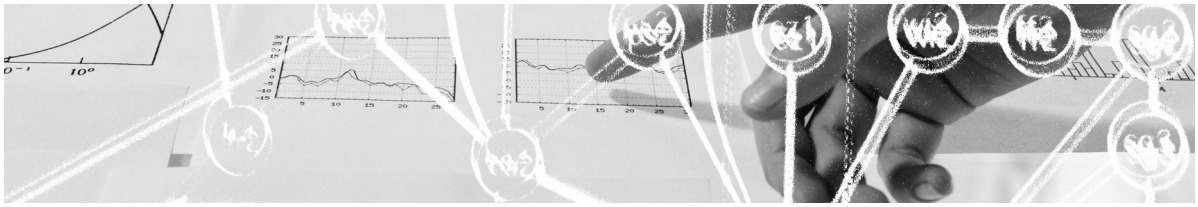
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.nic.ch

Automated DNSSEC Provisioning

Guidelines for CDS processing at SWITCH



Version 1.8, July 7, 2022

Content

1 Introduction

After signing a DNS zone with DNSSEC, DS records have to be submitted to the registry for inclusion in the parent zone in order to complete the chain of trust.

Traditionally, this operation has been performed using EPP updates by the domain's registrar.

The automated DNSSEC provisioning process implemented by SWITCH adds an additional method of updating DS records for DNS operators of second level domains in .ch and .li.

Requests to modify DS records are signaled to the registry by publishing special records in the child zone: CDS (child DS) records. These records are polled regularly by SWITCH in order to process DS updates. Changes made through this method are then communicated to the registrar via EPP poll messages.

This process is implemented according to RFC 7344 and RFC 8078.

2 Instructions for DNS operators

To signal change requests of the DS record set to the parent zone, DNS operators can publish a CDS (type 59) record set. Several name server software products support generating CDS records automatically from the current keys used to sign the zone.

The following example signals a CDS record set during a KSK Double Signature Rollover (see RFC 6781, chapter 4.1.2 Key Signing Key Rollovers):

Current DS in the .ch zone:

einbeispiel.ch. 3600 IN DS 61301 13 2
FB7DF3397DB9AEA62EB81423CA1BB229CCAE3590DCBB16CE46C04D62B48DFB91

When the DS record of the new KSK is ready to be published in the parent zone:

einbeispiel.ch. 3600 IN CDS 45224 13 2
8A7BD58EF0CFA7FFD3813B28A288C69DE9D38D3B5FE71816E82AE26AF0615165

The new DS in the .CH zone after the change has been processed:

einbeispiel.ch. 3600 IN DS 45224 13 2
8A7BD58EF0CFA7FFD3813B28A288C69DE9D38D3B5FE71816E82AE26AF0615165

A child zone can also signal to turn off DNSSEC by removing the DS record set in the parent zone. In this case, the operator may publish a special CDS record which must exactly match:

CDS 0 0 0 00

3 Acceptance criteria

Before changes from discovered CDS record sets are committed to the .ch or .li zone, several syntactic, semantic and security tests are performed. The following conditions must be met before a CDS record set is considered for inclusion:

- The domain name exists and is in the status REGISTERED at the registry.
- DNSSEC validation must succeed using the new DS record set.
- The CDS record set is signed with a key that is represented in both the current DNSKEY and DS record set.
- The CDS record set does not contain syntactic or semantic errors.
- The inception time of the Resource Record Signature (RRSIG) for the CDS RRset is later than the inception time of the last executed change signaled over CDS.
- All key algorithms and digest types in the CDS record set must be supported by the registry:
  - supported algorithms: 8, 10, 13, 14, 15, and 0 for deletion
  - supported digest types: 2, 4, and 0 for deletion
  - **Please note** that algorithms 5 (RSASHA1) and 7 (RSASHA1-NSEC3-SHA1) and digest type 1 (SHA1) are outdated and can no longer be introduced into the DS RRSET. Key rollovers for existing keys using these algorithms and digest type are only accepted for a limited time.

For bootstrapping, the following additional conditions apply:

- The change must be consistently published for more than three consecutive days. Any change to the CDS record set resets the counter. Any change to the DS record set performed through EPP resets the counter as well. This delay does not apply if the CDS RRSET is authenticated, see next chapter "Authenticated Bootstrapping Support".
- A published CDS record set must not change for at least three verification runs. This delay does not apply if the CDS RRSET is authenticated, see next chapter "Authenticated Bootstrapping Support".
- All name servers are reachable over TCP on all their IP addresses and deliver a consistent CDS record set.

For rollovers and delete, the following additional conditions apply:

- DNSSEC validation returns a SECURE result using the current DS record set.

4 Authenticated Bootstrapping Support

If CDS records are authenticated according to https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-bootstrapping, the three-day delay is not necessary and DS records can be activated immediately after the first scan, provided all other consistency checks pass successfully.

Example: If *einbeispiel.ch* has name servers *ns1.example.com* and *ns2.example.net*, the CDS RRSET can be authenticated by co-publishing the same CDS RRSET under *_dsboot.einbeispiel.ch._signal.ns1.example.com* and *_dsboot.einbeispiel.ch._signal.ns2.example.net*.
These records under the name server domain must already be DNSSEC secure.

5 CDS Status Check

DNS operators can verify the current state of CDS processing for any domain name at

https://www.nic.ch/cds

This status page shows the expected processing date for ongoing change requests and additional information for any error preventing a requested change from going forward.

The status information provided over the web interface can also be accessed directly in JSON format with the following RESTful Web Service link:
https://registrar.nic.ch/reg/services/cds/domain_to_check.ch?lang=en

6 Instructions for registrars

6.1 Registry initiated EPP poll messages with ChangePoll extension

Changes to domain names are normally initiated by the registrar using EPP commands. In some cases however, the change may be initiated by the registry and communicated to the registrar through EPP poll messages.

So far, SWITCH uses such messages to inform about outgoing domain name transfers or registry initiated deletion of domain names only. Now, poll messages are also used to inform about DNSSEC changes at the registry triggered by CDS records.
These poll messages are enriched with an `urn:ietf:params:xml:ns:changePoll-1.0` extension element, allowing the registry to provide additional information about the change like date/time and reason (see RFC 8590 https://tools.ietf.org/html/rfc8590). Registrars may use these poll messages to update locally cached state information about a domain name.

6.2 EPP poll messages for automated DNSSEC updates

In the process described in this document, DNSSEC configuration is extracted from the DNS and applied to the domain object.

To inform registrars about such changes, a poll message is prepared and put into the registrar's poll queue. These poll messages contain elements of the secDNS-1.1 and changePoll-1.0 EPP extensions.

The client supported extension list configured at the EPP Login command will influence the rendering of the new poll messages as follows:

- XML elements of extensions configured at Login command will be included in the usual path intended for extension content: **/epp/response/extension**
- XML elements of extensions **not** configured at Login command will be included in the following path: **epp/response/result/extValue**

This rule corresponds to https://datatracker.ietf.org/doc/draft-ietf-regext-unhandled-namespaces (work in progress) and will be applied to all poll messages containing extensions.

Registrars may add the changePoll-1.0 extension to the list of client supported extensions at the Login command. Registrars may add the secDNS-1.1 extension as well if they support provisioning DNSSEC via EPP (see also newest version of our EPP manual).

The **epp/response/result/extValue** element is skipped for the XML schema validation and can contain any XML content. This prevents validation failures for validating client-parsers which are not prepared to process the changePoll-1.0 extension and/or the secDNS-1.1 extension elements. If you intend to unmarshal and parse the data of these extensions you are recommended to include them in the Login command of the session that polls the message and configure the corresponding schemas in your XML parser.

Example Login command with secDNS-1.1, changePoll-1.0 and rgp-1.0 extensions configured:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
   <login>
   <clID>XXXXXXXX</clID>
   <pw>xxxxxxx</pw>
   <options>
    <version>1.0</version>
    <lang>en</lang>
   </options>
   <svcs>
    <objURI>urn:ietf:params:xml:ns:domain-1.0</objURI>
    <objURI>urn:ietf:params:xml:ns:contact-1.0</objURI>
    <objURI>urn:ietf:params:xml:ns:host-1.0</objURI>
    <svcExtension>
     <extURI>urn:ietf:params:xml:ns:rgp-1.0</extURI>
     <extURI>urn:ietf:params:xml:ns:secDNS-1.1</extURI>
     <extURI>urn:ietf:params:xml:ns:changePoll-1.0</extURI>
    </svcExtension>
   </svcs>
  </login>
  <clTRID>EA03_RY_10_1_C</clTRID>
 </command>
</epp>
```

Whatever extension you configure at Login, your EPP client MUST be ready to receive and process EPP poll messages triggered by automated DNSSEC updates. How to test this is described in the next chapter.

6.3 Testing of CDS record triggered EPP poll messages

To provide the possibility to test receiving and processing such messages, SWITCH has implemented a mechanism to trigger predefined CDS related poll messages, using a special domain name in an EPP *domain create* command. The response to such a *domain create* will be as usual but a test poll message is created in the background. It can be received with the ordinary poll command. This feature is only available in the STAGE environment (epp-test.switch.ch).

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
 <command>
  <create>
   <domain:create xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
    <domain:name>polltest-cds-[bootstrap|rollover|delete].ch</domain:name>
    <domain:registrant>SWITCH60</domain:registrant>
    <domain:authInfo>
     <domain:pw>sonstnPW</domain:pw>
    </domain:authInfo>
   </domain:create>
  </create>
  <clTRID>abc</clTRID>
 </command>
</epp>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
 <response>
  <result code="1000">
   <msg lang="en">Poll msg successfully created.</msg>
  </result>
  <trID>
   <clTRID>YOURclTRID</clTRID>
   <svTRID>svTRID</svTRID>
  </trID>
 </response>
</epp>
```

Examples of `<domain:name>` for poll message creation:

A previously not DNSSEC enabled domain name has been configured with DNSSEC:
`<domain:name>`**`polltest-cds-bootstrap.ch`**`</domain:name>`

Changes in the DNSSEC configuration of a DNSSEC configured domain name:
`<domain:name>`**`polltest-cds-rollover.ch`**`</domain:name>`

DNSSEC has been disabled for the domain name:
`<domain:name>`**`polltest-cds-delete.ch`**`</domain:name>`

6.4 Annex: Examples of EPP poll messages

The following section contains examples of all scenarios of enabled or not enabled ChangePoll and secDNS extensions. Messages for rollover of DNSSEC keys and bootstrapping DNSSEC look the same except for the `<changePoll:reason>` which can be:

- DNSSEC initialized
- Rollover of DNSSEC digest
- DNSSEC deactivated

Example of Bootstrap poll response with the following extensions configured at Login:

secDNS-1.1	yes
changePoll-1.0	yes

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1301">
      <msg lang="en">Command completed successfully; ack to dequeue</msg>
    </result>
    <msgQ count="1" id="46533741">
      <qDate>2018-11-20T15:01:01+01:00</qDate>
    </msgQ>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>polltest-cds-bootstrap.ch</domain:name>
        <domain:roid>D123456-SWITCH</domain:roid>
        <domain:status s="inactive" lang="en" />
        <domain:registrant>D1234567-SWITCH</domain:registrant>
        <domain:clID>D1234568-SWITCH</domain:clID>
        <domain:upDate>2018-11-20T15:01:01+01:00</domain:upDate>
      </domain:infData>
    </resData>
    <extension>
      <changePoll:changeData xmlns:changePoll="urn:ietf:params:xml:ns:changePoll-1.0" state="after">
        <changePoll:operation>update</changePoll:operation>
        <changePoll:date>2018-11-20T15:01:01+01:00</changePoll:date>
        <changePoll:svTRID>20181120.123456</changePoll:svTRID>
        <changePoll:who>SWITCH CDS: see https://www.nic.ch/cds/</changePoll:who>
        <changePoll:reason>DNSSEC initialized</changePoll:reason>
      </changePoll:changeData>
      <secDNS:infData xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
        <secDNS:dsData>
          <secDNS:keyTag>1337</secDNS:keyTag>
          <secDNS:alg>13</secDNS:alg>
          <secDNS:digestType>4</secDNS:digestType>

<secDNS:digest>AAAA54840FBBB6F4270F8B6D8C06C6A2B3152E55D2E9F81132130E507829B6D24FA56A4E074B4692DDC46F512B0
48AAC</secDNS:digest>
        </secDNS:dsData>
        <secDNS:dsData>
          <secDNS:keyTag>1337</secDNS:keyTag>
          <secDNS:alg>13</secDNS:alg>
          <secDNS:digestType>2</secDNS:digestType>
          <secDNS:digest>AAAA9AB3E7D203FF7923B8773599E248717F1DC79A9BEF09D8981B13AB7A049E</secDNS:digest>
        </secDNS:dsData>
      </secDNS:infData>
    </extension>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20181120.75241918.758340721</svTRID>
    </trID>
  </response>
</epp>
```

Example of Bootstrap poll response with the following extensions configured at Login:

secDNS-1.1	no
changePoll-1.0	no

```
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1301">
      <msg lang="en">Command completed successfully; ack to dequeue</msg>
      <extValue>
        <value>
          <secDNS:infData xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
            <secDNS:dsData>
              <secDNS:keyTag>1337</secDNS:keyTag>
              <secDNS:alg>13</secDNS:alg>
              <secDNS:digestType>4</secDNS:digestType>

<secDNS:digest>AAAA54840FBBB6F4270F8B6D8C06C6A2B3152E55D2E9F81132130E507829B6D24FA56A4E074B4692DDC46F512B0
48AAC</secDNS:digest>
            </secDNS:dsData>
            <secDNS:dsData>
              <secDNS:keyTag>1337</secDNS:keyTag>
              <secDNS:alg>13</secDNS:alg>
              <secDNS:digestType>2</secDNS:digestType>
              <secDNS:digest>AAAA9AB3E7D203FF7923B8773599E248717F1DC79A9BEF09D8981B13AB7A049E</
secDNS:digest>
            </secDNS:dsData>
          </secDNS:infData>
        </value>
        <reason lang="en">urn:ietf:params:xml:ns:secDNS-1.1 not in login services</reason>
      </extValue>
      <extValue>
        <value>
          <changePoll:changeData xmlns:changePoll="urn:ietf:params:xml:ns:changePoll-1.0">
            <changePoll:operation>update</changePoll:operation>
            <changePoll:date>2018-11-20T15:01:01+01:00</changePoll:date>
            <changePoll:svTRID>20181120.123456</changePoll:svTRID>
            <changePoll:who>SWITCH CDS: see https://www.nic.ch/cds/</changePoll:who>
            <changePoll:reason>DNSSEC initialized</changePoll:reason>
          </changePoll:changeData>
        </value>
        <reason lang="en">urn:ietf:params:xml:ns:changePoll-1.0 not in login services</reason>
      </extValue>
    </result>
    <msgQ count="1" id="46533741">
      <qDate>2018-11-20T15:01:01+01:00</qDate>
    </msgQ>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>polltest-cds-bootstrap.ch</domain:name>
        <domain:roid>D123456-SWITCH</domain:roid>
        <domain:status s="inactive" />
        <domain:registrant>D1234567-SWITCH</domain:registrant>
        <domain:clID>D1234568-SWITCH</domain:clID>
        <domain:upDate>2018-11-20T15:01:01+01:00</domain:upDate>
      </domain:infData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20181120.75241919.758340724</svTRID>
    </trID>
  </response>
</epp>
```

Example of Bootstrap poll response with the following extensions configured at Login:

secDNS-1.1	no
changePoll-1.0	yes

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1301">
      <msg lang="en">Command completed successfully; ack to dequeue</msg>
      <extValue>
        <value>
          <secDNS:infData xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
            <secDNS:dsData>
              <secDNS:keyTag>1337</secDNS:keyTag>
              <secDNS:alg>13</secDNS:alg>
              <secDNS:digestType>4</secDNS:digestType>

<secDNS:digest>AAAA54840FBBB6F4270F8B6D8C06C6A2B3152E55D2E9F81132130E507829B6D24FA56A4E074B46
92DDC46F512B048AAC</secDNS:digest>
            </secDNS:dsData>
            <secDNS:dsData>
              <secDNS:keyTag>1337</secDNS:keyTag>
              <secDNS:alg>13</secDNS:alg>
              <secDNS:digestType>2</secDNS:digestType>

<secDNS:digest>AAAA9AB3E7D203FF7923B8773599E248717F1DC79A9BEF09D8981B13AB7A049E</
secDNS:digest>
            </secDNS:dsData>
          </secDNS:infData>
        </value>
        <reason lang="en">urn:ietf:params:xml:ns:secDNS-1.1 not in login services</reason>
      </extValue>
    </result>
    <msgQ count="1" id="46533741">
      <qDate>2018-11-20T15:01:01+01:00</qDate>
    </msgQ>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>polltest-cds-bootstrap.ch</domain:name>
        <domain:roid>D123456-SWITCH</domain:roid>
        <domain:status s="inactive" lang="en" />
        <domain:registrant>D1234567-SWITCH</domain:registrant>
        <domain:clID>D1234568-SWITCH</domain:clID>
        <domain:upDate>2018-11-20T15:01:01+01:00</domain:upDate>
      </domain:infData>
    </resData>
    <extension>
      <changePoll:changeData xmlns:changePoll="urn:ietf:params:xml:ns:changePoll-1.0"
state="after">
        <changePoll:operation>update</changePoll:operation>
        <changePoll:date>2018-11-20T15:01:01+01:00</changePoll:date>
        <changePoll:svTRID>20181120.123456</changePoll:svTRID>
        <changePoll:who>SWITCH CDS: see https://www.nic.ch/cds/</changePoll:who>
        <changePoll:reason>DNSSEC initialized</changePoll:reason>
      </changePoll:changeData>
    </extension>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20181120.75241920.758340727</svTRID>
    </trID>
  </response>
</epp>
```

Example of Rollover poll response with the following extensions configured at Login:

secDNS-1.1	yes
changePoll-1.0	no

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1301">
      <msg lang="en">Command completed successfully; ack to dequeue</msg>
      <extValue>
        <value>
          <changePoll:changeData xmlns:changePoll="urn:ietf:params:xml:ns:changePoll-1.0">
            <changePoll:operation>update</changePoll:operation>
            <changePoll:date>2018-11-20T15:55:16+01:00</changePoll:date>
            <changePoll:svTRID>20181120.123456</changePoll:svTRID>
            <changePoll:who>SWITCH CDS: see https://www.nic.ch/cds/</changePoll:who>
            <changePoll:reason>Rollover of DNSSEC Digest</changePoll:reason>
          </changePoll:changeData>
        </value>
        <reason lang="en">urn:ietf:params:xml:ns:changePoll-1.0 not in login services</reason>
      </extValue>
    </result>
    <msgQ count="1" id="46533743">
      <qDate>2018-11-20T15:55:16+01:00</qDate>
    </msgQ>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>polltest-cds-rollover.ch</domain:name>
        <domain:roid>D123456-SWITCH</domain:roid>
        <domain:status s="inactive" lang="en" />
        <domain:registrant>D1234567-SWITCH</domain:registrant>
        <domain:clID>D1234568-SWITCH</domain:clID>
        <domain:upDate>2018-11-20T15:55:16+01:00</domain:upDate>
      </domain:infData>
    </resData>
    <extension>
      <secDNS:infData xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
        <secDNS:dsData>
          <secDNS:keyTag>1337</secDNS:keyTag>
          <secDNS:alg>13</secDNS:alg>
          <secDNS:digestType>4</secDNS:digestType>

<secDNS:digest>AAAA54840FBBB6F4270F8B6D8C06C6A2B3152E55D2E9F81132130E507829B6D24FA56A4E074B4692DDC46F51
2B048AAC</secDNS:digest>
        </secDNS:dsData>
        <secDNS:dsData>
          <secDNS:keyTag>1337</secDNS:keyTag>
          <secDNS:alg>13</secDNS:alg>
          <secDNS:digestType>2</secDNS:digestType>
          <secDNS:digest>AAAA9AB3E7D203FF7923B8773599E248717F1DC79A9BEF09D8981B13AB7A049E</
secDNS:digest>
        </secDNS:dsData>
      </secDNS:infData>
    </extension>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20181120.75241927.758340753</svTRID>
    </trID>
  </response>
</epp>
```

Example of Delete poll response with the following extensions configured at Login:

secDNS-1.1	yes
changePoll-1.0	yes

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1301">
      <msg lang="en">Command completed successfully; ack to dequeue</msg>
    </result>
    <msgQ count="1" id="46533742">
      <qDate>2018-11-20T15:12:41+01:00</qDate>
    </msgQ>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>polltest-cds-delete.ch</domain:name>
        <domain:roid>D123456-SWITCH</domain:roid>
        <domain:status s="inactive" lang="en" />
        <domain:registrant>D1234567-SWITCH</domain:registrant>
        <domain:clID>D1234568-SWITCH</domain:clID>
        <domain:upDate>2018-11-20T15:12:41+01:00</domain:upDate>
      </domain:infData>
    </resData>
    <extension>
      <changePoll:changeData xmlns:changePoll="urn:ietf:params:xml:ns:changePoll-1.0"
state="after">
        <changePoll:operation>update</changePoll:operation>
        <changePoll:date>2018-11-20T15:12:41+01:00</changePoll:date>
        <changePoll:svTRID>20181120.123456</changePoll:svTRID>
        <changePoll:who>SWITCH CDS: see https://www.nic.ch/cds/</changePoll:who>
        <changePoll:reason>DNSSEC deactivated</changePoll:reason>
      </changePoll:changeData>
    </extension>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20181120.75241923.758340738</svTRID>
    </trID>
  </response>
</epp>
```

7 References

Automating DNSSEC Delegation Trust Maintenance
https://tools.ietf.org/html/rfc7344

Managing DS Records from the Parent via CDS/CDNSKEY
https://tools.ietf.org/html/rfc8078

DNS Transport over TCP - Implementation Requirements
https://tools.ietf.org/html/rfc7766

Change Poll Extension for the Extensible Provisioning Protocol (EPP)
https://tools.ietf.org/html/rfc8590