Sommario

1. Premessa

Nel mese di dicembre 2016 è stata avviata la prima fase della sperimentazione DNSSec nel .it, che prevedeva il test, da parte dei Registrar, del nuovo server EPP del Registro.it, dotato di tutte le funzionalità necessarie alla registrazione/modifica di nomi a dominio firmati digitalmente.
Il presente documento fornisce invece ai Registrar le indicazioni e specifiche tecniche per poter partecipare alla seconda fase della sperimentazione DNSSec nel .it. Tale fase prevede il test completo della nuova architettura software che è stata sviluppata dal Registro.it e include anche la fase di validazione DNSSec dei nameserver configurati dai Registrar partecipanti alla sperimentazione.

Nel documento si fa riferimento ad una piattaforma server Ubuntu 16.04 x86_64, equipaggiata con i software Bind9.10 e SoftHSM2.

Maggiori informazioni sui due software sopra citati e sul loro utilizzo in ambiente DNSSec, sono disponibili qui:

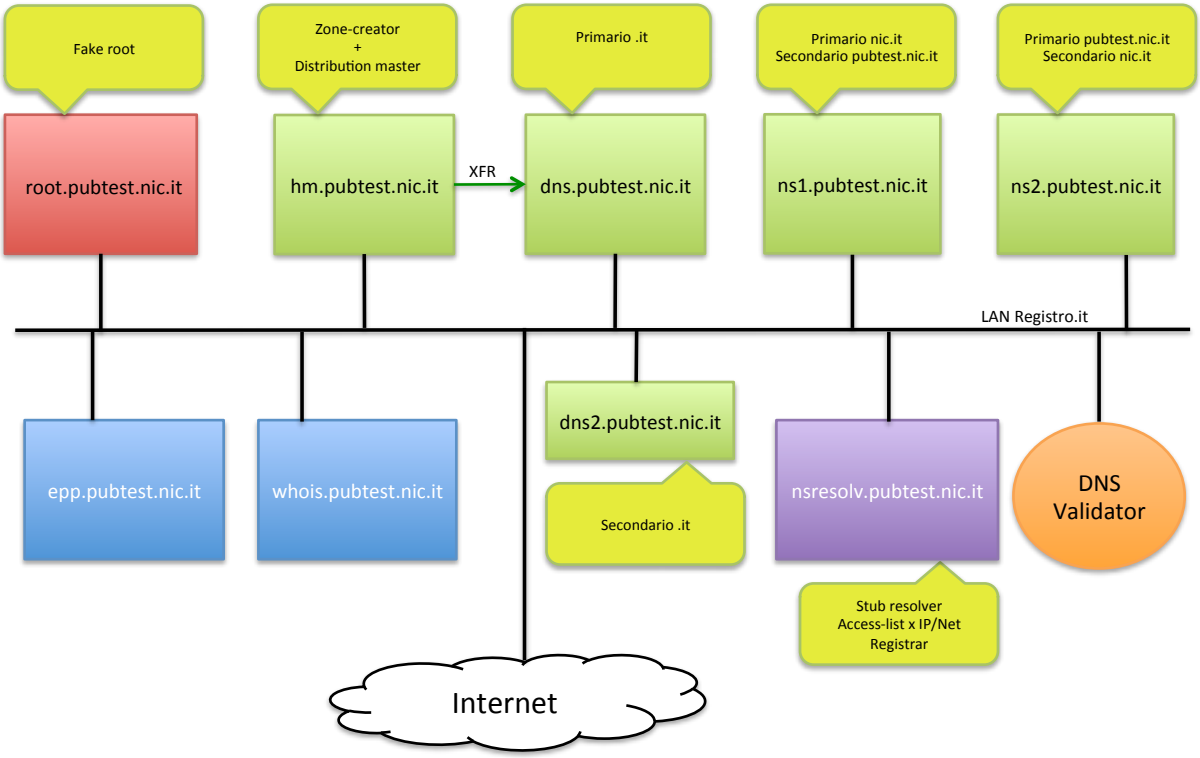
- https://www.isc.org/downloads/bind/doc/bind-9-10/
- https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf
- https://wiki.opendnssec.org/display/SoftHSMDOCS/SoftHSM+Documentation+v2

2. La piattaforma DNSSec di test

Il Registro.it, al fine di avviare la seconda fase della sperimentazione, ha opportunamente modificato la piattaforma di test (pubtest.nic.it), utilizzata dai Registrar per verificare la compatibilità dei loro client con le varie release del server EPP del Registro, integrandola con una serie di componenti necessarie per l'implementazione delle funzionalità DNSSec.

2.1. **Architettura**

Lo schema concettuale della nuova piattaforma di test e della sua architettura DNSSec è il seguente:



2.2.**Componenti**

Di seguito sono descritte le principali componenti dell'ambiente di test DNSSec del Registro.it.

È importante sottolineare che, dove non espressamente specificato, si fa riferimento sempre e comunque a configurazioni e/o servizi non in produzione, appositamente predisposti per simulare un ambiente del tutto simile a quello reale.

La piattaforma di test dispone di un "fake root nameserver" ***root.pubtest.nic.it***, equivalente a quello presente sui root nameserver ufficiali. L'unica eccezione consiste nella modifica delle deleghe del ccTLD .it che, nella fattispecie, non puntano ai veri namesever del .it, ma bensì ai due "fake nameserver", ***dns.pubtest.nic.it*** e ***dns2.pubtest.nic.it***, predisposti appositamente per la piattaforma di test. Pertanto, la zona .it della piattaforma di test è generata dai dati contenuti nel database di pubtest.nic.it, che non ha nulla a che vedere con il database ufficiale dei nomi a dominio del ccTLD .it.

Il server ***hm.pubtest.nic.it*** è l'Hidden Master della zona .it suddetta e su esso risiede il software per la generazione della zona .it a cadenza bi-oraria (analogamente all'ambiente di produzione). Quando la zona .it di test è stata generata e firmata, viene inviato un DNS NOTIFY al server ***dns.pubtest.nic.it***, il primario della zona .it di test.
La Key Signing Key (KSK) e Zone Signing Key (ZSK), utilizzate per la zona .it di test, utilizzano l'algoritmo 10, ossia RSASHA512 (analogamente a quanto avverrà in produzione).

Il server ***nsresolv.pubtest.nic.it*** è stato opportunamente configurato per funzionare come *recursive resolver* per l'ambiente pubtest.nic.it.

I server ***ns1.pubtest.nic.it*** e ***ns2.pubtest.nic.it*** sono i nameserver opportunamente predisposti per le *zone fake* **nic.it** e **pubtest.nic.it**. Le suddette zone sono state predisposte appositamente per la piattaforma di pubtest e sono firmate anch'esse con gli stessi algoritmi della zona .it di test (RSASHA512).
In particolare, ***ns1.pubtest.nic.it*** è il primario della *zona fake* **nic.it** e secondario della *zona fake* **pubtest.nic.it**, mentre ***ns2.pubtest.nic.it*** è primario della *zona fake* **pubtest.nic.it** e secondario della *zona fake* **nic.it**.

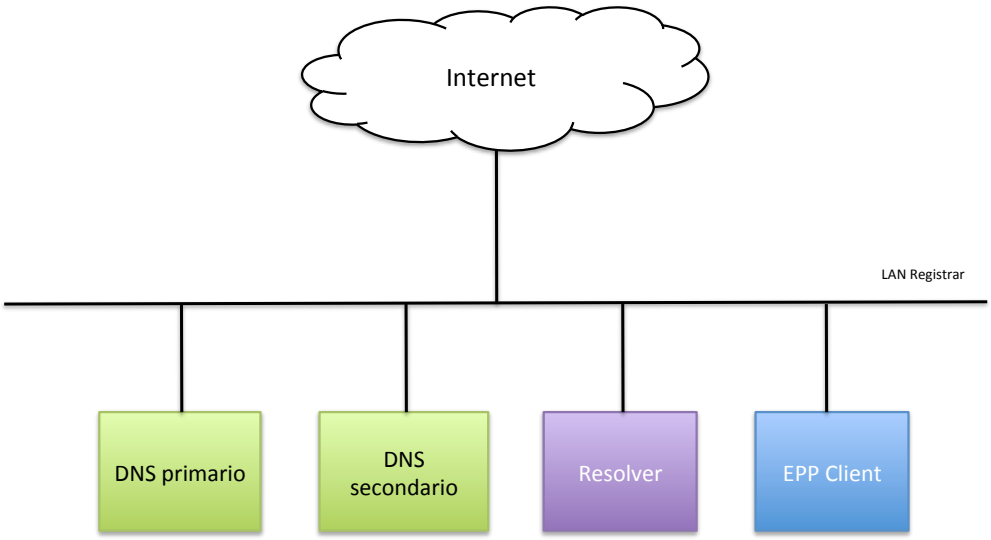
Il servizio di validazione del DNS utilizza come resolver quello della piattaforma di test (***nsresolv.pubtest.nc.it***), per effettuare le verifiche di consistenza e correttezza della configurazione dei nameserver associati ai domini sottomessi sulla piattaforma di test. La validazione DNS, oltre alle normali verifiche di correttezza delle configurazioni, effettuerà anche la validazione DNSSEC.

3. Partecipazione alla sperimentazione da parte di un Registrar

In questo paragrafo sono riportate tutte le indicazioni utili ad un Registrar, affinché possa partecipare alla seconda fase di sperimentazione del DNSSEC nel .it. In particolare, oltre all'indicazione dell'architettura della piattaforma di test che un Registrar dovrebbe implementare, sono dettagliate anche le configurazioni e i comandi che un Registrar deve eseguire al fine di registrare, sulla piattaforma di test, un dominio firmato digitalmente.

3.1. **Architettura della piattaforma di test lato Registrar**

Di seguito è riportato uno schema di come un Registrar potrebbe implementare la sua piattaforma di test al fine di partecipare alla seconda fase della sperimentazione DNSSEC:



Nel grafico sono rappresentati:

- due nameserver, uno primario e uno secondario, necessari per la configurazione DNS/DNSSEC dei domini da registrare/modificare sulla piattaforma pubtest.nic.it;
- un *recursive resolver* da utilizzare come resolver di default per interagire con l'ambiente di test del Registro.it;
- un EPP client per sottomettere le richieste a epp.pubtest.nic.it/epp-deleted.pubtest.nic.it.

N.B. Onde evitare problemi di disallineamento temporale, tutte le macchine coinvolte nel processo di firma ed erogazione del servizio devono essere correttamente sincronizzate via NTP.

3.2. **Configurazioni lato Registrar**

3.2.1. **Root zone**

Analogamente a quanto avviene per tutte le macchine appartenenti alla piattaforma di test del Registro, anche i server del Registrar, partecipanti alla sperimentazione, devono riferire il *fake root nameserver* predisposto dal Registro. Pertanto, il file della zona HINT (es: /etc/bind/db.root) deve essere opportunamente modificato per la sperimentazione e contenere solo ed esclusivamente quanto segue:

```
.                       518400     IN    NS    root.pubtest.nic.it.
root.pubtest.nic.it.    3600000    IN    A     192.12.192.239
```

Occorre, inoltre, associare alla *fake root* le corrette chiavi managed-keys e trusted-keys (es: /etc/bind/bind.keys):

```
managed-keys {
        "." initial-key 257 3 13
"PxjKVaSRiO4BPpBDGUXgPp1oEu37QJCQAxuwNImqRR2woNNKWYR4MFbfPtsM2oAzm05qv/w
Wpt2AzNV5sCbQ9A==";
};

trusted-keys {
        "." 257 3 13
"PxjKVaSRiO4BPpBDGUXgPp1oEu37QJCQAxuwNImqRR2woNNKWYR4MFbfPtsM2oAzm05qv/w
Wpt2AzNV5sCbQ9A==";
};
```

NB.: la direttiva managed-keys può anche essere rimossa.

Nel file di configurazione dei nameserver utilizzati per la sperimentazione (es. /etc/bind/named.conf), verificare che siano definite le seguenti direttive per il corretto supporto del DNSSEC:

```
dnssec-enable yes;
dnssec-validation yes;
```

3.2.2. **Recursive Resolver**

I Registrar possono eventualmente utilizzare anche il *recursive resolver* (***nsresolv.pubtest.nic.it***) messo a disposizione dal Registro. In tal caso, il Registrar dovrà inviare una richiesta a hostmaster@nic.it con Subject:

"Comunicazione IP per l'utilizzo di nsresolv.pubtest.nic.it" contenente gli indirizzi IP delle macchine dalle quali il Registrar effettuerà le query DNS.

3.3.**Firma e registrazione di un nuovo dominio**

Supponiamo che il Registrar desideri registrare il dominio **dnssec.it**.
Per prima cosa deve configurare almeno 2 nameserver autoritativi (uno primario e uno secondario) per il dominio in oggetto.
Una volta prodotto il file di zona (non ancora firmato), il Registrar dovrà generare le chiavi KSK e ZSK associate al dominio e procedere alla firma della zona.

Esempio di file di zona non firmato per il dominio dnssec.it
(Es: /var/named/unsigned/dnssec.it)

```
$TTL 3600
;;
;;    AUTHORITATIVE DATA FOR: dnssec.it.
;;
@           IN    SOA   ns1.dnssec.it. hostmaster.dnssec.it. (
                  2017040300   ;file Version #
                  86400        ;Refresh        1 day
                  1800         ;Retry          30 minutes
                  2592000      ;Expire         30 days
                  900          ;Negative Cache 15 minutes
                  )

@           IN    NS    ns1.dnssec.it.
@           IN    NS    ns2.dnssec.it.

www   IN    A     192.168.1.100
ns1   IN    A     192.168.1.10
ns2   IN    A     192.168.1.20
```

Prima di procedere con la generazione delle chiavi KSK e ZSK, occorre inizializzare opportunamente la libreria SoftHSM2 come segue:

Definizione del Token PIN

```
mkdir /var/lib/softhsm/tokens
mkdir /etc/bind/softhsm
chmod 600 /etc/bind/softhsm
chown root:root /etc/bind/softhsm
echo -n "12345" > /etc/bind/softhsm/token_pin
```

N.B.: *Il comando precedente crea un file contenente il Token PIN con un carattere di new-line (\n) al termine della stringa, indispensabile per il corretto funzionamento dei comandi successivi.*

Inizializzazione del Token

```
softhsm2-util --init-token 0 --slot 0 --label pubtest_dnssec
```

Inizializza il token, che conterrà le chiavi KSK e ZSK, allo slot 0 e gli assegna come etichetta pubtest_dnssec.

Generazione e scrittura delle chiavi PKCS#11 sul dispositivo softHSM

```
pkcs11-keygen -a RSASHA512 -b 2048 -l zsk_pubtest
pkcs11-keygen -a RSASHA512 -b 2048 -l ksk_pubtest
```

Generazione su file delle chiavi KSK e ZSK

Per generare su file le chiavi ZSK e KSK associate alla zona relativa al dominio dnssec.it, il Registrar dovrà eseguire i seguenti comandi:

```
mkdir /etc/bind/softhsm/dnssec.it_keys
cd /etc/bind/softhsm/dnssec.it_keys
dnssec-keyfromlabel-pkcs11 -a RSASHA512 \
      -l "pkcs11:object=zsk_pubtest;pin-source=/etc/bind/softhsm/token_pin"  \
      dnssec.it

dnssec-keyfromlabel-pkcs11 -a RSASHA512 -f KSK \
      -l "pkcs11:object=ksk_pubtest;pin-source=/etc/bind/softhsm/token_pin"  \
      dnssec.it
```

I 2 comandi precedenti generano su file le 2 chiavi KSK e ZSK con algoritmo 10 (RSASHA512) e con data di creazione, pubblicazione e attivazione uguale alla data di invio del comando.
Ciascun comando produce 2 file per chiave (.key e .private). I 4 file prodotti si trovano tutti nella medesima directory */etc/bind/softhsm/dnssec.it_keys*.

```
$ ls -la
total 28
drwxr-sr-x 2 root bind 4096 Mar 31 16:32 .
drwxr-sr-x 3 root bind 4096 Mar 31 16:00 ..
-rw-r--r-- 1 root bind  588 Mar 31 16:03 Kit.+010+21288.key
-rw------- 1 root bind  624 Mar 31 16:03 Kit.+010+21288.private
-rw-r--r-- 1 root bind  589 Mar 31 16:02 Kit.+010+44813.key
-rw------- 1 root bind  624 Mar 31 16:02 Kit.+010+44813.private
```

I file Kit.+010+21288.key e Kit.+010+21288.key sono quelli relativi alla KSK, mentre gli altri 2 sono quelli associati alla ZSK.

Firma della zona

Il Registrar potrà ora procedere alla firma della zona, tramite il seguente comando:

```
dnssec-signzone-pkcs11 -A \
     -3 $(head -c 1000 /dev/urandom | sha1sum | cut -b 1-16) \
     -T 3600 -N KEEP -K /etc/bind/softhsm/dnssec.it_keys -o dnssec.it \
     -t -f /var/named/signed/dnssec.it -S /var/named/unsigned/dnssec.it
```

Con tale comando si firma la zona associata al dominio dnssec.it con il meccanismo *NSEC3 OPTOUT*.
Per i dettagli sui parametri utilizzati nel comando precedente, far riferimento al manuale del comando dnssec-signzone-pkcs11 (*man dnssec-signzone*).

File di zona firmato (Es: /var/named/signed/dnssec.it)

```
$TTL 3600
;;
;;    AUTHORITATIVE DATA FOR: dnssec.it.
;;
@           IN    SOA   ns1.foobar.it. hostmaster.foobar.it. (
                  2017040300    ;file version #
                  86400         ;Refresh        1 day
                  1800          ;Retry          30 minutes
                  2592000           ;Expire         30 days
                  900             ;Negative Cache 15 minutes
                  )
                  3600  RRSIG SOA 10 3 3600 (
                              20170503132219 20170403132219 5090 dnssec.it.
                              D6ZyBzb89AoKmJeJL0cw8hssR5zaG5OSVWQI
                              kuynGVkC1XFB/N+mIYVSBb/QhqTGvV0+NV33
                              Ea+ni7djuA9GCBAwxPeZqZGtHA9NVI5wZEgz
                              ToYJKO5XNMD/5pfTdD3zGMo/t+UM4jDaOf6m
                              urLRyDFMjS8wdooTrT5wQx5vKLIsdgOm7TFM
                              vsddM1gQz4I2HvY37YuCE8PPUSLRHv3/8muU
                              MjRsHJUbeY5IRiXdiNwEGKBI5hgWJTDb3Rrg
                              DHES2nkrTixfYYug9RdnHXKLxCgSN8stI+TE
                              Bq8K5dl6a4bH1QbGToqOsD2vlKraiT3CLJMM
                              D1Ut+dv7XpPMbfvDSA== )

                  3600  NS    ns1.foobar.it.
                  3600  NS    ns2.foobar.it.
                  3600  RRSIG NS 10 3 3600 (
                              20170503132219 20170403132219 5090 dnssec.it.
                              UPY9yPLPBlTAUNerE0IpQaoiBssusi8cBlhM
                              UBl8cddcHZp7/4EZBBWrSO23pY1ZdcsknUI4
                              ml4vJtHrW75ljMInVwDbWTX66JMkD8hzwesr
                              g66A71fHGkpQe4fVxNCHji2SIzOwVAYaYYH1
                              8eEbe4GwIaPOJGfdO8BR69OrQxnjZTGWvCie
                              BXO8OOEwMvfSb+qAeNirgenF8eWXYkmkgWCD
                              L8iKDwyldh+fztPxVk1XVC12k4zEwHmA/CWP
                              u71+77guVi5oZlv28Aojt8dihBd5gNiMzGGb
                              pw7sBbNRQ9dERMfDXWBurIEf7cMOkdgwzyQz
                              JrsmzVoFwqz3MIsQXg== )

                  3600  DNSKEY      256 3 10 (
                              AwEAAcqSjOhWQXF2AQOJkLWhAnoBYMSMHgnD
```

```
                                jI5KwxVSY+vz8bF4CPZTwjbRZBJxtrWbecGY
                                K3Lc3o7g/yk0CSZpgYz2D4TutzgRWsotZ8FN
                                XRgLm/yP2EMco8mSU3OKgUKpOlI8PoofYmO5
                                Ngu+O6kFWgisho14cbSag/tNtwOrAC8hXuip
                                oPxx0HHdO+U1xNc1sOxB+57n42+qy1eU9nFj
                                Mdx1dyMe18ug1tOKNZzZS+ag5kwKt4h1zSp5
                                ZZ1GmqL6jp96GXC8O/8EjNEd/QDP/byH7KKK
                                NqXNEt1LXOZEbQ7lLFnPItEOoYTlblMbq7Fr
                                Ns3yYVapcZRKOY6rofbXuw8=
                                ) ; ZSK; alg = RSASHA512; key id = 5090
                    3600  DNSKEY      257 3 10 (
                                AwEAAaWLn6kj59QaKBqdtDWdS5zdOQT5D+BF
                                OlBpcLXMDxhRgpQMm+ez8K3/zbXkm1Qd8Bf1
                                H/eq/MGwCHlgOz8iYV7JPCkDcShevmONiwnR
                                q1bNPODMgDbSuV2HWBaY2ETY95WuhmfQbrhj
                                tpHtfu4JmSgQjdTQwrUp6TOk/DQS57NuPRNk
                                FLOfT1Z33Z76nCIP/o8D7gBTf+ofqn8XMzll
                                fqGEFblJIL4jhDOpbNvRJZc7BPqXWHhsLI42
                                AGjQHvhjB5xajSqDRLy16v6cc3PZaXBNGrk7
                                v+CjeMckz/d1oYkhOxpgpXAeTZDT2h3yrcQp
                                AbGtdPV7QtoENEhf1lSSRus=
                                ) ; KSK; alg = RSASHA512; key id = 32577
                    3600  RRSIG DNSKEY 10 3 3600 (
                                20170503132219 20170403132219 5090 dnssec.it.
                                FB3K9pyuJGCm7vDrKtt7w8w+NZ+LenDfpHuC
                                zik769vNMQWtwNQhqktfkJseLMzkjGQuYKM1
                                ngvpn86lyrirumrnAhrL8yOZIvAh9fk2/pyk
                                TeVYGilqSG9jiurpxO5GU7KYsYmLxqZ7uTqw
                                hUUWEpYHplrgHR9ntMU/2/9SvXyNf3Gt2Bao
                                FYUWbdgOHxWguRAIza43pS5B39yxKthFrQz4
                                pZpH3SkKSZ5ABDKC19cG9sYzLrs9inmBX9Y3
                                K/oP6NhlRALtH+9TMHuKyEbcsv1g1zSdvqaq
                                IqVTSkoK+Io+IZoo1OsMnteIqfrWtaKw9v8R
                                R5QrTEYXj8vRjArQ9w== )
                    3600  RRSIG DNSKEY 10 3 3600 (
                                20170503132219 20170403132219 32577 dnssec.it.
                                X3Tp7akkaNVlxTwYviLVFB8XqIO3j7r4zUHA
                                AJNnQmpMzuKZxyfcdjRh/fHpNKE6sCDK2pJL
                                +tmsXbUc6SQw4yTQwLdYjXLNyXvyXIUlHYZy
                                Q57ss2S9Qm8VxC5C3rCk22vOAqJb8KQ8QIjU
                                WIgvkPnhOk9Rb2kS/f7PGhlVyGt4QCcMNDfp
                                +SODr/pcGMPOxvhBHA7HXUO4+L4JoqQwvwDV
                                xqTsOAmDqNUm6N29XvrlX6RODwquAGEC3a1+
                                KyZcePuOkwY8tWWl8rDW/FIXSCIz26RjvijI
                                NE1QOCfhOnHwXS3l8A8OY39poHGIKODTEqqf
                                JXW17tr6zjQe90+l4w== )

                          NSEC3PARAM 1 0 10 F97954D9C34AD24D
                    0     RRSIG NSEC3PARAM 10 3 0 (
                                20170503132219 20170403132219 5090 dnssec.it.
                                ZArRqJatlRJVRb8xQ5hYFTsf5x4N6mAUMuMc
                                1+Iw2nO+N9qVSVqnOF18XrkElFt5ONpnaejw
                                hk7AB3xYICv6zCIszvztKO2bxtgvtfk3xd43
                                YBrfHoXHz6/HObUyjzn9WPvZvjADeIixnM82
                                SAoyNITTsPiOB/vvwO5VFu8b8m5dAxAZPesG
                                ivuYsVAMWFS+TfuaxNi7noHDzJ3qO5hPg1a8
                                eOhEODgB1wec4m+5IHolToAIMi+fJCl7Gy3d
                                dW4VMEPE2d4+3/MsLrKEv46AuNTG37adcJMc
                                t1trv71ltW75ltrJs9ft2xgUd6o9VyxIBh8E
                                3uR92bpOwslJy/AqBg== )

www   3600  IN A  192.168.42.1
                    3600  RRSIG A 10 4 3600 (
                                20170503132219 20170403132219 5090 dnssec.it.
                                eRiNx7ahh2VTOnTndulMibiAEUwu4tWgJdAM
                                O9P6Ro3HDK6V7cgBzPEDK8OUjWP96VHOVLGN
                                MY6SvOGaoTpszE+e+NvkZ/LSG54As9bNXfok
                                V42mGLLD9l8DObCOlk6pqvU9tfphnOoXh4MG
                                +ghB3dHqhJ9dbQsXgM3fnAlpms2E1X71YU1U
```

```
                                nomZtOCgPmu3h8rwZVCUEXTQV5ajTG+p20no
                                PN8szbjYypTNMsY+ECs4FYOgdZixBKiy8yS4
                                S51I7NYWqbZ7tjY50244atLBRZbDsZH7RJKn
                                yK+zYJ6dfF+MPaETJkFhtE3bxBLTHZVYhCuF
                                uwfJ0CdReZdAKMUGMg== )

AO6I1817408G8BQA9H04AHV35Q1RL08N.dnssec.it. 900 IN NSEC3 1 1 10
F97954D9C34AD24D (
                                B7SQTJO2UVJ3UVSQOB26GNLMRN9JA5PC
                                A RRSIG )
                      900   RRSIG NSEC3 10 4 900 (
                                20170503132219 20170403132219 5090 dnssec.it.
                                CEPZS+eRsFxyrOf65v3jhQca9j8nkv7/1Vnv
                                bSvQYortErpVrjFmOeL6ByLRFNj23Ma3PCIf
                                7WdWBzrytRQqO/ozB4SgiWgaw0By5Da6VhgN
                                y+Oqr4vBUSPp12Dr/7Bz2idJFIJ8ceeFWWM3
                                Yb5uyfOigF9gbXWOGzJ+BtlrmRN85jTeoKF+
                                rUHrb0h9n9+FmwV+ZI5lwbUgfx5G0ynVMOX0
                                +HpizLW0ry8/thYh8JdWWdIal4BBGaOMpIU4
                                6wUGlVr+SX2HuRwqsrAnSf8qCUE9zqRBJUEu
                                Zpvfy+f40aVasAy2alwoQQYMvZ/G4xZFIaMC
                                9KHmGC13Ci7Difh2Bg== )
```

Dopo la generazione della zona firmata, è necessario che BIND ricarichi la zona (Es: *rndc reload dnssec.it*).

In seguito al processo di firma della zona, nella directory contenente le chiavi associate al dominio è presente anche un file chiamato *dsset-dnssec.it*. Tale file contiene il record DS (Delegation Signer), nei due formati SHA1 e SHA256, relativo alla KSK utilizzata.

Esempio di file /etc/bind/softhsm/dnssec.it_keys/dsset-dnssec.it.

```
dnssec.it. \
      IN DS 32577 10 1 F7EC33C3B32001665CBADA326A4EC5D4EA3C2E8B
dnssec.it. \
      IN DS 32577 10 2 29B3CEABD206C799E194E7F5D159BDC83459A7A32E0CF7342A0DBEED
916C31CF
```

È possibile estrarre i dati relativi al record DS con il seguente comando, esplicitando anche il tipo di algoritmo desiderato:

```
      dnssec-dsfromkey-pkcs11 -a SHA-256 Kit.+010+21288.key >
/etc/bind/softhsm/dnssec.it_keys/dsset-dnssec.it_sha265.txt
```

Per procedere alla registrazione e alla delega del dominio firmato dnssec.it, il Registrar deve inviare al Registro uno dei due record DS precedenti. Tale operazione è eseguita tramite il comando *Domain Create* (in questo caso è stato scelto il record DS con lunghezza minore):

```
<?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>dnssec.it</domain:name>
            <domain:period unit="y">1</domain:period>
            <domain:ns>
                  <domain:hostAttr>
                        <domain:hostName>ns1.dnssec.it</domain:hostName>
                        <domain:hostAddr ip="v4">192.168.1.10</domain:hostAddr>
                  </domain:hostAttr>
                  <domain:hostAttr>
                        <domain:hostName>ns2.dnssec.it</domain:hostName>
                        <domain:hostAddr ip="v4">192.168.1.20</domain:hostAddr>
                  </domain:hostAttr>
            </domain:ns>
            <domain:registrant>XXXXXXXX</domain:registrant>
            <domain:contact type="admin">YYYYYYYY</domain:contact>
            <domain:contact type="tech">ZZZZZZZZ</domain:contact>
            <domain:authInfo>
                  <domain:pw>KKKKKKKK</domain:pw>
            </domain:authInfo>
            </domain:create>
      </create>
      <extension>
            <secDNS:create
              xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
            <secDNS:dsData>
                  <secDNS:keyTag>32577</secDNS:keyTag>
                  <secDNS:alg>10</secDNS:alg>
                  <secDNS:digestType>1</secDNS:digestType>
                  <secDNS:digest>F7EC33C3B32001665CBADA326A4EC5D4EA3C2E8B
</secDNS:digest>
            </secDNS:dsData>
            </secDNS:create>
      </extension>
      <clTRID>ABC-12345-DNSSEC</clTRID>
</command>
</epp>
```

Una volta ottenuta la conferma della corretta registrazione da parte del server EPP, la conferma della corretta validazione dei nameserver autoritativi da parte del DNS validator e attesi i tempi di generazione e firma (ogni 2 ore) della *fake zone .it* da parte del Registro, il dominio dnssec.it può considerarsi correttamente registrato, firmato e delegato.

Per ottenerne conferma si può utilizzare il comando whois interrogando il server *whois.pubtest.nic.it*.

Esempio query WHOIS:

```
$ whois -h whois.pubtest.nic.it dnssec.it

*******************************************************************
* Please note that the following result could be a subgroup of    *
* the data contained in the database.                             *
*                                                                 *
* Additional information can be visualized at:                    *
* http://www.nic.it/cgi-bin/Whois/whois.cgi                       *
```

```
*************************************************************************

Domain:             dnssec.it
Status:             ok
Signed:             yes
Created:            2017-05-10 09:01:00
Last Update:        2017-05-11 00:30:02
Expire Date:        2018-05-10

Registrant
  Organization:     ccTLD '.it' Registry - IIT/CNR
  Address:          Via Giuseppe Moruzzi 1
                    Pisa
                    56124
                    PI
                    IT
  Created:          2007-03-01 10:26:04
  Last Update:      2016-06-03 15:19:28

Admin Contact
  Name:             Domenico Laforenza
  Organization:     Istituto di Informatica e Telematica del CNR - ccTLD ".it"
Registry
  Address:          Via Giuseppe Moruzzi, 1
                    Pisa
                    56124
                    PI
                    IT
  Created:          2008-07-11 11:23:04
  Last Update:      2016-06-03 15:19:28

Technical Contacts
  Name:             Daniele Vannozzi
  Organization:     Istituto di Informatica e Telematica del CNR - ccTLD ".it"
Registry
  Address:          Via Giuseppe Moruzzi, 1
                    Pisa
                    56124
                    PI
                    IT
  Created:          2002-02-20 00:00:00
  Last Update:      2016-06-03 15:19:28

  Name:             Maurizio Martinelli
  Organization:     Istituto di Informatica e Telematica del CNR - ccTLD ".it"
Registry
  Address:          Via Giuseppe Moruzzi, 1
                    Pisa
                    56124
                    PI
                    IT
  Created:          1998-04-14 00:00:00
  Last Update:      2016-06-03 15:19:28

Registrar
  Organization:     ccTLD 'it' Registry
  Name:             REGISTRY-REG
  DNSSEC:           yes

Nameservers
  ns1.pubtest.nic.it
  ns2.pubtest.nic.it
```

3.4. Verifica della corretta configurazione DNSSEC

Comando DELV

Esempio di verifica della corretta Chain of Trust per www.nic.it (sempre per quanto concerne il solo ambiente di pubtest) utilizzando il comando delv, messo a disposizione dalla versione 9.10 (in poi) del Bind:

```
delv +multi +vtrace www.nic.it A

;; fetch: www.nic.it/A
;; validating www.nic.it/CNAME: starting
;; validating www.nic.it/CNAME: attempting positive response validation
;; fetch: nic.it/DNSKEY
;; validating nic.it/DNSKEY: starting
;; validating nic.it/DNSKEY: attempting positive response validation
;; fetch: nic.it/DS
;; validating nic.it/DS: starting
;; validating nic.it/DS: attempting positive response validation
;; fetch: it/DNSKEY
;; validating it/DNSKEY: starting
;; validating it/DNSKEY: attempting positive response validation
;; fetch: it/DS
;; validating it/DS: starting
;; validating it/DS: attempting positive response validation
;; fetch: ./DNSKEY
;; validating ./DNSKEY: starting
;; validating ./DNSKEY: attempting positive response validation
;; validating ./DNSKEY: verify rdataset (keyid=32013): success
;; validating ./DNSKEY: signed by trusted key; marking as secure
;; validating it/DS: in fetch_callback_validator
;; validating it/DS: keyset with trust secure
;; validating it/DS: resuming validate
;; validating it/DS: verify rdataset (keyid=11649): success
;; validating it/DS: marking as secure, noqname proof not needed
;; validating it/DNSKEY: in dsfetched
;; validating it/DNSKEY: dsset with trust secure
;; validating it/DNSKEY: verify rdataset (keyid=21288): success
;; validating it/DNSKEY: marking as secure (DS)
;; validating nic.it/DS: in fetch_callback_validator
;; validating nic.it/DS: keyset with trust secure
;; validating nic.it/DS: resuming validate
;; validating nic.it/DS: verify rdataset (keyid=44813): success
;; validating nic.it/DS: marking as secure, noqname proof not needed
;; validating nic.it/DNSKEY: in dsfetched
;; validating nic.it/DNSKEY: dsset with trust secure
;; validating nic.it/DNSKEY: verify rdataset (keyid=28773): success
;; validating nic.it/DNSKEY: marking as secure (DS)
;; validating www.nic.it/CNAME: in fetch_callback_validator
;; validating www.nic.it/CNAME: keyset with trust secure
;; validating www.nic.it/CNAME: resuming validate
;; validating www.nic.it/CNAME: verify rdataset (keyid=23021): success
;; validating www.nic.it/CNAME: marking as secure, noqname proof not needed
;; fetch: web-r3.nic.it/A
;; validating web-r3.nic.it/A: starting
;; validating web-r3.nic.it/A: attempting positive response validation
;; validating web-r3.nic.it/A: keyset with trust secure
;; validating web-r3.nic.it/A: verify rdataset (keyid=23021): success
;; validating web-r3.nic.it/A: marking as secure, noqname proof not needed
; fully validated
www.nic.it.       60 IN CNAME web-r3.nic.it.
www.nic.it.       60 IN RRSIG CNAME 10 3 60 (
                        20170503132503 20170403132503 23021 nic.it.
```

```
                        waNkkNcPFZ9IflX7MsTVSYVG2x/uNw3AHSZUtjaooabA
                        NWc0IwpSbB53QREdXmUsGHFmyromaQg1hRUagvuxVyHM
                        PxLwmiYB4Epfu3Ws0aXosMXCmEA5HIi9k2g4TTFBOCAv
                        KmLuxkoleDGY5bu7I86B7/s8yHhoWJbu19rAQhhVlJBf
                        aKj9mvSx/nMreWAqAHrpHe0k6K5XAXEOPxXzQiSdvAuX
                        g4WdBZZmCdHMYspvxFx1ROwkAwN1HcYc9UwkyYz4sUAn
                        +QYSjD6YSPepDZXCvjp93NaKjzpxL1y3vA/Ix4PNphJC
                        NvVzjbBQGzpsRlb5j1BlkowLqU5JWASh+Q== )
web-r3.nic.it.          60 IN A     192.12.192.28
web-r3.nic.it.          60 IN RRSIG A 10 3 60 (
                        20170503132503 20170403132503 23021 nic.it.
                        LLPO1ASgzTILONohbB2vBlttZd7xJmizezOtbx7QpwrD
                        rSHsJIrjpMOwC4oG9uBhY8GeObI5yc6Oj2cesMvYczQT
                        BwC+hjSD+oH1IsN1reKOLDxfS9N83lOPJTvv7tFASELb
                        Fj8kW65U3OzaelLdGpYr1m//u8bC+ZgqW/4dkRbks9SV
                        aiUxOSk3jhCco+oZ4oQdxZmd9zoXYiQMjEhEUjScapfO
                        zr9lZtV9gk/5CXrSNB7f6UNQja9lXEdqTn/OIM/Q6OuV
                        wgTYCQeO8b6bV7con/d9N/Q8FC57H1fHzyCu/VLOfH9/
                        57apTdRMw7by/fKMxtOQKXUkMq+uskTZiQ== )
```

Affinché la validazione avvenga con successo occorre che il file /etc/bind/bind.keys (facendo riferimento a piattaforme Ubuntu/Debian) esista e contenga la trusted-key corretta del fake root nameserver di pubtest.

Comando DIG

Per versioni del Bind inferiori alla 9.10 si può sempre utilizzare il comando dig. In questo caso la trusted-key del fake root nameserver di pubtest va esplicitamente passata come parametro all'interno di un file opportunamente creato.

```
dig . DNSKEY | grep -Ev '^($|;)' > root.keys

dig +sigchase +multiline +trusted-key=root.keys A www.nic.it

;; RRset to chase:
www.nic.it.       60 IN CNAME web-r3.nic.it.


;; RRSIG of the RRset to chase:
www.nic.it.       60 IN RRSIG CNAME 10 3 60 (
                        20170503132503 20170403132503 23021 nic.it.
                        waNkkNcPFZ9IflX7MsTVSYVG2x/uNw3AHSZUtjaooabA
                        NWc0IwpSbB53QREdXmUsGHFmyromaQg1hRUagvuxVyHM
                        PxLwmiYB4Epfu3Ws0aXosMXCmEA5HIi9k2g4TTFBOCAv
                        KmLuxkoleDGY5bu7I86B7/s8yHhoWJbu19rAQhhVlJBf
                        aKj9mvSx/nMreWAqAHrpHe0k6K5XAXEOPxXzQiSdvAuX
                        g4WdBZZmCdHMYspvxFx1ROwkAwN1HcYc9UwkyYz4sUAn
                        +QYSjD6YSPepDZXCvjp93NaKjzpxL1y3vA/Ix4PNphJC
                        NvVzjbBQGzpsRlb5j1BlkowLqU5JWASh+Q== )


Launch a query to find a RRset of type DNSKEY for zone: nic.it.

;; DNSKEYset that signs the RRset to chase:
nic.it.                 8726 IN     DNSKEY 256 3 10 (
                        AwEAAdizWMwFPjLPbUZohp5nONDcplTsCO4EE+EHtgUq
                        eWIQOEaF9G1jf2u/YFhoEhD+ZbUzrgI2P7abCIxJfP7k
                        ZRTnb4G0kav6lEVJRyl4V2BCgIOgLBzv3EhEZHSQOvG2
```

```
                        OVgC1m2JbsnL0rTGVvsVYSr8xh6H37IbZMK7qlb8f/+u
                        F6rw8cUWYRs1bsMH2Vri21e1LmTzLvFlfncT0vpG5vkD
                        VQdxZOFp9O8lXEqvrHVW5nzWpfzpaWrYtKoNzGmXi8yR
                        QQuK8dRFGJwO/wmMwstSSzGo7DL4OxpYl2txIw4Nq/ww
                        GcHOv83M+3MyoCXcigwp2TsCamkomygUNS9NYWO=
                        ) ; ZSK; alg = RSASHA512; key id = 23021
                    8726 IN     DNSKEY 257 3 10 (
                        AwEAAdilKQPHLhRSu/YisveWQpwwxSVXsL0RmqQoIa+V
                        k/kcrjgV5jorzaQwiVjpsLkdu2lCMUPL5OlYZc9ZMhRI
                        kvE0KI5hLqfOUAppWViwoI4PyX9MdjreueYsBf5pPZVC
                        y1o+W96wxgQv3/DmvBGLebHfuJpBO6f4vPdyuYGM0/cl
                        7P8jaOde2eNPv8yZEpL07cjR3gaInH5O2qEEH2CM2Wge
                        QPOjj7NXpd0vlXp/e1RkAGFjUypwAy4s7Nq626Q4EayN
                        Qj07c+idHLuv7x/i4F9+xHYr0DsjzjhOeiQ+D+Jhv+NK
                        WNmmE4TeNrDRdvOG8O26fSxMXdusK3JCzORsxq0=
                        ) ; KSK; alg = RSASHA512; key id = 28773


;; RRSIG of the DNSKEYset that signs the RRset to chase:
nic.it.                 8726 IN     RRSIG DNSKEY 10 2 10800 (
                        20170503132503 20170403132503 23021 nic.it.
                        Qo7AFDW5ZovGqOXcCj4SWZ7UqQSS8OJlJFgYNZvPqQ+u
                        0QXDIWO/nSh8kWOs36BwGVZOGiJmxV5ebxIE8L+6P5YY
                        V28S8JY6/7As4WbFaUY9f2b7wWITiP1DQ2OZZjTpaJGX
                        1O1qAJkdlYfzPeDw14XvP3V5o5Nl4Y8V/oqWRccTB97a
                        48gJFhJJDMlcc6kv339ZkungdjZD+Ugqlo+OJkMdX+1j
                        vZdJuZZbXDKGzDgOqPkuNTFO3tuDbwpXlpxbzrCJ61JL
                        HmTCQjTIu7j6f284PUVEnqrzdFnlHkDy5y0PTKhHCtGb
                        NH2E5aMVdgRhTv1H8QZ48nKUp/rjiY5+qw== )
                    8726 IN     RRSIG DNSKEY 10 2 10800 (
                        20170503132503 20170403132503 28773 nic.it.
                        KKPw3p/Hu2jiYfblh87swvZr9sRST0AIiSODdGgCGQSO
                        7OgzsmJGPRH8Wff+d7pI5EHr+WPgFcBRPSmkCWrykigI
                        cHUZ/hrVWOvaNmO/dPjSkeAgw3TTnzO89Sj/d/qU6BYi
                        uA3j1OajyobvpZIF7nkhtTLoOATaPfwo4f0a2fFc9rrm
                        N5wOsj/+ffXTjhlZJh3t9QO9LPQugERxwSHATyKaSNW6
                        +kuOPeDKq2sEhlzr4n9jkiI9wrxp6bPI2nwtjaiVLQpd
                        klZaf30MBT9zl3AkJOwfhsKjUwIHpg4KflQ0p7GYyPFh
                        nN3LtM9YN3lbEB7Aqjl2YoY7cDlvFxagMg== )


Launch a query to find a RRset of type DS for zone: nic.it.

;; DSset of the DNSKEYset
nic.it.                 8726 IN     DS 28773 10 1 (
                        DDE65DBC575BCE8B7F8C571C385862F9AF321666 )


;; RRSIG of the DSset of the DNSKEYset
nic.it.                 8726 IN     RRSIG DS 10 2 10800 (
                        20170504080205 20170404080205 44813 it.
                        WmmYqmV1nuCb3/VdCpRJ8SU6AVwqdagri0xNT5I77Sgb
                        +Utw4WdWhMMVrXVvH6RE5NGbvEzaAfyhS3li2NNBM0De
                        BLD63L2vutmGTRG/OeuHwkepPMZ2FnHIen8MJPuj3muG
                        wZLd1AxZ3NIW7Lx26HCpk69h7OiOhKLGe5m1xO+Ub9N2
                        HuDTPgJhZW5EE869+D/SwUy+uCPAe/3XAYwP6M8/Y8cW
                        kxpK2QOeB8CtpPAjgwStsdUAZjGxndT/1rEdvAegSKnK
                        FJX7WETCWKScKfaCZlUb4NkS9Z3vs/4tDWxat4czrbEo
                        unFaAD3vWYJzM9Js2b3l6CECNdDnZY2RJg== )



;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING CNAME RRset for www.nic.it. with DNSKEY:23021: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
```

```
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for nic.it. with DNSKEY:28773: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs,
thus the DNSKEY validates the RRset
;; Now, we want to validate the DS :  recursive call


Launch a query to find a RRset of type DNSKEY for zone: it.

;; DNSKEYset that signs the RRset to chase:
it.               8726 IN     DNSKEY 256 3 10 (
                        AwEAAe8a4wzeXYPEQ4thwqA5/ddCZo5YkHEkw0cpBNLZ
                        Of5zP3m+KQrM+chXwI6Jn2/LT5RkDm3ubMViXCGwUc1g
                        6bR1Si9wqpbDk6hnRzbxXYWkSfZZLBj4+ysIFoUUQtow
                        MnBgbQRZDDYFoVAeXg4rAJwb6eiVkotH8js8s1ev6qTl
                        zzld0QEOxjfwvXnS+F+u0LiD++upBCy8b06DaZheHkZl
                        yejgTwEvS5iJDVl+f3WWXOhF0hiJKAl9UsiDP5zKhv6v
                        K5eLW0Tuz8+SbNQrtMsRrIOY+wD+SQYDLY0uJKyBc/gQ
                        wi+wbPVj0ESnckIQUHiepCwcQ+MT/S6Spg83LQc=
                        ) ; ZSK; alg = RSASHA512; key id = 44813
                  8726 IN     DNSKEY 257 3 10 (
                        AwEAAcMCNpEDx9RgzpOM8t5LctEHQm1/laputp39IEjk
                        ZnsgF4sNKAU4CcaGWGBICbzxArYLxxf/WBQQyHRKpeGP
                        xSWZAHStHT9S7+hKClc5nzrWl8hnY+tJVP4tCynLbj4+
                        op9ENv8dntoAy/YE1I5cUGNDSLKxQVADel39rSu4sIYP
                        1vMqeo7wB9UjH7PtDNckL39zMiNNjiilrzrlR6ZPEi7F
                        1aPsXhMiGGwa23ajqlDwuR7p2AnirDpZMx5wKr+6h5Mb
                        XPZvoY6TtAEFPKF9ror0vstfLG56UzMzP91m2liicmYo
                        mlJlzPzlZpamc4sTWUigSewrCNpLWuD7AxKx7Ss=
                        ) ; KSK; alg = RSASHA512; key id = 21288


;; RRSIG of the DNSKEYset that signs the RRset to chase:
it.               8726 IN     RRSIG DNSKEY 10 1 10800 (
                        20170504080205 20170404080205 21288 it.
                        ZLd5GQgrmPQgPE/OuwU8gmHU0w9h5UrcqR10C5PyFrsC
                        EP96PUYv/O5gQ0sbhuH3NGqw9nAn2arCBMdxEwzNoQXv
                        ImK3KSRJSHFulZLfiNkH+8puuM2L0BLOxBcwzvWGg8f+
                        u6ELDwPSRCdGix9Ss9RzueFGlebqgMHpmq6IkXw75rS/
                        T562eAHcdgJMjlHbT9L5tvBJIduqkS8lNYiZOOzC5haJ
                        Kk8bZmukiA55gnDk2IJU4sPV3vU6+jOHOQW4Oh2ZpDWZ
                        KrFI4NRxTUrd3piPpNRu68rHA529UAEJqOh1hYMWg9+W
                        k1wcEXf8vVdr8RGR0HkDucdw2ds7NrhHJw== )
                  8726 IN     RRSIG DNSKEY 10 1 10800 (
                        20170504080205 20170404080205 44813 it.
                        eidUpKs35wAvtfpGGO2628PO8uS1IzKB2uzcU/6Uhm9/
                        ZtMENi4d6SoYChdEcCn1yIQOc/idavSCxivdzHUkNaqI
                        O/LbUDvoZi1//DQUCFAHWbKQlipdPnnu1Z2lrKp3ahfm
                        aJPcbjQAv9KNa4vvYBf1F99bb2tpWEdLg3BeS9G3BXi9
                        by7oTcqtDq7/CXdFtD1P4QRgsnk1xoHyxYEgPLuGd7rr
                        LFb0DonbdZ+/ASQkofKXfeOlG6VDxrST5DnpKnbCcfTb
                        reYKkt9E51+BjbmkwEqMFJbJ7TDg6V/hjlGQFTcyMOu3
                        WbJV3bEwvYP6vEFA9+2smCTaUBiu8IWx3A== )


Launch a query to find a RRset of type DS for zone: it.

;; DSset of the DNSKEYset
it.               84326 IN DS 21288 10 2 (
                        9F4C740B6443EEEB3FEFAB359ABDE41277081FCA7CDA
                        B9AD4F81DE6489A919CD )


;; RRSIG of the DSset of the DNSKEYset
it.               84326 IN RRSIG DS 13 1 86400 (
                        20281231000000 20170403064823 11649 .
                        4yFEHdUq5Zsc7L9pvy1aBdRen1t/P9yxF1iM9X7UBLna
                        dc42rn9TUX1HL5uwKLFYXNivxV9Hdd5ukbvgOAe5Kw== )
```

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for nic.it. with DNSKEY:44813: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; OK a DS valids a DNSKEY in the RRset
;; Now verify that this DNSKEY validates the DNSKEY RRset
;; VERIFYING DNSKEY RRset for it. with DNSKEY:21288: success
;; OK this DNSKEY (validated by the DS) validates the RRset of the DNSKEYs,
thus the DNSKEY validates the RRset
;; Now, we want to validate the DS :  recursive call


Launch a query to find a RRset of type DNSKEY for zone: .

;; DNSKEYset that signs the RRset to chase:
.                 76672 IN DNSKEY   257 3 13 (
                        PxjKVaSRiO4BPpBDGUXgPp1oEu37QJCQAxuwNImqRR2w
                        oNNKWYR4MFbfPtsM2oAzm05qv/wWpt2AzNV5sCbQ9A==
                        ) ; KSK; alg = ECDSAP256SHA256; key id = 32013
                  76672 IN DNSKEY   256 3 13 (
                        Yu+SDzyfDOIMSzIC8wKQ5+qE4gfa18AR3/jApxLaoC3H
                        H5HHKa5YqRzU5DDtifPLGXsm1SRAsFpSL98Zatj+9g==
                        ) ; ZSK; alg = ECDSAP256SHA256; key id = 11649


;; RRSIG of the DNSKEYset that signs the RRset to chase:
.                 76672 IN RRSIG DNSKEY 13 0 86400 (
                        20281231000000 20170403064823 11649 .
                        WsT81mchRWb48RIq+7OpVeFzVWQDzCArhRQCs9war77e
                        LD15ABZfrVXh58QndEB4wRPfj+Jmc6BNjNnfZLrphw== )
                  76672 IN RRSIG DNSKEY 13 0 86400 (
                        20281231000000 20170403064823 32013 .
                        U/JvUaqEwBi2L+amtaNIOMr4NNW+wT7lL18kr+Yqhr5c
                        Xx19JkjEnvASy7qJ4D1OjngGaUBHJ9L30YQO1cX+2A== )


Launch a query to find a RRset of type DS for zone: .
;; NO ANSWERS: no more

;; WARNING There is no DS for the zone: .



;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING DS RRset for it. with DNSKEY:11649: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 32013
;; VERIFYING DNSKEY RRset for . with DNSKEY:32013: success

;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

Architettura completa