.1%).
- Error rate: The error rate remained at a very low level over the year. Average error rate of all DNSSEC domain names: 0.17%, same as 2023.

DMARC and SPF

- 1 January 2025: 20.1% correctly configured (1 January 2024: 4.5%). Figures for .ch and .li domain names, correct configuration of both DMARC and SPF.
  Data according to statistics from the external monitoring service provider.

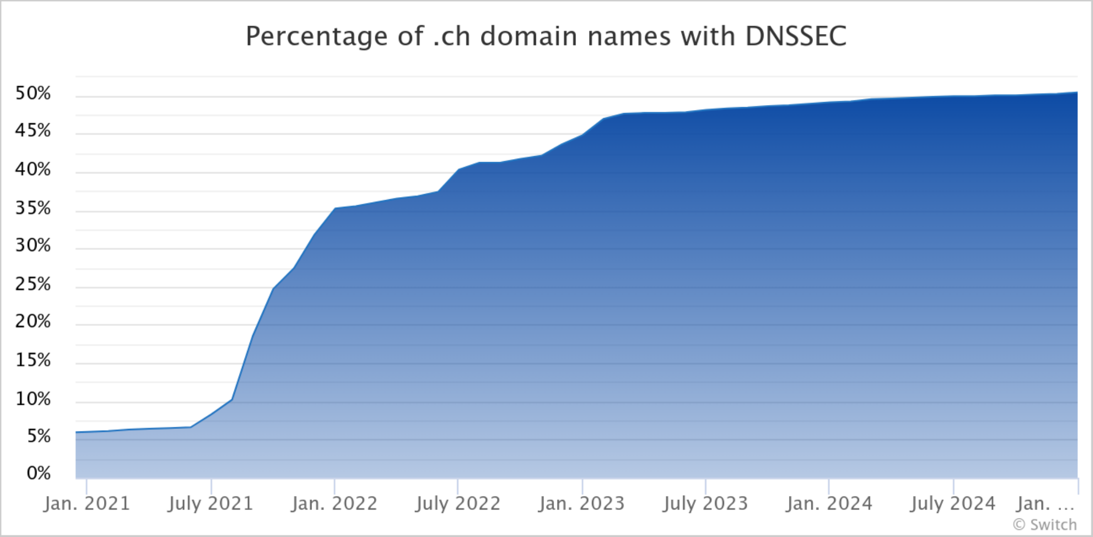
DNSSEC statistics at Switch

Statistics at OpenIntel

Refund calculation for 2024

- Additional revenue collected from price differentiation: CHF 1,569,687
- Minus fixed compensation for Switch and the external monitoring service provider for 2024: CHF – 444,907
- Total refund CHF 1,124,780

The refund will be made at the end of February 2025.



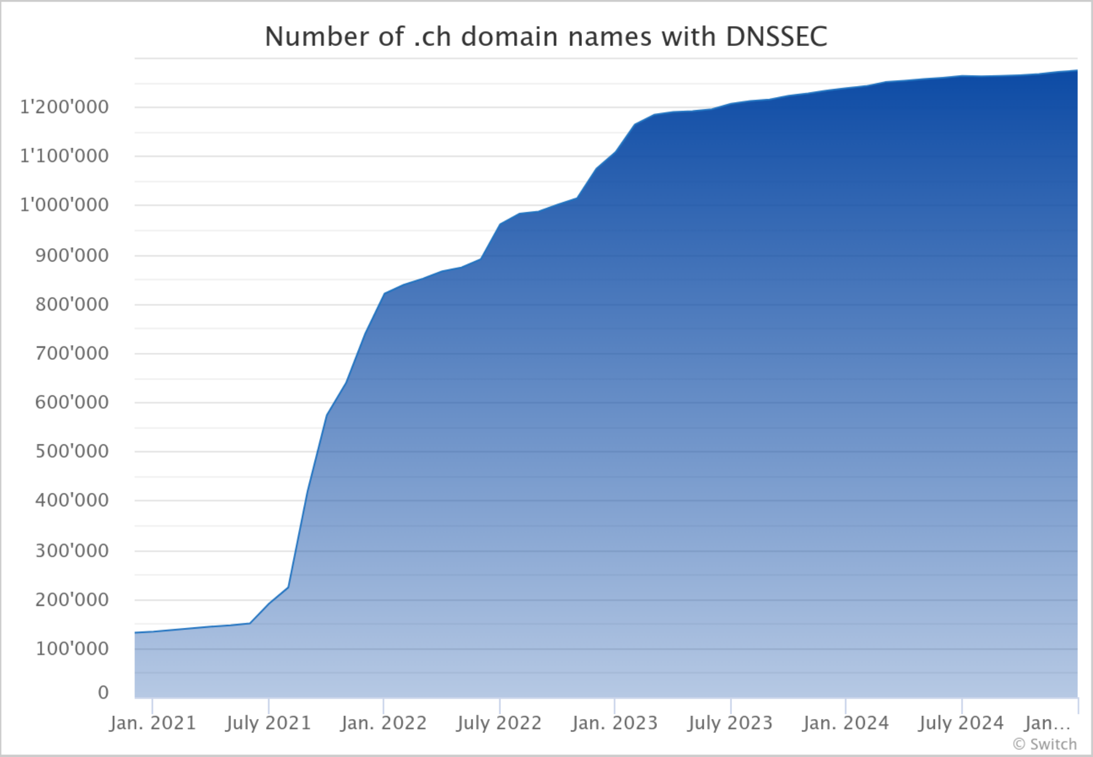
Switch

DNSSEC developments
Number of signed domain names

As of the end of 2024, more than 1.27 million .ch domain names have been signed with DNSSEC.

This corresponds to 50.4% of all .ch domain names with name servers, compared with 45% at the end of 2022 and 35% at the end of 2021. The strong growth in 2021 and 2022 was mainly driven by registrars signing all their clients' domain names as part of the DNS resilience programme. However, this growth slowed in the following years.

The larger Swiss registrars have now signed as many of their domain names as possible. If the domain names have 'external' name servers, the registrars have no influence on the signature. For large registrars abroad, the .ch TLD is only a very small part of their business, and the effort of signing is not worth it for them. As a result, minimal growth is expected in the future.

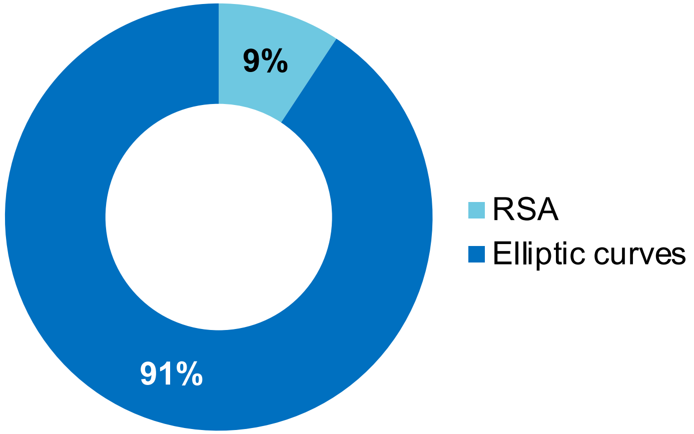


1,273,817 .ch domain names signed with DNSSEC as of 1 January 2025

DNSSEC developments Distribution of DS algorithms

More than 90% of all .ch domain names use the currently recommended algorithm 13 (ECDSAP256SHA256).

However, there has been a slight increase in signing with Edwards curves (EdDSA algorithms 15 and 16). These are not supported or are only partially supported by older operating systems and are therefore recommended only to a limited extent.



DNSSEC signatures used

DNSSEC algorithm	Number	Percentage
8 – RSASHA256	11,806	9.27%
10 – RSASHA512	86	0.01%
13 – ECDSAP256SHA256	1,153,418	90.55%
14 – ECDSAP384SHA384	150	0.01%
15 – Ed25519	1,929	0.15%
16 – Ed448	123	0.01%

DNSSEC validation in Switzerland

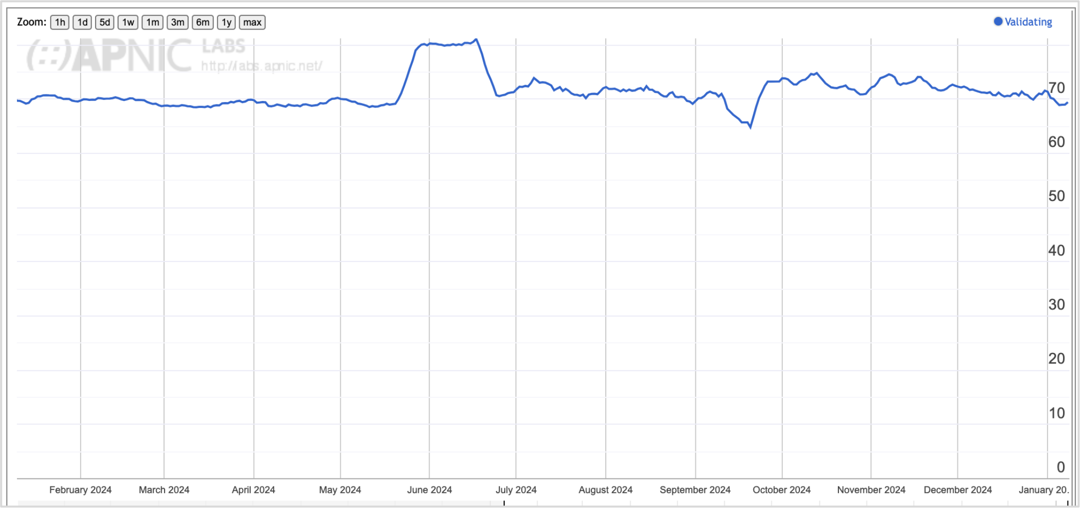
DNSSEC validation

To protect users from DNS spoofing, not only must the domain names be signed, but these signatures must also be validated by the DNS resolver.

According to APNIC measurements, the validation rate of DNSSEC on resolvers of Swiss ISPs remained constant at around 70% in the past year.

Website: https://stats.labs.apnic.net/dnssec/CH

DNSSEC validation on Swiss resolvers

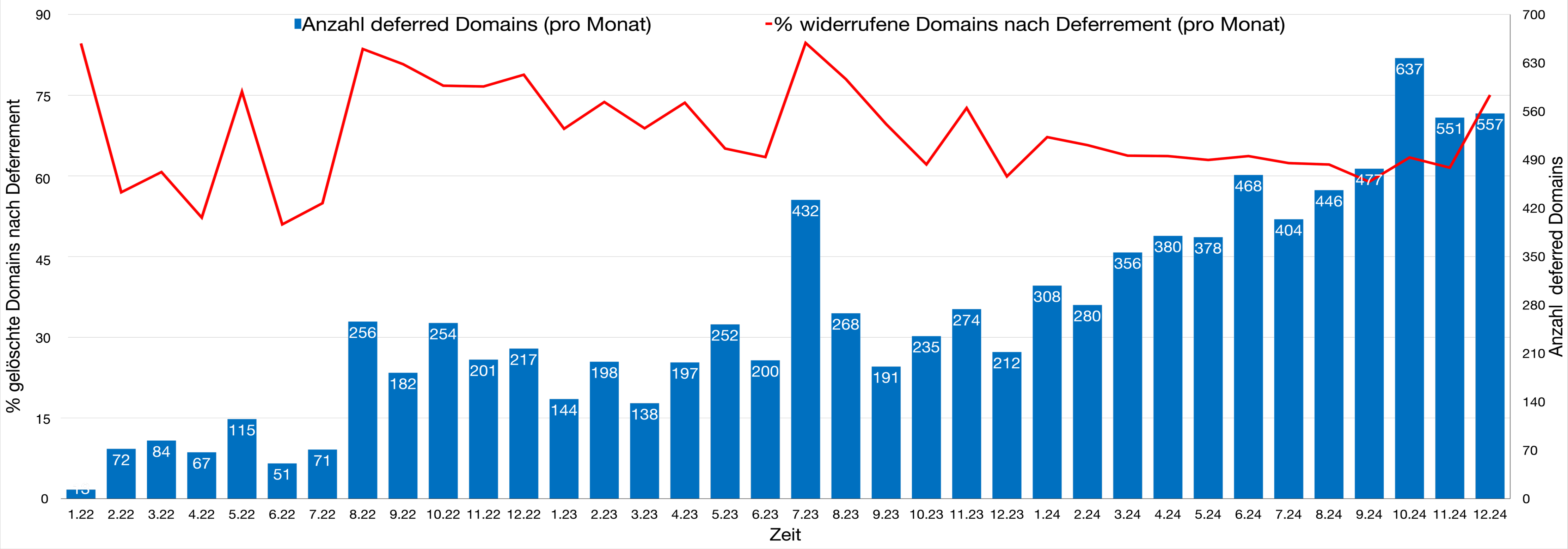


Deferred Delegation

A look back at Deferred Delegation

Last year, we significantly increased the number of deferred registrations again, by a factor of around two, by further strengthening the rules.

As would be expected from such an increase, the proportion of domain names that were released again after positive identification of the holder also increased slightly. However, this occurred to a much lesser extent due to a careful and iterative expansion of the criteria.



Switch

Dispute resolution

OFCOM has tasked Switch with providing an affordable dispute resolution service (DRS). Since 2004, Switch has been using the WIPO (World Intellectual Property Organization) dispute resolution service. WIPO operates an ICANN-accredited dispute resolution service for over 70 other registries.

In 2024, the experts made decisions on 13 .ch domain names. The expert decision is the final step in the process. A somewhat smaller number of cases are closed, for example, during arbitration or because proceedings are abandoned.

WIPO decision	2023	2024
Transfer to applicant	11	10
Complaint rejected	5	3
Number of decisions	**16**	**13**

WIPO decisions (as of 17 February 2025)

	Domain names
Transfer to applicant	girlscancode.ch axashop.ch salonmoulinrouge.ch veka-fenster.ch vekafenster.ch floqast.ch elfbar.ch aqara.ch giezemon.ch universalgeneve.ch
Complaint rejected	carify.ch johntaylor.ch meinl.ch

Registrar developments

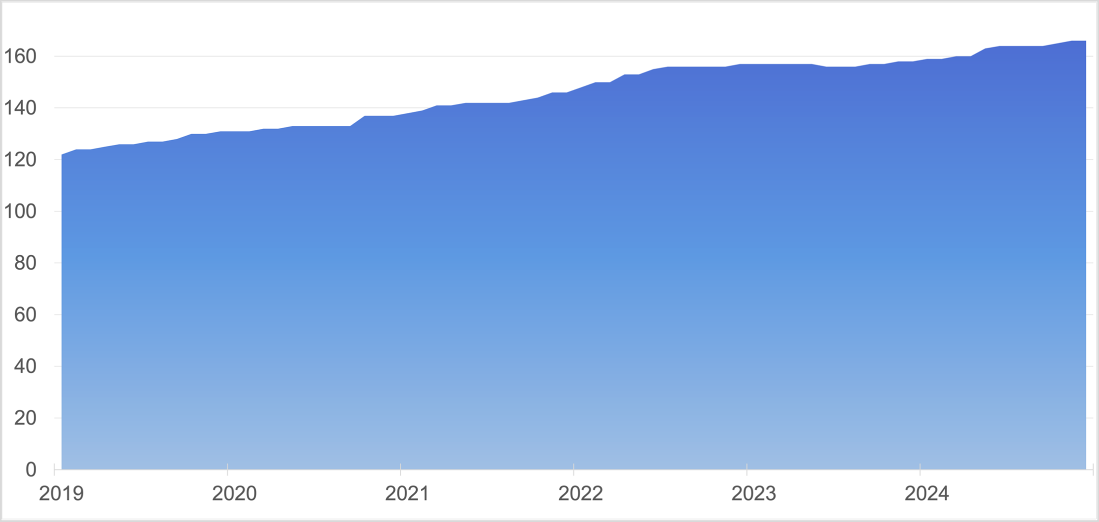
In 2019, the number of registrars rose to 131, and the registry had 137 registrars at the end of 2020. In 2021, the number of registrars increased by nine to a total of 146.

In 2022, 11 registrars first signed a test contract for access to the test system. We switched these registrars to the productive system once they had successfully completed the test phase and passed the test course. The total number of recognised registrars therefore increased to 157.

In 2023 we were only able to give one more registrar access to the productive system, increasing the number to 158.

Seven registrars were added in 2024, bringing the total to 165 by the end of the year.

The 8 new registrars added in 2023 and 2024 have a combined portfolio of 8,500 domain names, with one of them managing about 7,500 domain names.



Performance of name servers

In terms of DNS performance measurement, Switch relies on the response time requirements for DNS queries stipulated by the ICANN Agreement: queries in the CH zone must be answered by at least one logical name server within 500 ms (UDP) or 1,500 ms (TCP).

In 2024, this requirement was met in each instance.

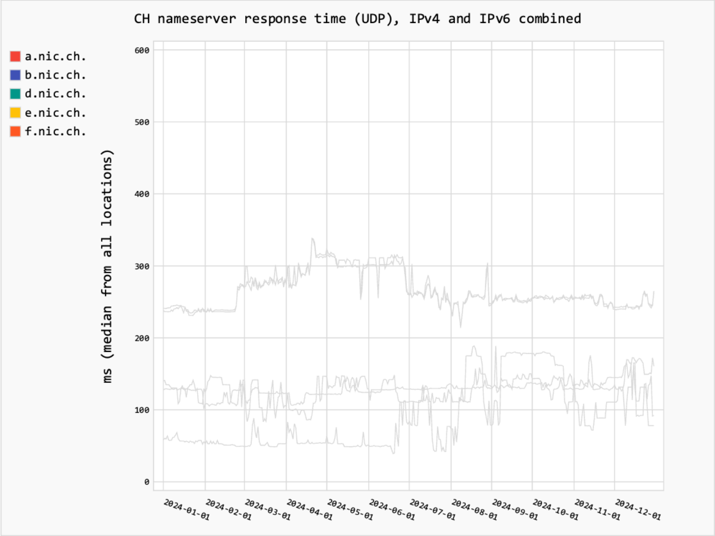
The measurements are carried out by RIPE and are publicly available. https://atlas.ripe.net/dnsmon/group/ch

Unicast: a.nic.ch (CH), b.nic.ch (CH)

Anycast: d.nic.ch, e.nic.ch, f.nic.ch

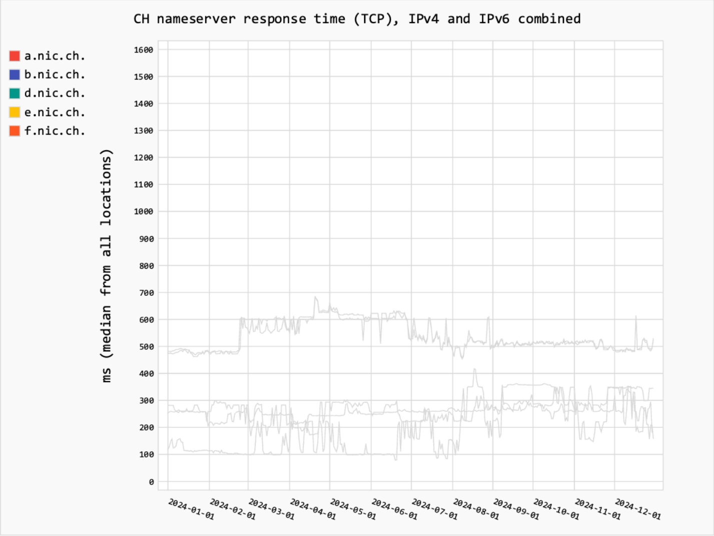
UDP response times

Combined response times of IPv4 and IPv6



TCP response times

Combined response times of IPv4 and IPv6



Cybercrime in 2024

Quantitative

In the reporting year, we captured and processed the following cases:

Number of malware and phishing cases 2024 quantitative view

	# malware cases	# phishing cases
Reports received	**1,730**	**451**
Suspicion confirmed	**1,392**	**239**
Number of blocked domain names	**656**	**115**
Reason for lifting block: - Statutory period expired - Eliminated after block - In progress on the cut-off date	 **83** **402** **3**	 **2** **15** **3**
Revoked domain names	**170**	**95**

Qualitative

The time spent on cases was:

Number of malware and phishing cases 2024 qualitative view

	Duration	
Duration of blocking according to OID Art. 15 (1), (2), (3) Max. blocking time 30 days (720 hours)	Min. time Average Max. time	**0.22 h** **103.74 h** **166.92 h**
Response time from Switch following notification	Average	**5.13 h**
Time until removal of threat after notifying the holders	Average	**86.8 h**

DNS Health Report

The DNS Health Report checks the accessibility of name servers and .ch and .li domain names. In the event of technical problems, Switch informs the operator and makes recommendations for resolving them. As such, the DNS Health Report improves the reliability of the Internet in Switzerland. What is being checked:

- Name servers: The function of the name servers is being checked for compliance with the DNS standards.
- Domain names: It checks whether DNSSEC-signed domain names can be resolved using a validating recursive resolver.

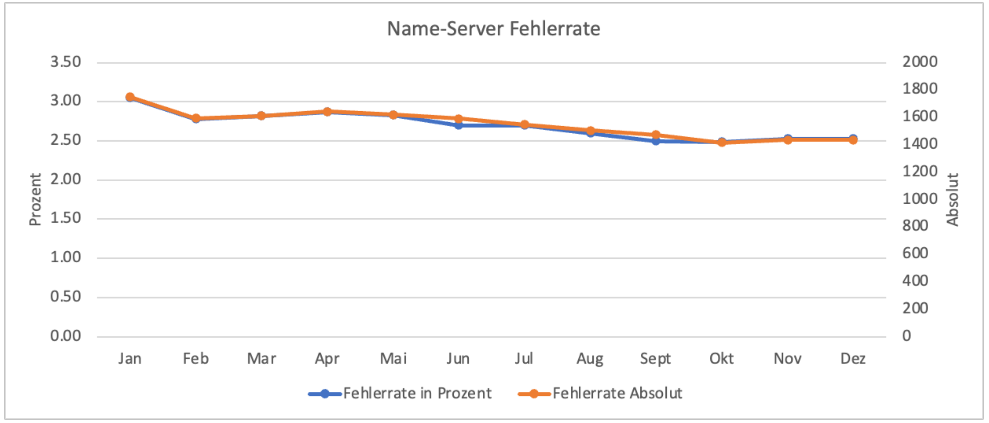
Name server report

The error rate for the name server accessibility measurement has decreased only slightly but steadily since the beginning of the measurement. This is most likely due to software updates.

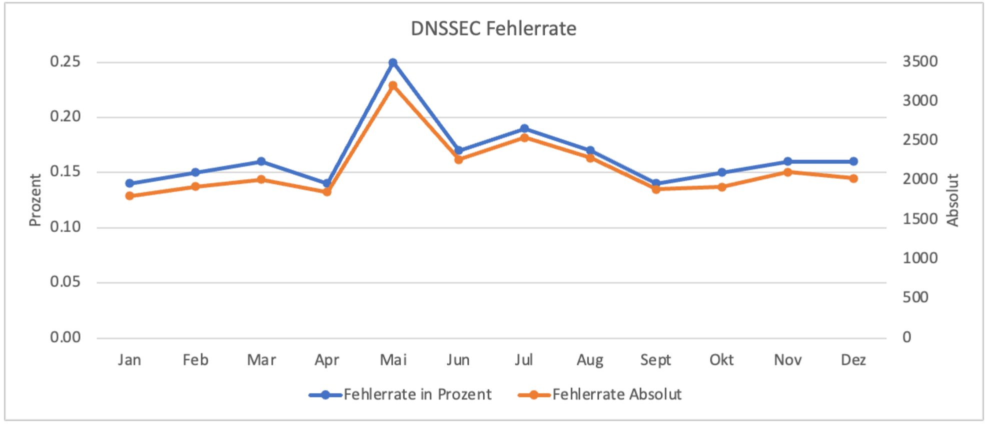
Domain name report

The error rate for the domain name accessibility measurement has plateaued. Most faulty domain names are parked domain names, where there is little motivation to correct the errors.

Error rate for name server accessibility measurement



Error rate for domain name accessibility measurement



Switch

4.

Activity report – economic indicators

Economic indicators

The Switch foundation’s 2024 annual report will be approved along with the balance sheet and income statement at the Foundation Council session on 12 June 2025. Publication will take place from 13 June 2025.

No figures will be published at this point. Instead, interested parties will be referred to the comprehensive documents of Switch's 2024 annual report.

5.

Activity report – developments

Switch

Looking back at 2024

DNS resilience programme

The price differentiation for correctly DNSSEC signed domain names has been maintained in 2024. The programme's financial incentives promote cryptographic protection of the Domain Name System and the adoption of other secure protocols. In 2024, these were the email security standards DMARC and SPF. Measurements and feedback to registrars went smoothly.
Read more on page 21.

Web crawler for the registry

The new Web crawler was launched in early 2024. This new registry service became necessary because reports were no longer coming in from the NCSC since their crawler had been discontinued. The statistics on page 33 show the impressive track record of the Web crawler and the corresponding domain abuse processes.

Domain Abuse 4.0

The project is scheduled to run for two years and should be completed by the end of 2025. We are very satisfied with the progress made in 2024 and we remain on track for the completion date.

The framework conditions of the agreement with OFCOM clearly states that data related to the fight against cybercrime must be processed on Switch systems. In-depth discussions with potential software providers for some elements of the application made it clear that only in-house development could meet this requirement. The internal development team is supported by two external specialists for the duration of the implementation.

Further details on the progress of the project can be found on page 27.

ISMS ISO 27001:2022

The migration of the internal ISMS to the new ISO standard was planned for 2024 but had to be rescheduled.

Planned innovations for 2025

DNS resilience programme: IPv6 measurements

In 2026, the criterion for the refund will be IPv6 on name servers. This should further increase resilience. Switch is preparing the measurement infrastructure accordingly. The dashboard will also be extended to allow registrars and hosts to check whether they have implemented the configuration correctly according to Switch’s recommendations.

Domain Abuse 4.0

Much of the registry’s development capacity is focused on completing the new infrastructure to fight cybercrime. This also includes training for professionals, who will eventually be provided with new tools. The rough project plan can be found on page 28.

Database upgrade

In Q2 2025, the PostgreSQL database will be migrated from version 13 to version 16. This modernises the core of the registration application. Meticulous preparation is an important prerequisite, and we also rely on external database experts.

ISMS ISO 27001:2022

The two-day audit in accordance with the 2022 standard will take place on 10 and 11 September 2025. In the meantime, all documents and processes for the registry’s Information Security Management System (ISMS) will be adapted.

Planned innovations for 2025

Deferred Delegation and machine learning

Whether or not a domain name enters the deferred delegation process after re-registration is determined using rules that look for certain patterns and then weight the results. This can be traced transparently in every case.

Switch is currently developing a new algorithm that uses machine learning. While patterns are still crucial, the weighting will become more dynamic. The system is trained using domain names that have been confirmed as abused or that have been registered without abuse for a longer period of time. Registries of Belgium and the Netherlands are already using such tools and sharing their experience.

We are not expecting to switch to the new system until after 2025. The first step is to build up knowledge and verify the concept.

Domain scanner for CDS

In 2025, there are plans to update the infrastructure for the automated management of DNSSEC DS records. The scanner, which scans the entire zone daily for CDS records (RFC8078) is made more efficient thanks to an improved search algorithm. CDS records are found and processed more quickly. Preparations are also being made to enable searches for individual domain names to be initiated at any time in the future, rather than having to wait for the next daily search.

In addition to DNSSEC data, the updated scanning infrastructure will form the basis for processing CSYNC records (RFC7344) in the future, which will enable the automated management of name server information.

RPP – RESTful Provisioning Protocol

From EPP to RPP

The Extensible Provisioning Protocol (EPP) was standardised in 2009 and has simplified communication between registries and registrars. Prior to the introduction of EPP, the different registries did not have uniform interfaces for the registration and management of domain names.

While EPP still serves the industry well, advances in development and integration tools, operational processes and deployed technologies are driving the need for a new provisioning protocol.

What could a modern protocol look like?

An obvious approach would be to use the REST architecture and the JSON data exchange format. This design could leverage the benefits of stateless architecture and widely used solutions such as OpenAPI, testing and code generation tools, API gateways, authorisation servers and load balancers.

The REST architecture should facilitate integration between registries and registrars. The successful introduction of RDAP has demonstrated the effectiveness of this type of architecture. Integration and efficiency can be increased without sacrificing standardisation.

The new protocol will be called RPP (RESTful Provisioning Protocol).

- It is intended to serve as a modern complement to EPP.
- A new working group on RPP is currently being set up within the IETF (Internet Engineering Task Force).
- The aim of this working group is the specification and standardisation of RPP.
- Switch is following the latest developments and contributing its expertise in EPP and REST.

Article about RPP at DENIC

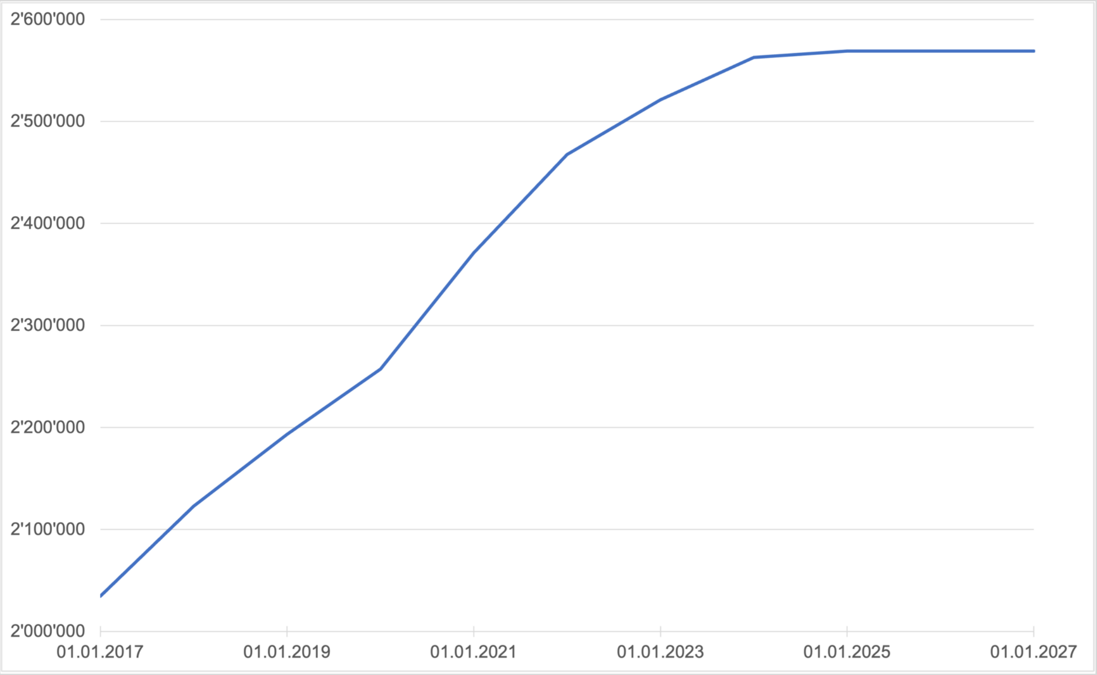
Growth forecast for .ch domain names

2018 and 2019 showed a slightly smaller increase year-on-year. In 2020, the pandemic-related surge in digitalisation and the marketing initiatives of web hosting companies led to increased demand and growth of 4.8%. The increase had already fallen to 3.9% in 2021 but was still higher than before the pandemic.

In 2022, the registry recorded growth of 2.1%. The surge in digitalisation lasted two years and resulted in an unexpected increase of around 100,000 domain names.

In 2023, the growth was just over 40,000 domain names. This corresponds to 1.6%, which falls short of our forecast of 1.8%.

In 2024, we still experienced growth of 6,000 domain names. We predict zero growth for 2025.



Switch
Werdstrasse 2
PO Box
CH-8021 Zurich

Phone +41 44 268 15 15
www.switch.ch
info@switch.ch

Switch_