Transfer von Domain-Namen mit DNSSEC

3. DENIC Testbed Meeting

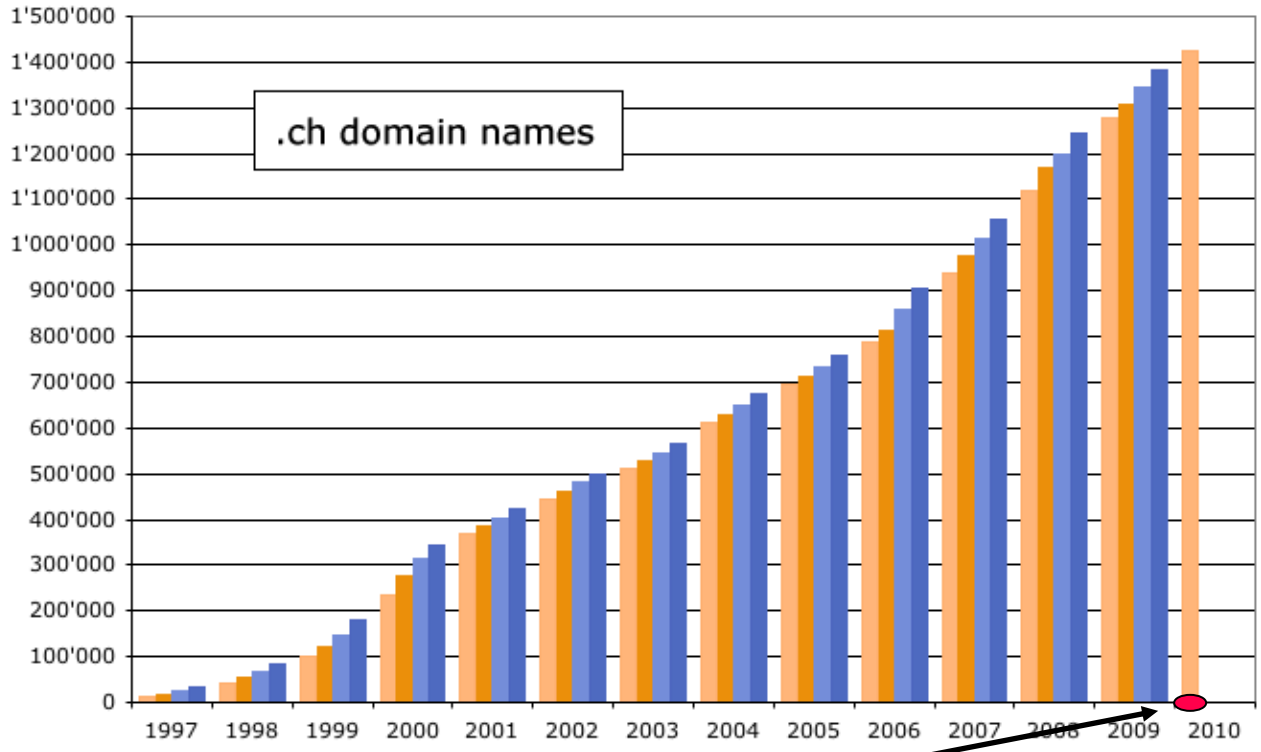
SWITCH
Serving Swiss Universities

Samuel Benz
samuel.benz@switch.ch

Frankfurt, 16. Juni 2010

DNSSEC in der Schweiz

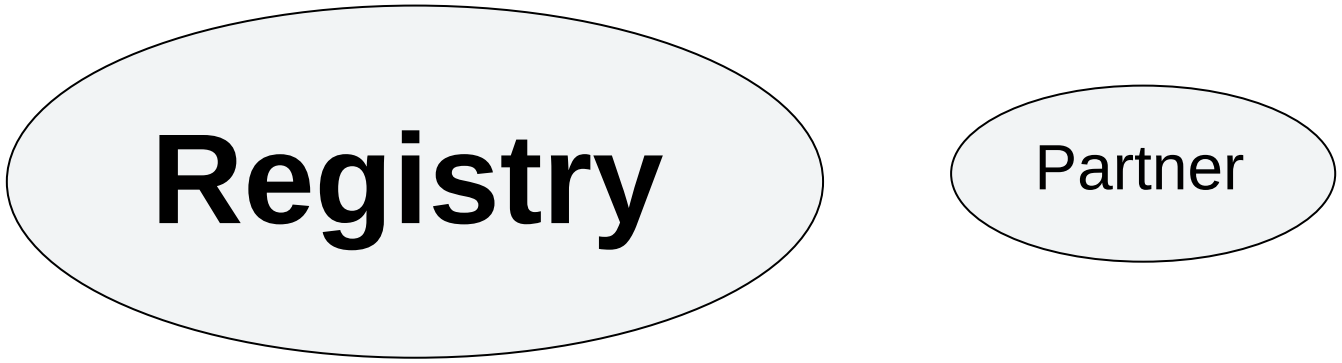
- CH. seit dem 11. September 2009 signiert, Schlüssel im ITAR
- Schlüssel-Registration öffentlich seit dem 2. Februar 2010



60 (0.004%) mit DNSSEC

Partner System Schweiz

- Registry- / Registrar- System
- Grösster Teil der Domain-Namen als Direktkunden bei der Registry



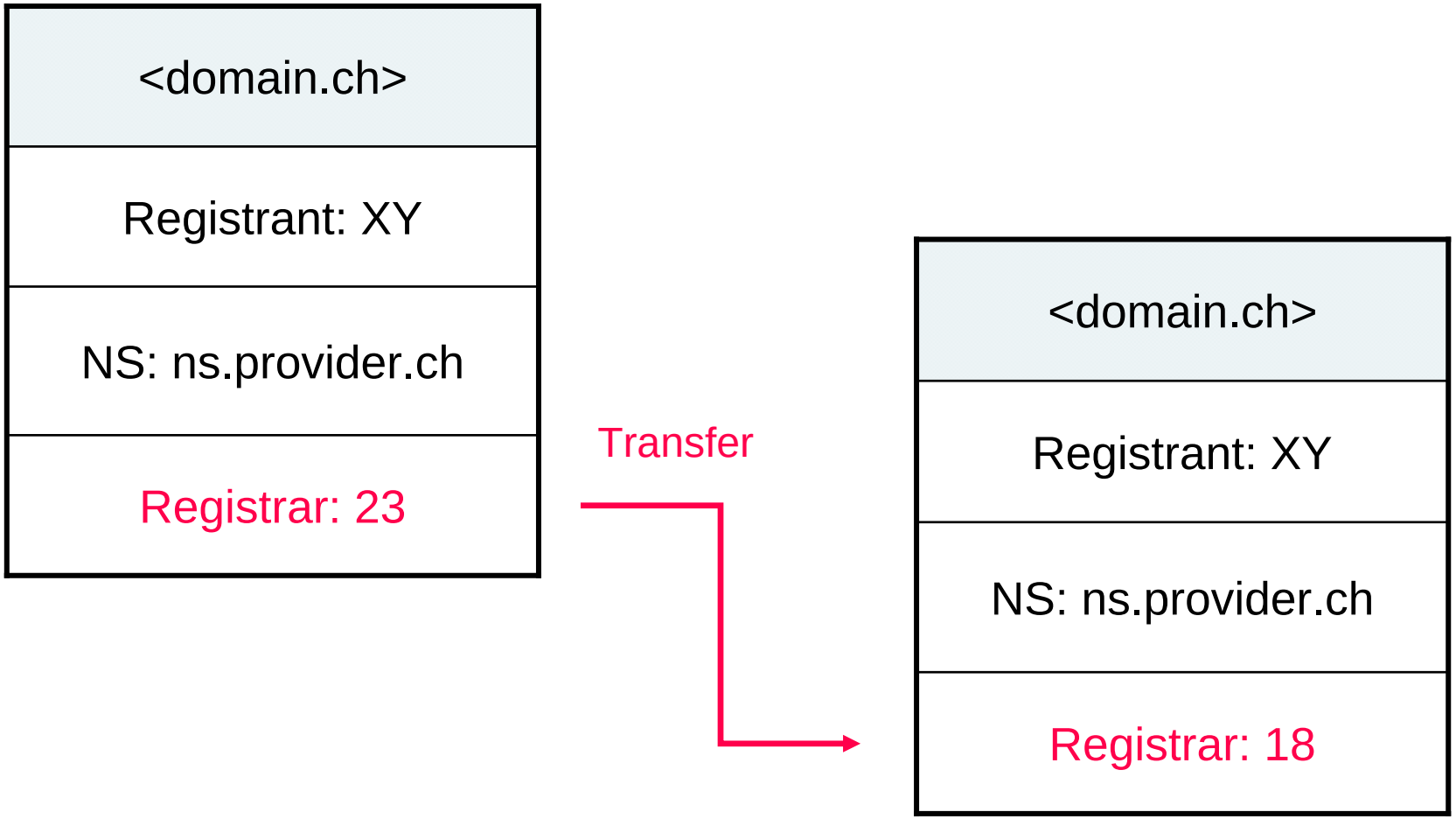
- ~50 Partner welche mittels EPP mit der Registry kommunizieren
- 0 Transfers eines Domain-Namen mit DNSSEC

Probleme im Zusammenhang mit DNSSEC

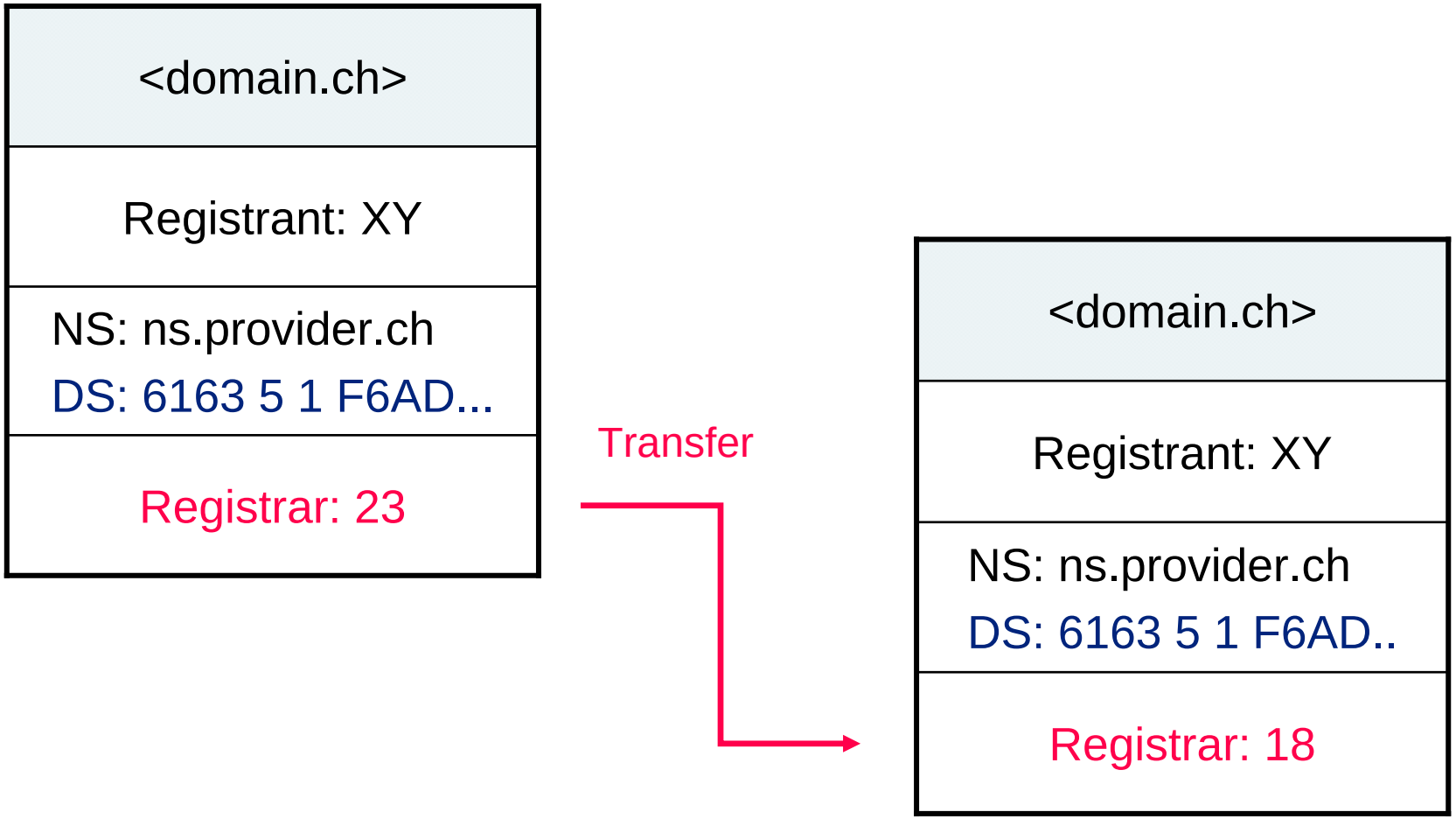
1. DNS Operator wechseln (Unabhängig von einem Registrar-Transfer)
   - > Mehr dazu im Anschluss an diese Präsentation

2. Transfer: DNSSEC Unterstützung der Registrare
   - > In dieser Präsentation betrachtetes Problem

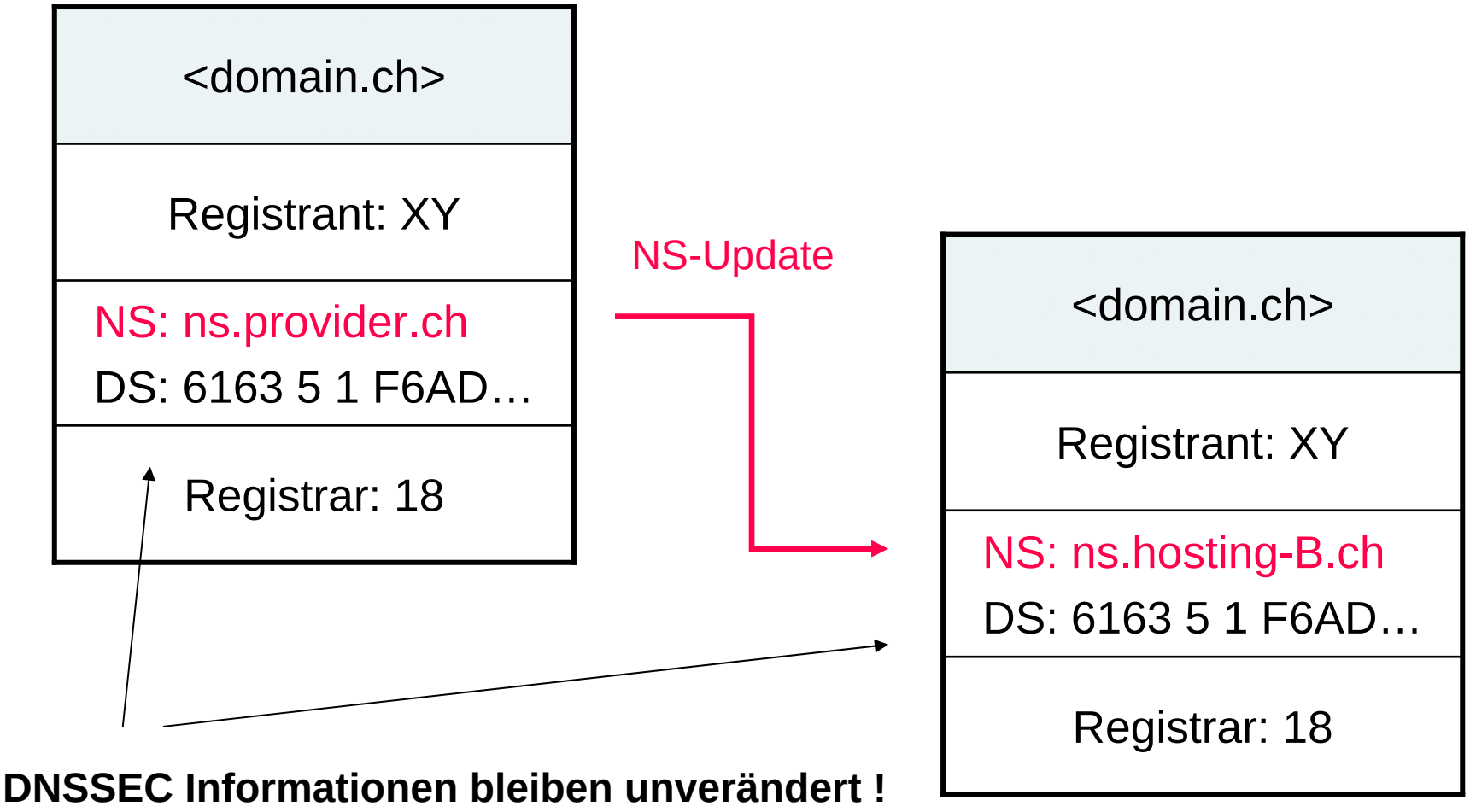
Der Transfer



Der Transfer mit DNSSEC



Problem nach einem Transfer mit DNSSEC



DNSSEC Informationen bleiben unverändert !

3 Mögliche Lösungen

1. Alle Registrare müssen DNSSEC unterstützen (oder zumindest das Kommando um DNSSEC auszuschalten).
2. Die Registry schaltet DNSSEC bei einem Transfer zu einem Registrar ohne DNSSEC Support stillschweigend aus.
3. Die Registry verweigert einen Transfer eines Domain-Namens mit DNSSEC zu einem Registrar welcher DNSSEC nicht unterstützt. (Der alte Registrar muss in diesem Fall, DNSSEC zuerst ausschalten)

SWITCH wählte die Option 3.

Umsetzung Option 3

• Der Registrar muss für die Nutzung von DNSSEC separat freigeschaltet werden (Vertrags-Zusatz).

•Login mit DNSSEC nur für aktivierte Partner möglich

•Transfer von Domain-Namen mit DNSSEC nur zu aktivierten Partnern möglich

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
 <command>
  <login>
   <clID>YOUR-CLID</clID>
   <pw>ABCDEF</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>
   </svcs>
  </login>
  <clTRID>ABC.1</clTRID>
 </command>
</epp>
```

DNSSEC Zusatz

```
<svcExtension>
  <extURI>urn:ietf:params:xml:ns:secDNS-1.0</extURI>
</svcExtension>
```

•Problem: Gewisse EPP Libraries verwenden Extension automatisch!

EPP Implementation

- EPP Extension gemäss RFC 4310
  - Keine SWITCH spezifischen Änderungen
  - Es wird das Domain-Objekt erweitert
  - DS Records müssen, DNSKEY Records können übergeben werden
  - SWITCH macht keine Delegationschecks und überprüft nicht, ob signierte Domain-Namen erreichbar sind.

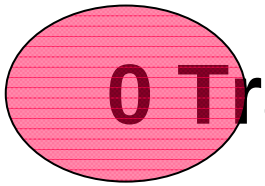
- Weitere Details sind im Anhang dieser Präsentation

Ausblick: RFC 4310 vs. RFC 5910

- RFC 5910 ersetzt RFC 4310
- secDNS-1.0 → secDNS-1.1

- NEU: dsData- oder keyData- Interface
- update:rem über dsData und nicht key_id
- Add/Rem/Chg nun EPP konform
  - rem/add als Sequenz möglich
  - remove all
  - chg ändert und ersetzt nicht alles

Wie weiter ?



Transfers eines Domain-Namen mit DNSSEC ?!

http://www.nic.ch/dnssec

Anhang: EPP Details

Zugelassene Werte in den EPP Attributen:

DNSSEC Attribut	M	Bemerkung
alg	Y	Alghoritmus (Aktuell 3,5,6,7,8,10)
digestType	Y	1 oder 2
digest	Y	Max. 128 Charakter
flags	N	256 oder 257
protocol	N	3
keyTag	Y	0-65535
pubKey	N	Max. 1024 Charakter

M = Obligatorisch (mandatory)

Y = Yes

N = No

epp:login

Beispiel login Command

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
 <command>
  <login>
   <clID>YOUR-CLID</clID>
   <pw>ABCDEF</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>
   </svcs>
  </login>
  <clTRID>ABC.1</clTRID>
 </command>
</epp>
```

DNSSEC Zusatz

```
<svcExtension>
  <extURI>urn:ietf:params:xml:ns:secDNS-1.0</extURI>
</svcExtension>
```

domain:info

Beispiel domain info Response

```
<?xml version="1.0" encoding="UTF-8"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1000">
      <msg lang="en">Command completed successfully</msg>
    </result>
    <resData>
      <domain:infData xmlns:domain="urn:ietf:params:xml:ns:
       domain-1.0">
        <domain:name>yourname.ch</domain:name>
        <domain:roid>D2586061-SWITCH</domain:roid>
        <domain:status s="ok"/>
        <domain:registrant>5527981</domain:registrant>
        <domain:contact type="tech">5527981</domain:contact>
        <domain:ns>
          <domain:hostObj>ns1.yourname.ch</domain:hostObj>
          <domain:hostObj>ns2.yourname.ch</domain:hostObj>
        </domain:ns>
        <domain:clID>3703709</domain:clID>
        <domain:exDate>2009-01-31T00:00:00+01:00
        </domain:exDate>
        <domain:authInfo>
          <domain:pw>foo#Bar%</domain:pw>
        </domain:authInfo>
      </domain:infData>
    </resData>
    <trID>
      <clTRID>ABC-12345</clTRID>
      <svTRID>20080529.27664.913190</svTRID>
    </trID>
  </response>
</epp>
```

Bei DNSSEC signierten Domain-Namen

```
<extension>
  <secDNS:infData
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0">
    <dsData xmlns="urn:ietf:params:xml:ns:secDNS-1.0">
      <keyTag>43837</keyTag>
      <alg>5</alg>
      <digestType>2</digestType>
      <digest>838C3D0966B9EE55</digest>
      <keyData>
        <flags>257</flags>
        <protocol>3</protocol>
        <alg>5</alg>
        <pubKey>TH3PUBL1CK3Y</pubKey>
      </keyData>
    </dsData>
  </secDNS:infData>
</extension>
```

domain:create

Beispiel domain create Command

```
<?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>yourname.ch</domain:name>
         <domain:ns>
          <domain:hostObj>ns1.yourname.ch</domain:hostObj>
          <domain:hostObj>ns2.yourname.ch</domain:hostObj>
         </domain:ns>
        <domain:registrant>HOLDERCONTACT</domain:registrant>
        <domain:contact
         type="tech">TECHCONTACT</domain:contact>
        <domain:authInfo>
          <domain:pw/>
        </domain:authInfo>
      </domain:create>
    </create>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

DNSSEC Zusatz

```
<extension>
  <secDNS:create
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0">
    <secDNS:dsData>
      <secDNS:keyTag>12345</secDNS:keyTag>
      <secDNS:alg>3</secDNS:alg>
      <secDNS:digestType>1</secDNS:digestType>
      <secDNS:digest>49FD46E6C4B45C55</secDNS:digest>
      <secDNS:keyData>
        <secDNS:flags>256</secDNS:flags>
        <secDNS:protocol>3</secDNS:protocol>
        <secDNS:alg>3</secDNS:alg>
        <secDNS:pubKey>TH3PUBL1CK3Y</secDNS:pubKey>
      </secDNS:keyData>
    </secDNS:dsData>
  </secDNS:create>
</extension>
```

`keyData` ist optional. Bei Mitsenden muss die Berechnung des `pubKey` zum `digest` führen.

domain:update

Beispiel domain update Command

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <update>
      <domain:update
       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>yourname.ch</domain:name>
        <domain:add>
          <domain:ns>
            <domain:hostObj>ns.yourns.ch</domain:hostObj>
          </domain:ns>
         <domain:contact
          type="tech">NEWTECHCONTACT</domain:contact>
        </domain:add>
           <domain:rem>
             <domain:contact
              type="tech">OLDTECHCONTACT</domain:contact>
           </domain:rem>
        <domain:chg>
          <domain:authInfo>
            <domain:pw>2BARfoo</domain:pw>
          </domain:authInfo>
        </domain:chg>
      </domain:update>
    </update>
    <clTRID>Test3</clTRID>
  </command>
</epp>
```

DNSSEC Zusatz

DNSSEC Daten hinzufügen:

```
<extension>
  <secDNS:update
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0">
    <secDNS:add>
      <secDNS:dsData>
        <secDNS:keyTag>12346</secDNS:keyTag>
        <secDNS:alg>3</secDNS:alg>
        <secDNS:digestType>1</secDNS:digestType>
        <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
      </secDNS:dsData>
    </secDNS:add>
  </secDNS:update>
 </extension>
```

DNSSEC Daten ersetzen (alle DS-Records werden überschrieben):

```
<extension>
  <secDNS:update
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0">
    <secDNS:chg>
      <secDNS:dsData>
        <secDNS:keyTag>12345</secDNS:keyTag>
        <secDNS:alg>3</secDNS:alg>
        <secDNS:digestType>1</secDNS:digestType>
        <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
        <secDNS:keyData>
          <secDNS:flags>256</secDNS:flags>
          <secDNS:protocol>3</secDNS:protocol>
          <secDNS:alg>1</secDNS:alg>
          <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
        </secDNS:keyData>
      </secDNS:dsData>
    </secDNS:chg>
  </secDNS:update>
</extension>
```

DNSSEC Daten entfernen (Alle DS-Records die den mitgelieferten Attributen ensprechen werden gelöscht):

```
<extension>
  <secDNS:update
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.0">
   <secDNS:rem>
     <secDNS:keyTag>12345</secDNS:keyTag>
   </secDNS:rem>
  </secDNS:update>
</extension>
```