Rules of the DNS resilience programme

The DNS resilience programme aims to significantly increase the implementation of DNSSEC and other DNS-based security standards for .ch and .li domain names by the recognised Switch Registrars. It is limited to a period of five years. The programme will start on 1 January 2022 and continue until the end of 2026.

Versions

Version	Main changes
June 2021	1st version
November 2021	Criteria from 2024 added
February 2022	Language adjusted for greater clarity
June 2022	Details for DMARC added
November 2022	Criteria for 2025 and further details for DMARC added
June 2023	Details for DANE added
November 2023	Criteria for 2026 added
August 2024	Details for IPv6 added

1 Roles and responsibilities

OFCOM: has commissioned Switch, as part of the renewal agreement, to implement the DNS resilience programme for the domain .ch.

Switch: is the registry for .ch and .li domain names. With the approval of the Liechtenstein Office of Communications, Switch has extended the DNS resilience programme to the .li domain and is implementing the programme on behalf of OFCOM and the Liechtenstein Office of Communications.

Registrars: are organisations that have a contract with Switch and are authorised to register .ch and .li domain names as TLDs. All Switch-recognised Registrars are included in the DNS resilience programme automatically.

DNSSEC Advisory Board: the board consists of one person from OFCOM, one from Switch and a party representing the Registrars. The board defines the criteria for secure domain names.

Monitoring service provider: independent provider that tracks, evaluates and publishes metrics and statistics on the use of security standards in the .ch and .li zone.

2 How it works

Financial incentives are provided to encourage Registrars to invest in security standards. There are two complementary mechanisms for doing this:

A. A **price differentiation** for domain names that meet the criteria for secure domain names versus domain names that do not meet these criteria. The prices are published in the Registrar Portal.
    a. The lower price is billed for all domain names that meet the criteria for secure domain names at the time of subscription renewal.
    b. The higher price is billed for all domain names that do not meet the criteria for secure domain names and also for all newly registered and inactive domain names.

B. The additional revenue from the price differentiation (see A.) will be **refunded** to Registrars whose managed domain names meet the criteria for secure domain names. See chapter 4 for details.

3 Criteria for secure domain names

The criteria for secure domain names are defined by the DNSSEC Advisory Board on an annual basis. Where possible, they aim to coordinate with national and industry-wide incentive measures to increase effectiveness. The measurements carried out by the monitoring service provider form the basis for deciding whether the criteria have been met.

3.1 Criteria for 2022

For price differentiation

Valid DNSSEC signing and validation for the 7 days prior to subscription renewal.

- A query for a non-existing sub-label must trigger a valid NXDOMAIN response.
- At least one authoritative name server must respond correctly.
- Algorithms 5 (RSASHA1), 6 (DSA-NSEC3-SHA1) & 7 (RSASHA1-NSEC3-SHA1) are not permitted.

Note 1: Make sure to allow for sufficient lead time when using CDS.

Note 2: Inactive domain names will be billed at the higher price. The lower price will be billed if the domain name is delegated, activated and signed on a name server, and can be validated. No A or AAAA record is required. We recommend an MX 0 as well as SPF and DMARC record.

For refunds

1 resilience point is awarded for every domain name regarded as secure at the time of subscription renewal based on the above criteria.

3.2 Criteria for 2023

For price differentiation

Valid DNSSEC signing and validation for the 365 days prior to subscription renewal.

- A query for a non-existing sub-label must trigger a valid NXDOMAIN response.
- At least one authoritative name server must respond correctly.
- Algorithms 5 (RSASHA1), 6 (DSA-NSEC3-SHA1) & 7 (RSASHA1-NSEC3-SHA1) are not permitted.

If the criteria are not met, this will be allowed for a maximum of 20 days.

For refunds

1 resilience point is awarded for every domain name regarded as secure at the time of subscription renewal based on the above criteria for 2023.

3.3 Criteria for 2024

For price differentiation

Valid DNSSEC signing and validation for the 365 days prior to subscription renewal.

- A query for a non-existing sub-label must trigger a valid NXDOMAIN response.
- At least one authoritative name server must respond correctly.
- Algorithms 5 (RSASHA1), 6 (DSA-NSEC3-SHA1) & 7 (RSASHA1-NSEC3-SHA1) are not permitted.

If the criteria are not met, this will be allowed for a maximum of 20 days.

For refunds

1 resilience point is awarded for every domain name regarded as secure at the time of subscription renewal based on the above criteria for 2024.

An additional criterion for awarding the resilience point is the authentication of e-mails using DMARC. This criterion must be met for 30 days prior to subscription renewal. The technical requirements are as follows:

SPF

- Valid SPF record according to RFC 7208.
- The final evaluated mechanism must be 'all' with the '-' or '~' qualifier.
- The use of the 'all' mechanism with the '+' qualifier is not allowed.
- If the 'ip4' mechanism is used, the prefix length must not be smaller than 14.
- If the 'ip6' mechanism is used, the prefix length must not be smaller than 32.

DKIM
DKIM is not measured in the context of the resilience programme.

DMARC

- Valid DMARC record according to RFC 7489.
- pct=100, if pct exists.
- p=quarantine or p=reject must be present.

If the criteria are not met, this will be allowed for a maximum of 3 days.

3.4 Criteria for 2025

For price differentiation

Valid DNSSEC signing and validation for the 365 days prior to subscription renewal.

- A query for a non-existing sub-label must trigger a valid NXDOMAIN response.
- At least one authoritative name server must respond correctly.
- Algorithms 5 (RSASHA1), 6 (DSA-NSEC3-SHA1) & 7 (RSASHA1-NSEC3-SHA1) are not permitted.

If the criteria are not met, this will be allowed for a maximum of 20 days.

For refunds

1 resilience point is awarded for every domain name regarded as secure at the time of subscription renewal based on the above criteria for 2025.

An additional criterion for awarding the resilience point is DANE for SMTP. This criterion must be met for 30 days prior to subscription renewal. The technical requirements are as follows:

- If MX is set to '.' no TLSA record is required and the following criteria do not apply.
- Valid TLSA record according to RFC 7671.
- Every MX record at domain apex has at least one matching correctly DNSSEC signed TLSA record.
- Certification type 0 and 1 are not allowed.
- Matching type 0 is not allowed.

If the criteria are not met, this will be allowed for a maximum of 3 days.

3.5 Criteria for 2026

For price differentiation

Valid DNSSEC signing and validation for the 365 days prior to subscription renewal.

- A query for a non-existing sub-label must trigger a valid NXDOMAIN response.
- At least one authoritative name server must respond correctly.
- Algorithms 5 (RSASHA1), 6 (DSA-NSEC3-SHA1) & 7 (RSASHA1-NSEC3-SHA1) are not permitted.

If the criteria are not met, this will be allowed for a maximum of 20 days.

For refunds

1 resilience point is awarded for every domain name regarded as secure at the time of subscription renewal based on the above criteria for 2026.

An additional criterion for awarding the resilience point is IPv6. This criterion must be met for 30 days prior to subscription renewal. The technical requirements are as follows:

- A domain name needs to have at least two name servers with AAAA records and the domain name must resolve over IPv6.
- If the domain apex has an A record there must also be an AAAA record.

If the criteria are not met, this will be allowed for a maximum of 3 days.

4 Finances

As before, the **subscription price** will be settled on a prepaid basis.

The additional revenue, less compensation for the programme, will be **refunded** to the Registrar's account in the first quarter of the following year. The total refund is proportional to the number of resilience points of the Registrar.

5 Communication

Switch will inform all Registrars of the criteria defined for secure domain names by email. The data and statistics collected by the monitoring service provider are shown on their dashboard.

If you have any questions, please send an email to Switch at registrar@nic.ch.