DNSSEC nel ccTLD .it
Principali scelte implementative

Ultimo aggiornamento:
10 ottobre 2016

1. Introduzione

Il protocollo DNS (Domain Name System) definisce le specifiche per fornire un servizio di risoluzione dei nomi che non ha forme di autenticazione né implementa meccanismi per garantire l'integrità dei dati. Per superare questo limite è stato definito da IETF un protocollo noto come Domain Name System SECurity extensions (DNSSEC). DNSSEC utilizza meccanismi di crittografia a chiavi pubbliche/private per assicurare che l'informazione provenga dalla sorgente autorevole e non sia stata modificata durante il suo trasporto sulla rete.

DNSSEC consente:

- ai DNS server di firmare i propri resource record (RR) con una chiave privata;
- ai DNS resolver di verificare le informazioni tramite la relativa chiave pubblica.

Le chiavi pubbliche sono memorizzate nella zona "padre" di quella firmata digitalmente.

Per facilitare la verifica delle firme, DNSSEC ha definito alcuni nuovi RR:

- RRSIG: contenente una firma crittografica per un insieme di RR dello stesso tipo (RRset);
- DNSKEY: contenente una chiave pubblica.

DNSSEC inoltre ha introdotto il record Delegation Signer (DS) per implementare la "chain-of-trust" fra una zona padre e una zona figlia. Un gestore di zona genera un "digest" della chiave pubblica (record DNSKEY) associata al dominio firmato digitalmente e lo trasmette al gestore della zona padre che lo associerà alla delega di quel nome a dominio tramite un record DS.

2. Record DS

In generale le modalità più utilizzate per ottenere il record DS da associare ad un nome a dominio e creare la "chain-of-trust" nella zona di un TLD sono:

1. il Registrar (o colui che gestisce il nameserver autoritativo della zona che si intende firmare) lo genera e lo trasmette (via EPP, via portale Web, ecc.) al Registro che gestisce il TLD;
2. il Registrar (o colui che gestisce il nameserver autoritativo della zona che si intende firmare) trasmette al Registro del TLD (via EPP, via portale Web, ecc.) la chiave pubblica associata alla zona e, conseguentemente, la generazione del record DS è demandata al Registro del TLD.

Nel ccTLD.it è stata implementata la prima soluzione, cioè è il Registrar che deve trasmettere al Registro.it il record DS associato ad un nome a dominio. Anche nel caso in cui un nome a dominio abbia il servizio DNS gestito da un soggetto diverso dal Registrar, la trasmissione del record DS è comunque a carico del Registrar del nome a dominio e questa deve avvenire esclusivamente attraverso il protocollo EPP.

In pratica, il Registrar deve comunicare via EPP al Registro.it i seguenti quattro campi, che compongono il record DS associato al nome a dominio che è stato firmato:

- ***keytag***: questo valore è automaticamente calcolato quando il record DS è generato e dipende strettamente dalle informazioni relative alla chiave pubblica;
- ***algorithm***: i valori supportati dal Registro.it sono i seguenti:
  - **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***: i valori supportati dal Registro.it sono i seguenti:
  - **1** (SHA-1)
  - **2** (SHA-256)
  - **3** **(**GOST R 34.11-94)
  - **4** **(**SHA-384)
- ***digest***: è l'hash generato a partire dalla chiave pubblica in accordo ai valori dell'*algorithm* e del *digest type*.

3. Registrar e DNSSEC

Nel .it, l'adozione del DNSSEC da parte dei Registrar non è obbligatoria e vincolante. I Registrar interessati a fornire questo nuovo servizio ai propri clienti, lo potranno fare a seguito del superamento di un apposito "Test di accreditamento tecnico DNSSEC", le cui specifiche saranno definite in un apposito documento.

I Registrar che, al contrario, non intenderanno avvalersi di questo nuovo servizio, potranno continuare ad operare come allo stato attuale.

I Registrar saranno pertanto suddivisi in due categorie: quelli "accreditati DNSSEC" e quelli "non accreditati DNSSEC". Un apposito logo identificherà i Registrar "accreditati DNSSEC" sul sito web del Registro (nella sezione http://www.nic.it/registrars/list. Anche il servizio Whois conterrà, nella sezione Registrar", un nuovo campo "DNSSEC:" con i valori "yes" o "no" a seconda che il Registrar sia accreditato DNSSEC oppure no.

Analogamente il servizio Whois conterrà, per i domini, il campo "Signed:" con i valori "yes" o "no" a seconda che il dominio sia stato firmato o meno.

Anche l'ambiente di test pubblico prevederà la possibilità di registrare e gestire nomi a dominio firmati digitalmente. Per essere abilitati a testare le funzionalità del DNSSEC in tale ambiente, il Registrar dovrà inviare esplicita richiesta a hostmaster@nic.it. In seguito a ciò, diventeranno "accreditati DNSSEC" entrambi i Registrar di test associati al soggetto richiedente.

Un Registrar potrà effettuare il test di accreditamento tecnico DNSSEC se e solo se è un Registrar accreditato nel .it ed è nello stato "attivo".

Nel ccTLD.it la trasmissione dei record DS associati alle zone firmate digitalmente, per la loro pubblicazione nel file di zona del .it, è a carico dei Registrar "accreditati DNSSEC" e questa deve avvenire, esclusivamente, attraverso l'utilizzo del protocollo EPP.

4. EPP e DNSSEC

Vediamo adesso quali sono le implicazioni dell'introduzione del DNSSEC sulle richieste che un Registrar "accreditato DNSSEC" deve inviare al server EPP del Registro.it tramite il suo client.

L'estensione standard **secDNS-1.1** al protocollo EPP descrive 2 diverse modalità per consentire ad un Registrar la trasmissione, al Registro, delle informazioni relative ai record DS:

1. La prima modalità, chiamata "DS Data Interface", è quella che prevede la trasmissione, via EPP, delle informazioni dei record DS al Registro. Tale trasmissione avviene in concomitanza con la registrazione di un dominio "firmato" (tramite l'operazione EPP Domain Create) o di una successiva modifica del record DS ad esso associato (aggiunta, rimozione o sostituzione tramite un'operazione di EPP Domain Update). Il server EPP del Registro riporterà tali informazioni nella risposta alla richiesta di EPP Domain Info.

2. La seconda modalità, chiamata invece "Key Data Interface", è del tutto analoga alla precedente con la differenza che il Registrar, invece di fornire le informazioni relative al record DS, deve fornire i dati relativi alla chiave pubblica associata al dominio firmato (flags, protocol, alg, pubKey).

Opzionalmente, il protocollo prevede che nella "DS Data Interface" possano essere fornite, insieme alle informazioni del record DS, anche quelle inerenti alla "Key Data Interface". Ciò per agevolare un eventuale controllo di consistenza, da parte del Registro, tra la chiave pubblica e il record DS associato al nome a dominio.

È obbligatorio che il server EPP supporti un'unica modalità di trasmissione delle informazioni nell'ambito di una singola richiesta o risposta.

Nel ccTLD.it è stata scelta la modalità "DS Data Interface" con la trasmissione, da parte del Registrar al Registro, delle sole informazioni relative ai record DS.

Vediamo ora quali sono le principali operazioni EPP che sono interessate dall'introduzione del DNSSEC nel .it, nel caso in cui un Registrar abbia superato il test di accreditamento tecnico DNSSEC e sia, di conseguenza, un Registrar "accreditato DNSSEC".

4.1 EPP Login

Un Registrar "accreditato DNSSEC" deve sempre riportare nella richiesta di *EPP Login* anche i due namespace:

- **urn:ietf:params:xml:ns:secDNS-1.1**, riguardante le estensioni standard introdotte al protocollo EPP;
- **http://www.nic.it/ITNIC-EPP/extsecDNS-1.0**, riguardante le estensioni introdotte dal Registro.it.

Una richiesta di *EPP Login* avrà quindi il seguente formato XML:

```
<?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>
```

Se un Registrar "accreditato DNSSEC" non inserisce nella richiesta di *EPP Login* i due namespace sopra indicati, ottiene il seguente messaggio di errore:

- Codice **2003** (**Required parameter missing**) - Reason **4012** (**Extension URI missing**), con il riferimento al namespace mancante.

Se invece un Registrar "non accreditato DNSSEC" inserisce nella richiesta di *EPP Login* (o in qualsiasi altra richiesta EPP) uno o entrambi i namespace sopra indicati, ottiene il seguente messaggio di errore:

- Codice **2306** (**Parameter value policy error**) Reason **10001** (**DNSSEC: registrar is not DNSSEC accredited**), con il riferimento al namespace errato.

Le risposte restituite dal server EPP avranno un'intestazione diversa a seconda che il Registrar sia "accreditato DNSSEC" o "non accreditato DNSSEC":

- **Intestazione della risposta EPP per un Registrar "accreditato DNSSEC"**, in seguito ad un'operazione di *EPP Login* (la stessa intestazione vale per qualsiasi operazione effettuata dal 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">
```

- **Intestazione della risposta EPP per un Registrar "non accreditato DNSSEC"**, in seguito ad un'operazione di *EPP Login* (la stessa intestazione vale per qualsiasi operazione effettuata dal 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">
```

4.2 EPP Domain Create

Il comando *EPP Domain Create* è stato esteso con l'aggiunta, nella sezione **<extension>**, dell'elemento **<secDNS:create>** (dove secDNS è il prefisso che identifica il riferimento al namespace secDNS-1.1), che può contenere fino ad un massimo di 2 elementi **<secDNS:dsData>** corrispondenti ai record DS.

Pertanto una richiesta EPP Domain Create per un dominio .it, con l'estensione DNSSEC che faccia uso della DS Data Interface, assumerà il seguente formato XML:

```
<?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>49FD46E6C4B45C55D4AC</secDNS:digest>
    </secDNS:dsData>
```

```
    </secDNS:create>
  </extension>
  <clTRID>ABC-12345</clTRID>
</command>
</epp>
```

Gli eventuali errori che un Registrar "accreditato DNSSEC" può ottenere in seguito all'invio di una richiesta *EPP Domain Create* contenente l'estensione <secDNS:create> sono i seguenti:

- Codice **2102** (**Unimplemented option**) Reason **10002** (**DNSSEC: unsupported maxSigLife element**):
  - nel caso in cui all'interno dell'elemento <secDNS:create> sia stato riportato l'elemento <secDNS:maxSigLife>.

- Codice **2102** (**Unimplemented option**) Reason **10003** (**DNSSEC: unsupported keyData element**):
  - nel caso in cui all'interno dell'elemento <secDNS:create> sia stato riportato un elemento <secDNS:keyData> al posto o all'interno di un elemento <secDNS:dsData>.

- Codice **2308** (**Data management policy violation**) Reason **10006** (**DNSSEC: too many dsData items**):
  - nel caso in cui all'interno dell'elemento <secDNS:create> siano stati riportati un numero di elementi <secDNS:dsData> superiore a 2.

- Codice **2001** (**Command syntax error**) Reason **4003** (**Syntax error**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *keyTag* non compreso nell'intervallo 0-65535;
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digestType* non compreso nell'intervallo 0-255;
  - Nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *alg* non compreso nell'intervallo 0-255.

- Codice **2306** (**Parameter value policy error**) Reason **10007** (**DNSSEC: invalid digestType value**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digestType* non supportato o invalido.

- Codice **2306** (**Parameter value policy error**) Reason **10008** (**DNSSEC: invalid alg value**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *alg* non supportato o invalido.

- Codice **2306** (**Parameter value policy error**) Reason **10009** (**DNSSEC: invalid digest value**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digest* la cui lunghezza non sia compatibile con il *digest type* scelto.

- Codice **2306** (**Parameter value policy error**) Reason **10010** (**DNSSEC: duplicate dsData**):
  - nel caso in cui siano stati riportati 2 elementi <secDNS:dsData> contenenti gli stessi valori per i 4 campi previsti.

4.3 EPP Domain Update

Il comando *EPP Domain Update* è stato esteso riportando, nella sezione **<extension>**, l'elemento **<secDNS:update>**.

Pertanto, una richiesta *EPP Domain Update* per un dominio .it, con l'estensione DNSSEC che faccia uso della DS Data Interface, per il quale sia stata richiesta la sostituzione del DS Record correntemente associato con un altro DS Record, assumerà il seguente formato XML (nell'esempio che segue viene richiesta la sostituzione del record DS corrente con uno nuovo):

```
<?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>49FD46E6C4B45C55D4AC</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>
```

Nel caso in cui il Registrar intenda richiedere la rimozione di tutti record DS associati al dominio, può farlo tramite un'operazione di *EPP Domain Update*, utilizzando l'elemento **<secDNS:all>** nella sezione **<secDNS:rem>**.

Esempio:

```
<?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>
```

Gli eventuali errori che un Registrar "accreditato DNSSEC" può ottenere in seguito all'invio di una richiesta *EPP Domain Update* contenente l'estensione <secDNS:update> sono i seguenti:

- Codice **2102** (**Unimplemented option**) Reason **10002** (**DNSSEC: unsupported maxSigLife element**):
  - nel caso in cui all'interno dell'elemento <secDNS:update> sia stato riportato l'elemento <secDNS:maxSigLife>.

- Codice **2102** (**Unimplemented option**) Reason **10003** (**DNSSEC: unsupported keyData element**):
  - nel caso in cui all'interno dell'elemento <secDNS:update> sia stato riportato un elemento <secDNS:keyData> al posto o all'interno di un elemento <secDNS:dsData>.

- Codice **2102** (**Unimplemented option**) Reason **10004** (**DNSSEC: unsupported urgent attribute**):
  - nel caso in cui all'interno dell'elemento <secDNS:update> sia stato riportato l'attributo *urgent*.

- Codice **2306** (**Parameter value policy error**) Reason **10005** (**DNSSEC: no dsData to rem or add**)
  - nel caso in cui all'interno dell'elemento <secDNS:update> non sia stato riportato né l'elemento <secDNS:add>, né l'elemento <secDNS:rem>, oppure sia stato riportato l'elemento <secDNS:rem> che però non contiene né singoli elementi <secDNS:dsData> né l'elemento <secDNS:all>.

- Codice **2308** (**Data management policy violation**) Reason **10006** (**DNSSEC: too many dsData items**):
  - nel caso in cui il numero dei record DS, risultante dall'operazione di modifica, sia maggiore di 2 se il dominio è nello stato di inactive/dnsHold e maggiore di 4 se il dominio è nello stato di pendingUpdate.

- Codice **2001** (**Command syntax error**) Reason **4003** (**Syntax error**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *keyTag* non compreso nell'intervallo 0-65535;
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digestType* non compreso nell'intervallo 0-255;
  - Nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *alg* non compreso nell'intervallo 0-255.

- Codice **2306** (**Parameter value policy error**) Reason **10007** (**DNSSEC: invalid digestType value**):

- nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digestType* non supportato o invalido.

- Codice **2306** (**Parameter value policy error**) Reason **10008** (**DNSSEC: invalid alg value**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *alg* non supportato o invalido.

- Codice **2306** (**Parameter value policy error**) Reason **10009** (**DNSSEC: invalid digest value**):
  - nel caso in cui un elemento <secDNS:dsData> contenga un valore del campo *digest* la cui lunghezza non sia compatibile con il *digest type* scelto.

- Codice **2306** (**Parameter value policy error**) Reason **10010** (**DNSSEC: duplicate dsData**):
  - nel caso in cui siano stati riportati 2 elementi <secDNS:dsData> contenenti gli stessi valori per i 4 campi previsti.

- Codice **2306** (**Parameter value policy error**) Reason **10011** (**DNSSEC: dsData to add is already associated with the domain**):
  - nel caso in cui un record DS riportato nell'elemento <secDNS:add> sia già associato al dominio.

- Codice **2306** (**Parameter value policy error**) Reason **10012** (**DNSSEC: dsData to remove is not associated with the domain**):
  - nel caso in cui un record DS riportato nell'elemento <secDNS:rem> non sia associato al dominio.

4.4 EPP Domain Transfer

L'introduzione del DNSSEC non comporta alcuna modifica ai formati della richiesta *EPP Domain Transfer* e della sua risposta.

Non vi è alcun vincolo sui trasferimenti fra Registrar "accreditati DNSSEC" e Registrar "non accreditati DNSSEC".

L'operazione di *EPP Domain Transfer* non consente di alterare la configurazione DNS: il nuovo Registrar, se intende modificarla, può sottomettere una nuova configurazione DNS (con o senza estensione DNSSEC) tramite un'operazione di *EPP Domain Update*.

4.5 EPP Domain Delete

L'introduzione del DNSSEC non comporta alcuna modifica ai formati della richiesta *EPP Domain Delete* e della sua risposta.

4.6 EPP Domain Info

Nel caso di richiesta *EPP Domain Info* su un dominio "firmato", la richiesta prevede due formati XML distinti a seconda che la configurazione DNS del dominio sia sempre in fase di validazione oppure sia già stata validata.

L'introduzione del DNSSEC ha comportato l'introduzione dell'elemento **<extsecDNS:infDsOrKeyToValidateData>** (descritto nel namespace extsecDNS-1.0), che riporta, per un determinato dominio, la configurazione dei record DS che sono in validazione da parte del sistema di controllo del DNS del Registro.it.

Una risposta *EPP Domain Info* di un dominio "firmato" che è stato registrato, ma non ancora validato dal sistema di controllo del DNS e che si trova pertanto nello stato inactive/dnsHold, ha il seguente formato XML:

```
<?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>49FD46E6C4B45C55D4AC</secDNS:digest>
                    </secDNS:dsData>
                </extsecDNS:dsOrKeysToValidate>
            </extsecDNS:infDsOrKeyToValidateData>
        </extension>
        <trID>
            <svTRID>9141b61b-5272-4d63-90b1-7cb2348f5b40</svTRID>
        </trID>
    </response>
</epp>
```

Se la validazione DNS ha esito positivo (sia dei nameserver autoritativi che del/i record DS), il nome a dominio passa nello stato di ok e la risposta *EPP Domain Info* in tal caso assume il seguente formato XML:

```
<?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>49FD46E6C4B45C55D4AC</secDNS:digest>
                </secDNS:dsData>
            </secDNS:infData>
        </extension>
        <trID>
            <svTRID>615ec859-f80d-41f2-b55f-0d7108b91cb6</svTRID>
        </trID>
    </response>
</epp>
```

Nel caso in cui il nome a dominio "firmato" sia soggetto ad un'operazione di *EPP Domain Update* per variare i nameserver autoritativi e/o i record DS, dal momento che nello stato di pendingUpdate esiste già una configurazione DNS validata con successo, la risposta *EPP Domain Info*, in questo caso, potrà contenere contemporaneamente gli elementi <**domain:ns**> e <**extdom:infNsToValidateData**> (nel caso in cui sia stata richiesta la modifica dei nameserver) e <**secDNS:infData**> e <**extsecDNS:infDsOrKeyToValidateData**> (nel caso in cui sia stata richiesta la modifica dei record DS).

Il seguente esempio mostra il risultato di un'operazione di *EPP Domain Info* su un dominio per il quale è stata richiesta sia la modifica dei nameserver autoritativi che dei record DS:

```
<?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="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>49FD46E6C4B45C55D4AC</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>
```

Il seguente esempio mostra, invece, il risultato di un'operazione di *EPP Domain Info* su un dominio per il quale è stata richiesta la sola rimozione di tutti i record DS:

```
<?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="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>49FD46E6C4B45C55D4AC</secDNS:digest>
                </secDNS:dsData>
            </secDNS:infData>
            <extsecDNS:infDsOrKeyToValidateData>
                <extsecDNS:remAll/>
            </extsecDNS:infDsOrKeyToValidateData>
        </extension>
        <trID>
            <svTRID>3774a765-5418-4f43-a999-5d2f337560c0</svTRID>
        </trID>
    </response>
```

```
</epp>
```

4.7 EPP Poll

Nel caso di richiesta di EPP Poll (op="req"), è stato modificato il formato XML dei messaggi riguardanti l'esito di un controllo DNS che preveda, oltre a quella dei nameserver, anche la validazione dei record DS.

In sostanza sono stati modificati i formati dei due seguenti messaggi:

- **DNS check ended unsuccessfully**, messaggio di verifica del DNS terminato con fallimento;
- **DNS check ended successfully with warning**, messaggio di verifica del DNS terminato con successo e con presenza di warning.

Il formato XML dei suddetti messaggi è stato modificato aggiungendo, nella sezione <**extension**>, l'elemento <**extsecDNS:secDnsErrorMsgData**>.

5. Validazione della configurazione DNS

L'introduzione del DNSSEC ha naturalmente delle implicazioni sulla procedura di validazione della configurazione DNS. Questa, infatti, nel caso di nome a dominio firmato, provvede ad effettuare ulteriori controlli rispetto a quelli già esistenti.

In particolare verifica che:

- l'algoritmo che compare nel record DS deve essere uguale a quello che compare nel record DNSKEY 257;
- il/i digest del/i record DS indicati nella fase di registrazione/modifica di un nome a dominio siano congruenti con il contenuto del/i record DNSKEY 257;
    - Il suddetto controllo è effettuato per tutti i nameserver dichiarati autoritativi per la zona presa in considerazione;
- il digest del record SOA corrisponda con quello indicato nel record RRSIG SOA;
    - Il suddetto controllo è effettuato per tutti i nameserver dichiarati autoritativi per la zona presa in considerazione;
- il digest dei record NS corrisponda con quello indicato nei record RRSIG NS;
    - Il suddetto controllo è effettuato per tutti i nameserver dichiarati autoritativi per la zona presa in considerazione;
- il digest dei record DNSKEY corrisponda con quello indicato nei record RRSIG DNSKEY;
    - Il suddetto controllo è effettuato per tutti i nameserver dichiarati autoritativi per la zona presa in considerazione;
- le firme dei record RRSIG non siano scadute o nel futuro.

6. Riferimenti

1. Mockapetris P., "Domain names - concepts and facilities", RFC 1034, Novembre 1987.
2. Mockapetris P., "Domain names - implementation and specification", RFC 1035, Novembre 1987.
3. Eastlake D., Kaufman C. "Domain Name System Security Extensions", RFC 2065, Gennaio 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, Marzo 2005.
7. “Domain Name System Security (DNSSEC) Algorithm Numbers”, http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml, Marzo 2014.
8. “Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms”, http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml, Aprile 2012.
9. Gould J., Hollenbeck S.: "Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)", RFC 5910, Maggio 2010.