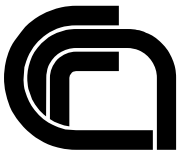

Consiglio Nazionale delle Ricerche

DNSSEC in the ccTLD .it - Main EPP implementation choices

M. Loffredo, M. Martinelli, R. Ravazzolo

IIT TR-01/2017

Technical Report

Gennaio 2017

Istituto di Informatica e Telematica

DNSSEC in the ccTLD .it
Main EPP implementation choices

Loffredo M., Martinelli M., Ravazzolo R.

Summary

1. Introduction

The DNS protocol (Domain Name System)[1,2] defines the specifications to provide a domain name resolution service that has no form of authentication nor implements mechanisms to ensure data integrity. In order to overcome this limitation, the IETF has defined a protocol known as Domain Name System Security Extensions (DNSSEC).

The registration system of the .it Registry allows Registrars to register and maintain domain names and their DNS configurations in real time. The system uses the EPP (Extensible Provisioning Protocol) protocol to comply with internationally accepted standards. The EPP is a synchronous client-server protocol based on XML requests and responses on HTTP protocol.

This document outlines the main choices of .it Registry about the DNSSEC implementation. Registrars wishing to provide DNSSEC service for .it domains must take some actions involving both their DNS and their EPP client.

2. DNSSEC

DNSSEC[3,4] uses public/private keys for cryptography to ensure that the information is coming from an authoritative source, and has not been altered during its transport through the network.

DNSSEC enables:

- DNS servers to sign their own resource records (RR) with a private key;
- DNS resolvers to verify the information through the corresponding public key.

Public keys are stored in the "parent" zone of the digitally signed zone.

To facilitate the verification of signatures, DNSSEC has established some new RR[5,6]:

- RRSIG: containing a cryptographic signature for a set of RR of the same type (RRset);
- DNSKEY: containing a public key.

DNSSEC also introduces the Delegation Signer (DS) record to implement the "chain-of-trust" between a parent zone and a child zone. A zone manager generates a "digest" of the public key (DNSKEY record) associated with the digitally signed domain and transmits it to the parent zone manager who associates the delegation of the domain name through a DS record.

3. DS Record

In general, the most commonly used methods to obtain the DS record to be associated with a domain name and to create the "chain-of-trust" in a TLD zone are:

1. the Registrar (the person managing the authoritative name server of the zone you wish to sign) generates and transmits the DS record (via EPP, via Web portal, etc.) to the Registry that manages the TLD;
2. the Registrar (the person managing the authoritative name server of the zone you wish to sign) generates and transmits (via EPP, via Web portal, etc.) to the Registry that manages the TLD the public key associated to the zone and consequently, the DS record generation is ascribed to the TLD Registry.

The ccTLD.it has implemented the first solution, that is: the Registrar shall transmit to Registro.it the DS records associated with a domain name. Even if a domain name has the DNS service managed by someone other than the Registrar, the DS record transmission is still under the responsibility of the Registrar of the domain name, and must be made exclusively through the EPP protocol.

In practice, the Registrar must communicate to the Registro.it via EPP the following four fields, which compose the DS record associated with the domain name that has been signed:

- ***keytag***: this value is automatically calculated when the DS record is generated and depends strictly on the information related to the public key;
- ***algorithm***: the values[7] supported by the Registro.it are the following:
    - **3** (DSA/SHA-1)
    - **5** (RSA/SHA-1)
    - **6** (DSA-NSEC3-SHA1)
    - **7** (RSASHA1-NSEC3-SHA1)
    - **8** (RSA/SHA-256)
    - **10** (RSA/SHA-512)
    - **12** (ECC-GOST)
    - **13** (ECDSAP256SHA256)
    - **14** (ECDSAP384SHA384)
- ***digest type***: the values[8] supported by the Registro.it are the following:
    - **1** (SHA-1)
    - **2** (SHA-256)
    - **3** **(**GOST R 34.11-94)
    - **4** **(**SHA-384)
- ***digest***: is the hash generated from the public key according to the *algorithm* and *digest type*.

4. Registrars and DNSSEC

In the .it ccTLD, the adoption of the DNSSEC protocol by the Registrars is neither mandatory nor binding. Registrars interested in providing this new service to their customers will have to carry out a "Technical DNSSEC accreditation test", whose specifications will be outlined in a dedicated document.

The Registrars that, on the contrary, do not wish to make use of this new service, will continue to operate as at present.

Registrars will therefore be divided into two categories: “DNSSEC accredited“ and "non DNSSEC accredited". A special logo will identify the "DNSSEC accredited" Registrars on the Registry website (http://www.nic.it/registrars/list section). The Whois service will contain, in the Registrar section, a new "DNSSEC" field with "yes" or "no" values depending on whether the Registrar is DNSSEC accredited or not.

Similarly, the Whois service will include, for domains, the field "Signed" with "yes" or "no" values, depending on whether the domain has been signed or not.

Also the public test environment will provide the opportunity to register and manage digitally signed domain names. In order to be enabled to test DNSSEC functionalities in this environment, the Registrar must send an explicit request to hostmaster@nic.it. As a result, both test Registrar accounts associated with the requesting entity, will become “DNSSEC accredited”.

A Registrar will have the possibility to carry out the DNSSEC technical accreditation test, if and only if, it is an accredited Registrar in the .it and in "active" status.

In the .it ccTLD the transmission of DS records associated with digitally signed zones, for their publication in the .it zone file, will be carried out by the "DNSSEC accredited" Registrars and this must take place exclusively through the EPP protocol.

5. EPP and DNSSEC

What are the implications of the introduction of DNSSEC on the requests that a "DNSSEC accredited" Registrar must send to the EPP[9,10] server of Registro.it through its client?

The **secDNS-1.1**[11] standard extension to the EPP protocol describes two different ways to enable a Registrar to transmit to the Registry the information regarding the DS records:

1. The first, referred to as "DS Data Interface" foresees the transmission via EPP of DS records information to the Registry. This transmission takes place concurrently with the registration of a "signed" domain (through the EPP Domain Create operation) or a subsequent modification of the DS records associated with it (addition, removal or replacement by an EPP Update Domain operation). The EPP server of the Registry will report such information in the response to the EPP Domain Info request.

2. The second, termed “Key Data Interface”, is quite similar to the first with the difference that the Registrar, instead of providing information about the DS records, must provide data on the public key associated with the signed domain (flags, protocol, alg, pubkey).

Optionally, the protocol provides that the "DS Data Interface" can be used to provide, along with the DS record information, also those relating to the "Key Data Interface". This is to facilitate an eventual consistency check by the Registry between the public key and the DS records associated with the domain name. It is mandatory that the EPP server supports a single mode of transmission of information within a single request or response.

The.it ccTLD has chosen the “DS Data Interface” way of transmission, by which the Registrar sends to the Registry information concerning only DS records.

Let us now see the main EPP operations that are involved in the introduction of DNSSEC in .it, where a Registrar has passed the DNSSEC technical accreditation test and consequently is a “DNSSEC accredited” Registrar.

5.1 EPP Login

A “DNSSEC accredited” Registrar must always indicate in the *EPP Login* request also the two following namespaces:

- **urn:ietf:params:xml:ns:secDNS-1.1**, concerning the standard extensions introduced by the EPP protocol;
- **http://www.nic.it/ITNIC-EPP/extsecDNS-1.0**, concerning the extensions introduced by the Registro.it.

An *EPP Login* request will then have the following XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
<command>
  <login>
    <clID>DEMO-REG</clID>
    <pw>14nov07</pw>
    <options>
      <version>1.0</version>
      <lang>en</lang>
    </options>
    <svcs>
      <objURI>urn:ietf:params:xml:ns:contact-1.0</objURI>
      <objURI>urn:ietf:params:xml:ns:domain-1.0</objURI>
      <svcExtension>
        <extURI>http://www.nic.it/ITNIC-EPP/extepp-2.0</extURI>
        <extURI>http://www.nic.it/ITNIC-EPP/extcon-1.0</extURI>
        <extURI>http://www.nic.it/ITNIC-EPP/extdom-2.0</extURI>
        <extURI>urn:ietf:params:xml:ns:rgp-1.0</extURI>
        <extURI>urn:ietf:params:xml:ns:secDNS-1.1</extURI>
        <extURI>http://www.nic.it/ITNIC-EPP/extsecDNS-1.0</extURI>
      </svcExtension>
    </svcs>
  </login>
</command>
</epp>
```

If the "DNSSEC accredited" Registrar does not include in the *EPP Login* request the two above indicated namespaces, it will obtain the following error message:

- Code **2003** (**Required parameter missing**) - Reason **4012** (**Extension URI missing**), with reference to the missing namespace.

If a "non DNSSEC accredited" Registrar inserts in the *EPP Login* request (or in any other EPP request) one or both of the above namespaces, it gets the following error message:

- Code **2306** (**Parameter value policy error**) Reason **10001** (**DNSSEC: registrar is not DNSSEC accredited**), with reference to the wrong namespace.

The responses obtained by the EPP server will have a different header depending on whether the Registrar is "DNSSEC accredited" or "not DNSSEC accredited":

- **Header of the EPP response for a "DNSSEC accredited" Registrar**, following an *EPP Login* operation (the same header is valid for any operation carried out by the Registrar):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
```

```
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extsecDNS="http://www.nic.it/ITNIC-EPP/extsecDNS-1.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
```

- **Header of the EPP response for a "not DNSSEC accredited" Registrar**, following an EPP Login operation (the same header applies to any operation carried out by the Registrar):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
```

5.2 EPP Domain Create

The *EPP Domain Create* command has been extended with the addition, in the **<extension>** section, of the **<secDNS:create>** element (where secDNS is the prefix that identifies the reference to the secDNS-1.1 namespace), which can contain up to a maximum of 2 elements <**secDNS:Dsdata**> corresponding to DS records.

Therefore, an EPP Domain Create request for a .it domain name with the DNSSEC extension that makes use of the DS Data Interface, has the following XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
<command>
   <create>
     <domain:create
     xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
     xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd">
     <domain:name>esempio.it</domain:name>
     <domain:period unit="y">1</domain:period>
     <domain:ns>
       <domain:hostAttr>
         <domain:hostName>x.dns.it</domain:hostName>
       </domain:hostAttr>
       <domain:hostAttr>
         <domain:hostName>y.dns.it</domain:hostName>
       </domain:hostAttr>
     </domain:ns>
     <domain:registrant>mm001</domain:registrant>
     <domain:contact type="admin">mm001</domain:contact>
```

```
    <domain:contact type="tech">mb001</domain:contact>
    <domain:authInfo>
      <domain:pw>22fooBAR</domain:pw>
    </domain:authInfo>
    </domain:create>
  </create>
  <extension>
    <secDNS:create
      xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
    <secDNS:dsData>
      <secDNS:keyTag>12345</secDNS:keyTag>
      <secDNS:alg>3</secDNS:alg>
      <secDNS:digestType>1</secDNS:digestType>
      <secDNS:digest>4347D0F8BA661234A8EADC005E2E1D1B646C9682</secDNS:digest>
    </secDNS:dsData>
    </secDNS:create>
  </extension>
  <clTRID>ABC-12345</clTRID>
</command>
</epp>
```

Possible error messages that a "DNSSEC accredited" Registrar can receive following the sending of an EPP Domain Create request containing the extension <secDNS:create> are as follows:

- Code **2001** (**Command syntax error**) Reason **4003** (**Syntax error**):
  - If a <secDNS:dsData> element contains a value of the *keyTag* field not included in the 0-65535 range;
  - If a <secDNS:dsData> element contains a value of the *digestType* field not included in the 0-255 range;
  - If a <secDNS:dsData> element contains a value of the *alg* field not included in the 0-255 range.

- Code **2102** (**Unimplemented option**) Reason **10002** (**DNSSEC: unsupported maxSigLife element**):
  - If within the <secDNS:create> element there is <secDNS:maxSigLife>.

- Code **2102** (**Unimplemented option**) Reason **10003** (**DNSSEC: unsupported keyData element**):
  - If within the <secDNS:create> element there is <secDNS:keyData> in place of or within <secDNS:dsData>.
- Code **2306** (**Parameter value policy error**) Reason **10007** (**DNSSEC: invalid digestType value**):
  - If the <secDNS:dsData> element contains an unsupported or invalid value of the *digestType* field.

- Code **2306** (**Parameter value policy error**) Reason **10008** (**DNSSEC: invalid alg value**):
  - If the <secDNS:dsData> contains an unsupported or invalid value of the *alg* field.

- Code **2306** (**Parameter value policy error**) Reason **10009** (**DNSSEC: invalid digest value**):
  - If the <secDNS:dsData> contains a value of the *digest* field whose length is not compatible with the chosen *digest type*.

- Code **2306** (**Parameter value policy error**) Reason **10010** (**DNSSEC: duplicate dsData**):
  - if 2 elements are indicated <secDNS:dsData> containing the same values for the 4 fields expected.

- Code **2308** (**Data management policy violation**) Reason **10006** (**DNSSEC: too many dsData items**):
  - If within the <secDNS:create> element a number of <secDNS:dsData> elements greater than 2 is indicated.

5.3 EPP Domain Update

The command *EPP Domain Update* has been extended indicating, in the **<extension>** section, the element **<secDNS:update>**.

Therefore, an *EPP Update Domain* request for a .it domain, with the DNSSEC extension that makes use of the DS Data Interface, for which the replacement of the DS Record currently associated with another DS record was requested, has the following XML format (in the example below it is requested to replace the current DS record with a new one):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <command>
   <update>
     <domain:update
     xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
     xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd">
        <domain:name>esempio.it</domain:name>
     </domain:update>
   </update>
   <extension>
     <secDNS:update
     xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
        <secDNS:rem>
        <secDNS:dsData>
        <secDNS:keyTag>12345</secDNS:keyTag>
        <secDNS:alg>3</secDNS:alg>
        <secDNS:digestType>1</secDNS:digestType>
        <secDNS:digest>4347D0F8BA661234A8EADC005E2E1D1B646C9682</secDNS:digest>
        </secDNS:dsData>
        </secDNS:rem>
        <secDNS:add>
        <secDNS:dsData>
        <secDNS:keyTag>45063</secDNS:keyTag>
        <secDNS:alg>3</secDNS:alg>
        <secDNS:digestType>2</secDNS:digestType>
        <secDNS:digest>
        E9B696C3AC8644735BF0A6409BE6D77BBFB4142D667E0EB0D41AD75BCC9D0D43
        </secDNS:digest>
        </secDNS:dsData>
        </secDNS:add>
     </secDNS:update>
   </extension>
   <clTRID>ABC-12345</clTRID>
   </command>
</epp>
```

If the Registrar intends to request the removal of all DS records associated with the domain, this is allowed through an EPP Domain Update operation in which, in **<secDNS:rem>** section, the **<secDNS:all>** element is used.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <command>
   <update>
     <domain:update
     xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
     xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd">
       <domain:name>esempio.it</domain:name>
     </domain:update>
   </update>
   <extension>
     <secDNS:update
     xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
       <secDNS:rem>
         <secDNS:all>true</secDNS:all>
       </secDNS:rem>
     </secDNS:update>
   </extension>
   <clTRID>ABC-12345</clTRID>
   </command>
</epp>
```

Possible error messages that a "DNSSEC" Registrar can receive following the sending of an EPP Update Domain request containing the extension <secDNS:update> are as follows:

- Code **2001** (**Command syntax error**) Reason **4003** (**Syntax error**):
  - If a <secDNS:dsData> element contains a value of the *keyTag* field not included in the 0-65535 range;
  - If a <secDNS:dsData> element contains a value of the *digestType* field not included in the 0-255 range;
  - If a <secDNS:dsData> element contains a value of the *alg* field not included in the 0-255 range.

- Code **2102** (**Unimplemented option**) Reason **10002** (**DNSSEC: unsupported maxSigLife element**):
  - If the <secDNS:update> contains the <secDNS:maxSigLife> element.

- Code **2102** (**Unimplemented option**) Reason **10003** (**DNSSEC: unsupported keyData element**):
  - If the <secDNS:update> element contains a <secDNS:keyData> element in place of or within the <secDNS:dsData> element.

- Code **2102** (**Unimplemented option**) Reason **10004** (**DNSSEC: unsupported urgent attribute**):
  - If the <secDNS:update> element contains the *urgent* attribute.

- Code **2306** (**Unimplemented option**) Reason **10005** (**DNSSEC: no dsData to rem or add**)

- If the <secDNS:update> element contains neither the <secDNS:add> element nor the <secDNS:rem> element; or contains the <secDNS:rem> element that contains neither single <secDNS:dsData> elements nor the <secDNS:all> element.

- Code **2306** (**Parameter value policy error**) Reason **10007** (**DNSSEC: invalid digestType value**):
  - If a <secDNS:dsData> element contains an unsupported or invalid *digestType* field.

- Code **2306** (**Parameter value policy error**) Reason **10008** (**DNSSEC: invalid alg value**):
  - If a <secDNS:dsData> element contains an unsupported or invalid *alg* field.

- Code **2306** (**Parameter value policy error**) Reason **10009** (**DNSSEC: invalid digest value**):
  - If a <secDNS:dsData> element contains a value of the *digest* field whose length is not compatible with the chosen *digest type*.

- Code **2306** (**Parameter value policy error**) Reason **10010** (**DNSSEC: duplicate dsData**):
  - If 2 <secDNS:dsData> elements contain the same values for the 4 fields foreseen.

- Code **2306** (**Parameter value policy error**) Reason **10011** (**DNSSEC: dsData to add is already associated with the domain**):
  - If a DS record indicated in the <secDNS:add> element is already associated with the domain name.

- Code **2306** (**Parameter value policy error**) Reason **10012** (**DNSSEC: dsData to remove is not associated with the domain**):
  - If a DS record indicated in the <secDNS:rem> element is not associated with the domain name.

- Code **2308** (**Data management policy violation**) Reason **10006** (**DNSSEC: too many dsData items**):
  - If the number of DS records, resulting from the modification operation, is more than 2 and the domain is in inactive/dnsHold status, more than 4 and the domain is in pendingUpdate status.

5.4 EPP Domain Transfer

The introduction of DNSSEC does not imply any change to the formats of the *EPP Domain Transfer* request and response.

No restrictions are applied to transfers between “DNSSEC accredited” Registrars and “non DNSSEC accredited” Registrars.

The *EPP Domain Transfer* operation does not alter the DNS configuration: if the new Registrar wishes to change it, a new DNS configuration (with or without DNSSEC extension) can be submitted through an *EPP Update Domain* operation.

5.5 EPP Domain Delete

The introduction of DNSSEC does not imply any change to the formats of *EPP Domain Delete* response and request.

5.6 EPP Domain Info

In case of an *EPP Domain Info* request for a "signed" domain name, the request involves two distinct XML formats depending on whether the domain DNS configuration is in the process of being validated or has already been validated.

The introduction of DNSSEC has involved the introduction of the element <**extsecDNS:infDsOrKeyToValidateData**> (described in the namespace extsecDNS-1.0), which shows, for a given domain name, the configuration of the DS record that are in the process of validation by the DNS check service of the Registro.it.

An *EPP Domain Info* response of a "signed" domain name that has been registered but not validated by the DNS check service, and which therefore is in inactive/dnsHold status, has the following XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extsecDNS="http://www.nic.it/ITNIC-EPP/extsecDNS-1.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
    <response>
        <result code="1000">
            <msg lang="en">Command completed successfully</msg>
        </result>
        <resData>
            <domain:infData>
                <domain:name>esempio.it</domain:name>
                <domain:roid>ITNIC-306194</domain:roid>
                <domain:status s="inactive" lang="en"/>
                <domain:registrant>MM001</domain:registrant>
                <domain:contact type="admin">MM001</domain:contact>
                <domain:contact type="tech">MB001</domain:contact>
                <domain:clID>DEMO-REG</domain:clID>
                <domain:crID>DEMO-REG</domain:crID>
                <domain:crDate>2016-06-29T08:26:44.000+02:00</domain:crDate>
                <domain:exDate>2017-06-29T23:59:59.000+02:00</domain:exDate>
                <domain:authInfo>
                    <domain:pw>22fooBAR</domain:pw>
                </domain:authInfo>
            </domain:infData>
        </resData>
        <extension>
            <extdom:infData>
                <extdom:ownStatus s="dnsHold" lang="en"/>
            </extdom:infData>
            <extdom:infNsToValidateData>
                <extdom:nsToValidate>
                    <domain:hostAttr>
                        <domain:hostName>m.dns.it</domain:hostName>
                    </domain:hostAttr>
```

```
                    <domain:hostAttr>
                        <domain:hostName>j.dns.it</domain:hostName>
                    </domain:hostAttr>
                </extdom:nsToValidate>
            </extdom:infNsToValidateData>
            <extsecDNS:infDsOrKeyToValidateData>
                <extsecDNS:dsOrKeysToValidate>
                    <secDNS:dsData>
                        <secDNS:keyTag>12345</secDNS:keyTag>
                        <secDNS:alg>3</secDNS:alg>
                        <secDNS:digestType>1</secDNS:digestType>
                        <secDNS:digest>
                        4347D0F8BA661234A8EADC005E2E1D1B646C9682
                        </secDNS:digest>
                    </secDNS:dsData>
                </extsecDNS:dsOrKeysToValidate>
            </extsecDNS:infDsOrKeyToValidateData>
        </extension>
        <trID>
            <svTRID>9141b61b-5272-4d63-90b1-7cb2348f5b40</svTRID>
        </trID>
    </response>
</epp>
```

If the DNS validation is successful (both authoritative name servers and DS records), the domain name passes into ok status and the EPP Domain Info response, in this case, takes the following XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extsecDNS="http://www.nic.it/ITNIC-EPP/extsecDNS-1.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
    <response>
        <result code="1000">
            <msg lang="en">Command completed successfully</msg>
        </result>
        <resData>
            <domain:infData>
                <domain:name>esenpio.it</domain:name>
                <domain:roid>ITNIC-306194</domain:roid>
                <domain:status s="ok" lang="en"/>
                <domain:registrant>MM001</domain:registrant>
                <domain:contact type="admin">MM001</domain:contact>
                <domain:contact type="tech">MB001</domain:contact>
                <domain:ns>
                    <domain:hostAttr>
                        <domain:hostName>m.dns.it</domain:hostName>
                    </domain:hostAttr>
                    <domain:hostAttr>
                        <domain:hostName>j.dns.it</domain:hostName>
                    </domain:hostAttr>
```

```
                </domain:ns>
                <domain:clID>DEMO-REG</domain:clID>
                <domain:crID>DEMO-REG</domain:crID>
                <domain:crDate>2016-06-29T08:26:44.000+02:00</domain:crDate>
                <domain:upID>DEMO-REG</domain:upID>
                <domain:upDate>2016-06-29T08:26:45.000+02:00</domain:upDate>
                <domain:exDate>2017-06-29T23:59:59.000+02:00</domain:exDate>
                <domain:authInfo>
                    <domain:pw>22fooBAR</domain:pw>
                </domain:authInfo>
            </domain:infData>
        </resData>
        <extension>
            <secDNS:infData>
                <secDNS:dsData>
                    <secDNS:keyTag>12345</secDNS:keyTag>
                    <secDNS:alg>3</secDNS:alg>
                    <secDNS:digestType>1</secDNS:digestType>
                    <secDNS:digest>
                    4347D0F8BA661234A8EADC005E2E1D1B646C9682
                    </secDNS:digest>
                </secDNS:dsData>
            </secDNS:infData>
        </extension>
        <trID>
            <svTRID>615ec859-f80d-41f2-b55f-0d7108b91cb6</svTRID>
        </trID>
    </response>
</epp>
```

If a "signed" domain name is subject to an *EPP Domain Update* operation in order to change the authoritative name servers and/or DS records, as in the pendingUpdate status a successfully validated DNS configuration already exists, the *EPP Domain Info* response can contain the <**domain:ns**> and <**extdom:infNsToValidateData**> elements (if name server change is requested) and <**secDNS:infData**> and <**extsecDNS:infDsOrKeyToValidateData**> elements (if DS records change is requested), at the same time.

The following example shows the result of an EPP Domain Info on a domain for which authoritative name servers and DS records update was requested:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extsecDNS="http://www.nic.it/ITNIC-EPP/extsecDNS-1.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
    <response>
        <result code="1000">
            <msg lang="en">Command completed successfully</msg>
        </result>
        <resData>
            <domain:infData>
```

```
        <domain:name>esempio.it</domain:name>
        <domain:roid>ITNIC-306194</domain:roid>
        <domain:status s="pendingUpdate" lang="en"/>
        <domain:registrant>MM001</domain:registrant>
        <domain:contact type="admin">MM001</domain:contact>
        <domain:contact type="tech">MB001</domain:contact>
        <domain:ns>
            <domain:hostAttr>
                <domain:hostName>m.dns.it</domain:hostName>
            </domain:hostAttr>
            <domain:hostAttr>
                <domain:hostName>j.dns.it</domain:hostName>
            </domain:hostAttr>
        </domain:ns>
        <domain:clID>DEMO-REG</domain:clID>
        <domain:crID>DEMO-REG</domain:crID>
        <domain:crDate>2016-06-29T08:26:44.000+02:00</domain:crDate>
        <domain:upID>DEMO-REG</domain:upID>
        <domain:upDate>2016-06-29T08:26:45.000+02:00</domain:upDate>
        <domain:exDate>2017-06-29T23:59:59.000+02:00</domain:exDate>
        <domain:authInfo>
            <domain:pw>22fooBAR</domain:pw>
        </domain:authInfo>
    </domain:infData>
</resData>
<extension>
    <extdom:infNsToValidateData>
        <extdom:nsToValidate>
            <domain:hostAttr>
                <domain:hostName>n.dns.it</domain:hostName>
            </domain:hostAttr>
            <domain:hostAttr>
                <domain:hostName>k.dns.it</domain:hostName>
            </domain:hostAttr>
        </extdom:nsToValidate>
    </extdom:infNsToValidateData>
    <secDNS:infData>
        <secDNS:dsData>
            <secDNS:keyTag>12345</secDNS:keyTag>
            <secDNS:alg>3</secDNS:alg>
            <secDNS:digestType>1</secDNS:digestType>
            <secDNS:digest>
           4347D0F8BA661234A8EADC005E2E1D1B646C9682
            </secDNS:digest>
        </secDNS:dsData>
    </secDNS:infData>
    <extsecDNS:infDsOrKeyToValidateData>
        <extsecDNS:dsOrKeysToValidate>
            <secDNS:dsData>
                <secDNS:keyTag>45063</secDNS:keyTag>
                <secDNS:alg>3</secDNS:alg>
                <secDNS:digestType>2</secDNS:digestType>
                <secDNS:digest>
  E9B696C3AC8644735BF0A6409BE6D77BBFB4142D667E0EB0D41AD75BCC9D0D43
                </secDNS:digest>
            </secDNS:dsData>
        </extsecDNS:dsOrKeysToValidate>
    </extsecDNS:infDsOrKeyToValidateData>
```

```
        </extension>
        <trID>
            <svTRID>1e53552c-585a-4a48-8c45-4b2068ea057d</svTRID>
        </trID>
    </response>
</epp>
```

The following example shows, however, the result of an EPP Domain info on a domain for which removal of all DS records has been requested:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp
xmlns="urn:ietf:params:xml:ns:epp-1.0"
xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xmlns:contact="urn:ietf:params:xml:ns:contact-1.0"
xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1"
xmlns:extcon="http://www.nic.it/ITNIC-EPP/extcon-1.0"
xmlns:extdom="http://www.nic.it/ITNIC-EPP/extdom-2.0"
xmlns:extsecDNS="http://www.nic.it/ITNIC-EPP/extsecDNS-1.0"
xmlns:extepp="http://www.nic.it/ITNIC-EPP/extepp-2.0">
    <response>
        <result code="1000">
            <msg lang="en">Command completed successfully</msg>
        </result>
        <resData>
            <domain:infData>
                <domain:name>esempio.it</domain:name>
                <domain:roid>ITNIC-306194</domain:roid>
                <domain:status s="pendingUpdate" lang="en"/>
                <domain:registrant>MM001</domain:registrant>
                <domain:contact type="admin">MM001</domain:contact>
                <domain:contact type="tech">MB001</domain:contact>
                <domain:ns>
                    <domain:hostAttr>
                        <domain:hostName>m.dns.it</domain:hostName>
                    </domain:hostAttr>
                    <domain:hostAttr>
                        <domain:hostName>j.dns.it</domain:hostName>
                    </domain:hostAttr>
                </domain:ns>
                <domain:clID>DEMO-REG</domain:clID>
                <domain:crID>DEMO-REG</domain:crID>
                <domain:crDate>2016-06-29T08:26:44.000+02:00</domain:crDate>
                <domain:upID>DEMO-REG</domain:upID>
                <domain:upDate>2016-06-29T08:26:45.000+02:00</domain:upDate>
                <domain:exDate>2017-06-29T23:59:59.000+02:00</domain:exDate>
                <domain:authInfo>
                    <domain:pw>22fooBAR</domain:pw>
                </domain:authInfo>
            </domain:infData>
        </resData>
        <extension>
            <secDNS:infData>
                <secDNS:dsData>
                    <secDNS:keyTag>12345</secDNS:keyTag>
                    <secDNS:alg>3</secDNS:alg>
```

```
                    <secDNS:digestType>1</secDNS:digestType>
                    <secDNS:digest>
                     4347D0F8BA661234A8EADC005E2E1D1B646C9682
                    </secDNS:digest>
                </secDNS:dsData>
            </secDNS:infData>
            <extsecDNS:infDsOrKeyToValidateData>
                <extsecDNS:remAll/>
            </extsecDNS:infDsOrKeyToValidateData>
        </extension>
        <trID>
            <svTRID>3774a765-5418-4f43-a999-5d2f337560c0</svTRID>
        </trID>
    </response>
</epp>
```

5.7 EPP Poll

For the EPP Poll (op="req") request, the XML format of the messages, concerning the DNS validation which foresees also the validation of DS records, has been modified.

In conclusion, the two following message formats have been modified:

- **DNS check ended unsuccessfully**, DNS ended with failure verification message;
- **DNS check ended successfully with warning**, DNS successfully completed verification message with the presence of warnings.

The XML format of these messages has been modified by adding, in the <extension> section, the <**extsecDNS:secDnsErrorMsgData**> element.

6. Validation of DNS configuration

The introduction of DNSSEC has obvious implications on the validation procedure of DNS configuration. This, in fact, in case of signed domain names, foresees further checks in addition to those already existing.

In particular, it verifies that:

- the algorithm that appears in the DS record must be the same as that which appears in the DNSKEY record 257;
- the digests of the DS records indicated in the registration/modification of a domain name are congruent with the content of DNSKEY 257 record;
    - the above control is carried out for all declared authoritative name servers for the zone concerned;
- the digest of the SOA record corresponds with that indicated in the RRSIG SOA record;
    - the above control is carried out for all declared authoritative name servers for the zone concerned;
- the digest of the NS record corresponds with that indicated in the record NS RRSIG;
    - the above control is carried out for all declared authoritative name servers for the zone concerned;
- the digest of the DNSKEY record corresponds with that indicated in the RRSIG DNSKEY record;

    - the above control is carried out for all declared authoritative name servers for the zone concerned;
- the signatures of RRSIG records are not expired or are not in the future.

7. References

1. Mockapetris P., "Domain names - concepts and facilities", RFC 1034, November 1987.
2. Mockapetris P., "Domain names - implementation and specification", RFC 1035, November 1987.
3. Eastlake D., Kaufman C. “Domain Name System Security Extensions”, RFC 2065, January 1997.
4. Arends R., Austein R., Larson M., Massey D., Rose S.: "DNS Security Introduction and Requirements", RFC 4033, March 2005.
5. Arends R., Austein R., Larson M., Massey D., Rose S.: "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.
6. Arends R., Austein R., Larson M., Massey D., Rose S.: "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.
7. “Domain Name System Security (DNSSEC) Algorithm Numbers”, http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml, March 2014.
8. “Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms”, http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml, April 2012.
9. Hollenbeck S.: "Extensible Provisioning Protocol (EPP)", RFC 5730, August 2009.
10. Hollenbeck S.: "Extensible Provisioning Protocol (EPP) Domain Name Mapping", RFC 5731, August 2009.
11. Gould J., Hollenbeck S.: "Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)", RFC 5910, May 2010.