BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

DNSSEC.vn

PHỤ LỤC

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC NĐK, ISP, DNS HOSTING PROVIDER

Quản lý phiên bản tài liệu:

Phiên bản	Ngày cập nhật	Ghi chú
1.0	10/12/2017	Biên soạn
2.0	12/11/2018	Cập nhật lần 1
3.0	18/9/2019	Cập nhật lần 2

MỤC LỤC

1. Các tính năng mới của BIND 9.11

1.1. Negative Trust Anchor (NTA)

1.1.1. Giới thiệu về NTA

Negative Trust Anchor (NTA) được sử dụng để thực hiện vô hiệu hóa quá trình xác thực cho một tên miền cụ thể trong một khoảng thời gian xác định, trong trường hợp tên miền không thể xác thực được do quá trình ký/thay khóa, do cấu hình hoặc do từ một cuộc tấn công, hệ thống vẫn có thể đáp ứng các truy vấn đến tên miền đó nhưng không thực hiện xác thực, và quá trình xác thực đối với tên miền đó sẽ được kích hoạt trở lại khi hết thời gian vô hiệu hóa. NTA được sử dụng trên các hệ thống máy chủ tên miền đệm (DNS Caching) của các ISP giúp hệ thống hoạt động linh hoạt và hiệu quả hơn.

NTA được sử dụng dưới công cụ rndc:

```
rndc nta [( -d | -f | -r | -l duration)] domain [view]
```

Thiết lập giá trị NTA cho tên miền ***domain*** cụ thể, trong khoảng thời gian là ***duration.*** Khoảng thời gian này có thể được thiết lập giá trị trong named.conf với tùy chọn nta-lifetime, và theo mặc định khoảng thời gian này là 1 giờ, nhưng có thể thay đổi thời gian lên đến một tuần. Khi thêm một NTA vào, nó sẽ được lưu vào trong tập tin (*viewname.nta* – thường là *_default.nta*).

Các tham số tùy chọn:

Tùy chọn	Mô tả	Ví dụ
-l (-lifetime)	Thiết lập khoảng thời gian có hiệu lực của NTA (đơn vị là giây/phút/giờ). Nếu NTA đã tồn tại, nó sẽ thực hiện cập nhật lại bằng giá trị tham số mới. Nếu thiết lập giá trị của lifetime bằng	rndc nta –l 60 example.vn

	0 sẽ tương đương với việc xóa NTA.	
-r (-remove)	Sử dụng để xóa NTA đã được thiết lập.	rndc nta –r example.vn
-d (-dump)	Liệt kê và in ra danh sách các NTA đang tồn tại áp dụng (nó cũng có thể in ra các NTA đã hết hạn nhưng chưa bị xóa).	rndc nta -dump
-f (-force)	Trong trường hợp nta-recheck kiểm tra định kỳ các tên miền và xác thực được trở lại trước khi hết thời gian lifetime. Khi áp dụng –f này, nó sẽ thực hiện buộc NTA đó phải duy trì trong suốt khoảng thời gian lifetime.	rndc nta –f example.com

Các tham số tùy chọn của nta được thiết lập trong *"named.conf"*

Cấu hình	Mô tả	Ví dụ
nta-lifetime	Thiết lập khoảng thời gian có hiệu lực chung cho tất cả các NTA.	nta-lifetime 1h;
nta-recheck	Khoảng thời gian mà named sẽ thực hiện định kỳ kiểm tra lại xác thực của tên miền được kích hoạt NTA, bằng cách gửi các truy vấn và bỏ qua NTA để xác định khi nào thì xác thực trở lại. Mặc định, cứ mỗi 5 phút sẽ thực hiện re-check.	nta-recheck 30s;

1.1.2. Triển khai thử nghiệm và kết quả

Ví dụ: Áp dụng NTA cho tên miền example trong khoảng thời gian 1 phút:

```
# rndc nta -l 60 example.vn
Negative trust anchor added: example.vn/_default, expires 15-
Nov-2016 09:33:20.000
```

Khi áp dụng NTA, các thiết lập sẽ được lưu tạm trong tập tin: mặc định là *_default.nta*:

```
# more _default.nta
example.vn. regular 20161115033549
```

Liệt kê danh sách các NTA:

```
# rndc nta -dump
example.vn: expired 15-Nov-2016 09:33:20.000
example1.vn: expiry 15-Nov-2016 09:34:19.000
example2.vn: expiry 15-Nov-2016 09:34:21.000
```

Thực hiện xóa NTA cho tên miền example.vn

```
# rndc nta –r example.vn
Negative trust anchor removed: example.vn/_default
```

1.2. DNSSEC Key Manager

1.2.1. Giới thiệu về DNSSEC Key Manager

DNSSEC Key Manager (dnssec-keymgr) được viết bằng ngôn ngữ Python dùng để quản lý việc Rollover Key. Bản chất dnssec-keymgr là sử dụng các lệnh *dnssec-keygen* và *dnssec-settime, dnssec-keymgr* sẽ tạo và cập nhật các khóa dựa vào việc sử dụng cấu hình định nghĩa các tập tin chính sách (theo mặc định tập tin này sẽ ở trong thư mục:

/etc/dnssec-policy.conf), trong tập tin này chứa các tham số về khóa như: thời gian công khai, thời gian hết hạn, chu kì thay khóa,…Tập tin này có thể sử dụng để định nghĩa chính sách cho một zone hoặc tất cả các zone để quá trình Rollover Key diễn ra một cách chính xác nhất, không bị gián đoạn làm sai lệch hệ thống và hỗ trợ người quản trị có thể tạo khóa, quản lý khóa một các dễ dàng hơn.

Lệnh chạy:

dnssec-keymgr [-K *directory*] [-c *file*] [-f] [-k] [-q] [-v] [-z] [-g *path*] [-r *path*] [-s *path*] [zone...]

Các tham số tùy chọn thường được sử dụng:

Tùy chọn	Đối số	Mô tả
-c	<path-to-file-policy.conf>	Nếu có tùy chọn –c, các chính sách DNSSEC sẽ được đọc từ tập tin (mặc định chính sách sẽ đươc đọc từ /etc/dnssec-policy.conf)
-f		Cho phép cập nhật thay đổi thông số của khóa đã tồn tại mà không cần hỏi (lưu ý không nên sử dụng cho các khóa đã được công khai)
-h		Hiển thị tất cả thông tin giúp đỡ về tiện ích này.
-K	<directory>	Đường dẫn thư mục chứa các khóa tạo ra. Mặc định là thư mục hiện hành.
-r	< randomdev>	Đường dẫn đến tập tin chứa dữ liệu ngẫu nhiên. Sử dụng –r /dev/urandom để việc tạo khóa nhanh hơn.

1.2.2. Cấu hình chính sách

Tập tin ***dnssec-policy.conf*** có thể xác định ba dạng chính sách:

- Các lớp chính sách (***policy name {… };***) có thể được thừa kế bởi các chính sách zone hoặc các lớp chính sách khác.
- Các thuật toán chính sách: (***algorithm-policy algorithm { … };***) khai báo thuật toán được sử dụng. Ví dụ, theo mặc định, thuật toán RSASHA256 có kích thướng 2048 bit sẽ được sử dụng chocar KSK và ZSK. Và có thể được thay đổi bằng cách sử dụng algorithm-policy.
- Các chính sách zone (***zone name { … };***) thiết lập chính sách sử dụng cho một zone. Một chính chính sách zone có thể thừa kế một lớp chính sách.

Các tùy chọn có thể được sử dụng trong chính sách:

Trường tùy chọn	Mô tả	Ví dụ
algorithm	Thuật toán dùng để tạo khóa. Nếu không định nghĩa, theo mặc định sẽ là RSASHA256	algorithm rsasha256;
coverage	Khoảng thời gian để đảm bảo rằng các khóa vẫn chính xác; Giá trị sẽ là đơn vị thời gian, mặc định là 6 tháng (6 months)	coverage 1y;
directory	Định nghĩa thư mục sẽ chứa các khóa sau khi tạo ra.	directory “/data/named/keys/vn”;
key-size	Khai báo số bit sử dụng để tạo khóa. Tham số này sử dụng để thiết lập cho cả zsk và ksk, và có thể được thiết lập trong các lớp chính sách khác hoặc trong các chính sách zone.	key-size zsk 1024; key-size ksk 2048;
keyttl	Thời gian sống của khóa. Mặc định là 1	keyttl 1h;

	giờ.	
post-publish	Khoảng thời gian khóa sẽ được xóa sau thời gian inactive của khóa đó. Nếu như tham số roll-period không được thiết lập, thì không cần phải thiết lập giá trị này. Tham số này sử dụng để thiết lập cho cả zsk và ksk, và có thể được thiết lập trong các lớp chính sách khác hoặc trong các chính sách zone. Mặc định khoảng thời gian là 1 tháng.	post-publish zsk 2w; post-publish ksk 2w;
pre-publish	Khoảng thời gian khóa sẽ được công khai trước khi khóa đó được kích hoạt. Nếu như tham số roll-period không được thiết lập, thì không cần phải thiết lập giá trị này. Tham số này sử dụng để thiết lập cho cả zsk và ksk, và có thể được thiết lập trong các lớp chính sách khác hoặc trong các chính sách zone. Mặc định khoảng thời gian là 1 tháng.	pre-publish zsk 2d;
roll-period	Tần suất, chu kỳ khóa được thực hiện rollover. Tham số này sử dụng để thiết lập cho cả zsk và ksk, và có thể được thiết lập trong các lớp chính sách khác hoặc trong các chính sách zone. Nếu giá trị tham số này không được cấu hình, mặc định sẽ là 1 năm đối với ZKS và không thiết lập thời gian cho KSK.	roll-period zsk 3mo;

Dưới đây là một số cấu hình đầy đủ để thiết lập chính sách để tạo khóa cho zone:

```
#/etc/dnssec-policy.conf
policy dnssec-01 {
        algorithm rsasha1;
        coverage 1y;
        roll-period zsk 3mo;
        pre-publish zsk 2w;
        post-publish zsk 2w;
        roll-period ksk 1y;
        keyttl 1h;
        key-size ksk 2048;
        key-size zsk 1024;
};
policy dnssec-02 {
        algorithm rsasha256;
        coverage 1y;
        roll-period zsk 3mo;
        pre-publish zsk 2w;
        post-publish zsk 2w;
        roll-period ksk 1y;
        keyttl 1h;
        key-size ksk 2048;
        key-size zsk 1024;
};

zone example1.vn {
        policy dnssec-01;
};

zone example2.vn {
        policy dnssec-02;
        key-size ksk 511;
};
```

1.2.3. Triển khai thử nghiệm:

Ví dụ: Tạo một chính sách (policy) sử dụng để tạo khóa cho zone ***example.vn*** với cấu hình file ***/etc/policy.conf*** như sau:

Với các thông số:

- Khóa ZSK:
  - Thời gian Pre-publish: 2 ngày
  - Thời gian xóa bỏ khóa: sau khi khóa hết hạn 2 tuần.
  - Chu kỳ roll-over khóa zsk: 3 tháng
  - Kích thước khóa sẽ sử dụng 1024 bit, và thuật toán RSASHA256.
- Khóa KSK:
  - Chu kỳ roll-over khóa zsk: 1 năm
  - Kích thước khóa sẽ sử dụng 2048 bit, và thuật toán RSASHA256.
- Giá trị TTL của các khóa là 1 giờ.

```
policy default-dnssec {
        algorithm rsasha256;
        coverage 1y;
        roll-period zsk 3mo;
        roll-period ksk 1y;
        pre-publish zsk 2d;
        post-publish zsk 2w;
        keyttl 1h;
        key-size zsk 1024;
        key-size ksk 2048;
};
zone example.vn {
        policy default-dnssec;
        directory "/data/named/keys/example_vn";
};
```

Câu lệnh thực hiện:

```
# dnssec-keymgr example.vn -r /dev/urandom -c /etc/dnssec-
policy.conf
```

Kết quả thu được:

```
Kexample.vn.+008+00795.key
Kexample.vn.+008+00795.private
Kexample.vn.+008+04491.key
Kexample.vn.+008+04491.private
Kexample.vn.+008+09366.key
Kexample.vn.+008+09366.private
Kexample.vn.+008+12540.key
Kexample.vn.+008+12540.private
Kexample.vn.+008+13134.key
Kexample.vn.+008+13134.private
```

Bảng chi tiết thông số khóa ZSK:

Khóa	**ID khóa**	**Thời gian Publish**	**Thời gian Activate**	**Thời gian Inactive**	**Thời gian Delete**
ZSK1	12540	14/11/2016	14/11/2016	12/2/2017	26/2/2017
ZSK2	09366	10/2/2017	12/2/2017	13/5/2017	27/2/2017
ZSK3	13134	11/5/2017	13/5/2017	11/8/2017	25/8/2017
ZSK4	04491	9/8/2017	11/8/2017	9/11/2017	23/11/2017
ZSK5	00795	7/11/2017	9/11/2017		

2. Một số ví dụ về các lệnh mở rộng secDNS-1.1

2.1. Mở rộng cho lệnh domain:create

Ví dụ về lệnh *domain:create* sử dụng hình thức dữ liệu bản ghi DS không có thành phần *secDNS:keyData*:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:  <command>
C:    <create>
C:      <domain:create
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:        <domain:period unit="y">2</domain:period>
C:        <domain:ns>
C:          <domain:hostObj>ns1.example.com</domain:hostObj>
C:          <domain:hostObj>ns2.example.com</domain:hostObj>
C:        </domain:ns>
C:        <domain:registrant>jd1234</domain:registrant>
C:        <domain:contact type="admin">sh8013</domain:contact>
C:        <domain:contact type="tech">sh8013</domain:contact>
C:        <domain:authInfo>
C:          <domain:pw>2fooBAR</domain:pw>
C:        </domain:authInfo>
C:      </domain:create>
C:    </create>
C:    <extension>
C:      <secDNS:create
C:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:        <secDNS:maxSigLife>604800</secDNS:maxSigLife>
C:        <secDNS:dsData>
C:          <secDNS:keyTag>12345</secDNS:keyTag>
C:          <secDNS:alg>3</secDNS:alg>
C:          <secDNS:digestType>1</secDNS:digestType>
C:          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
C:        </secDNS:dsData>
C:      </secDNS:create>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Ví dụ về lệnh *domain:create* sử dụng hình thức dữ liệu bản ghi DS có thành phần *secDNS:keyData*:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:  <command>
C:    <create>
C:      <domain:create
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
```

```
C:        <domain:name>example.com</domain:name>
C:        <domain:period unit="y">2</domain:period>
C:        <domain:ns>
C:          <domain:hostObj>ns1.example.com</domain:hostObj>
C:          <domain:hostObj>ns2.example.com</domain:hostObj>
C:        </domain:ns>
C:        <domain:registrant>jd1234</domain:registrant>
C:        <domain:contact type="admin">sh8013</domain:contact>
C:        <domain:contact type="tech">sh8013</domain:contact>
C:        <domain:authInfo>
C:          <domain:pw>2fooBAR</domain:pw>
C:        </domain:authInfo>
C:      </domain:create>
C:    </create>
C:    <extension>
C:      <secDNS:create
C:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:        <secDNS:maxSigLife>604800</secDNS:maxSigLife>
C:        <secDNS:dsData>
C:          <secDNS:keyTag>12345</secDNS:keyTag>
C:          <secDNS:alg>3</secDNS:alg>
C:          <secDNS:digestType>1</secDNS:digestType>
C:          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
C:          <secDNS:keyData>
C:            <secDNS:flags>257</secDNS:flags>
C:            <secDNS:protocol>3</secDNS:protocol>
C:            <secDNS:alg>1</secDNS:alg>
C:            <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
C:          </secDNS:keyData>
C:        </secDNS:dsData>
C:      </secDNS:create>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Ví dụ về lệnh *domain:create* sử dụng hình thức dữ liệu khóa công khai:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:  <command>
C:    <create>
C:      <domain:create
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:        <domain:period unit="y">2</domain:period>
C:        <domain:ns>
C:          <domain:hostObj>ns1.example.com</domain:hostObj>
C:          <domain:hostObj>ns2.example.com</domain:hostObj>
C:        </domain:ns>
C:        <domain:registrant>jd1234</domain:registrant>
C:        <domain:contact type="admin">sh8013</domain:contact>
C:        <domain:contact type="tech">sh8013</domain:contact>
C:        <domain:authInfo>
C:          <domain:pw>2fooBAR</domain:pw>
C:        </domain:authInfo>
C:      </domain:create>
C:    </create>
```

```
C:    <extension>
C:      <secDNS:create
C:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:        <secDNS:keyData>
C:          <secDNS:flags>257</secDNS:flags>
C:          <secDNS:protocol>3</secDNS:protocol>
C:          <secDNS:alg>1</secDNS:alg>
C:          <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
C:        </secDNS:keyData>
C:      </secDNS:create>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

2.2. Mở rộng cho lệnh domain:update

Ví dụ về lệnh *domain:update* sử dụng để thêm và xóa bản ghi DS sử dụng hình thức dữ liệu bản ghi DS:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:  <command>
C:    <update>
C:      <domain:update
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:      </domain:update>
C:    </update>
C:    <extension>
C:      <secDNS:update
C:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:        <secDNS:rem>
C:          <secDNS:dsData>
C:            <secDNS:keyTag>12345</secDNS:keyTag>
C:            <secDNS:alg>3</secDNS:alg>
C:            <secDNS:digestType>1</secDNS:digestType>
C:            <secDNS:digest>38EC35D5B3A34B33C99B</secDNS:digest>
C:          </secDNS:dsData>
C:        </secDNS:rem>
C:        <secDNS:add>
C:          <secDNS:dsData>
C:            <secDNS:keyTag>12346</secDNS:keyTag>
C:            <secDNS:alg>3</secDNS:alg>
C:            <secDNS:digestType>1</secDNS:digestType>
C:            <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
C:          </secDNS:dsData>
C:        </secDNS:add>
C:      </secDNS:update>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Ví dụ sử dụng lệnh *domain:update* để thay đổi thông tin maxSigLife:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
```

```
C:      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:   <command>
C:     <update>
C:       <domain:update
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:         <domain:name>example.com</domain:name>
C:       </domain:update>
C:     </update>
C:     <extension>
C:       <secDNS:update
C:        xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:         <secDNS:chg>
C:           <secDNS:maxSigLife>605900</secDNS:maxSigLife>
C:         </secDNS:chg>
C:       </secDNS:update>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C:</epp>
```

Ví dụ sử dụng lệnh *domain:update* sử dụng để thêm và xóa bản ghi DS sử dụng hình thức dữ liệu khóa công khai và thiết lập maxSigLife:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:   <command>
C:     <update>
C:       <domain:update
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:         <domain:name>example.com</domain:name>
C:       </domain:update>
C:     </update>
C:     <extension>
C:       <secDNS:update
C:        xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:         <secDNS:rem>
C:           <secDNS:keyData>
C:             <secDNS:flags>257</secDNS:flags>
C:             <secDNS:protocol>3</secDNS:protocol>
C:             <secDNS:alg>1</secDNS:alg>
C:             <secDNS:pubKey>AQPJ////4QQQ</secDNS:pubKey>
C:           </secDNS:keyData>
C:         </secDNS:rem>
C:         <secDNS:add>
C:           <secDNS:keyData>
C:             <secDNS:flags>257</secDNS:flags>
C:             <secDNS:protocol>3</secDNS:protocol>
C:             <secDNS:alg>1</secDNS:alg>
C:             <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
C:           </secDNS:keyData>
C:         </secDNS:add>
C:         <secDNS:chg>
C:           <secDNS:maxSigLife>605900</secDNS:maxSigLife>
C:         </secDNS:chg>
C:       </secDNS:update>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C:</epp>
```

Ví dụ về lệnh *domain:update* sử dụng để xóa bản ghi toàn bộ bản ghi DS sử dụng *secDNS:all*:

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

Ví dụ về lệnh *domain:update* với thuộc tính urgent:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:  <command>
C:    <update>
C:      <domain:update
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:      </domain:update>
C:    </update>
C:    <extension>
C:      <secDNS:update urgent="true"
C:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
C:        <secDNS:rem>
C:          <secDNS:all>true</secDNS:all>
C:        </secDNS:rem>
C:        <secDNS:add>
C:          <secDNS:dsData>
C:            <secDNS:keyTag>12346</secDNS:keyTag>
C:            <secDNS:alg>3</secDNS:alg>
C:            <secDNS:digestType>1</secDNS:digestType>
C:            <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
C:          </secDNS:dsData>
C:        </secDNS:add>
C:      </secDNS:update>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

2.3. Mở rộng cho lệnh domain:info

Ví dụ về một phản hồi cho lệnh *domain:info* với hình thức dữ liệu bản ghi DS không có thành phần *secDNS:keyData*:

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
S:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
S:        <domain:name>example.com</domain:name>
S:        <domain:roid>EXAMPLE1-REP</domain:roid>
S:        <domain:status s="ok"/>
S:        <domain:registrant>jd1234</domain:registrant>
S:        <domain:contact type="admin">sh8013</domain:contact>
S:        <domain:contact type="tech">sh8013</domain:contact>
S:        <domain:ns>
S:          <domain:hostObj>ns1.example.com</domain:hostObj>
S:          <domain:hostObj>ns2.example.com</domain:hostObj>
S:        </domain:ns>
S:        <domain:host>ns1.example.com</domain:host>
S:        <domain:host>ns2.example.com</domain:host>
S:        <domain:clID>ClientX</domain:clID>
S:        <domain:crID>ClientY</domain:crID>
S:        <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:        <domain:upID>ClientX</domain:upID>
S:        <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
S:        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
S:        <domain:trDate>2000-04-08T09:00:00.0Z</domain:trDate>
S:        <domain:authInfo>
S:          <domain:pw>2fooBAR</domain:pw>
S:        </domain:authInfo>
S:      </domain:infData>
S:    </resData>
S:    <extension>
S:      <secDNS:infData
S:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
S:        <secDNS:dsData>
S:          <secDNS:keyTag>12345</secDNS:keyTag>
S:          <secDNS:alg>3</secDNS:alg>
S:          <secDNS:digestType>1</secDNS:digestType>
S:          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
S:        </secDNS:dsData>
S:      </secDNS:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Ví dụ về một phản hồi cho lệnh *domain:info* với hình thức dữ liệu bản ghi DS có thành phần *secDNS:keyData*:

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
S:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
S:        <domain:name>example.com</domain:name>
S:        <domain:roid>EXAMPLE1-REP</domain:roid>
S:        <domain:status s="ok"/>
S:        <domain:registrant>jd1234</domain:registrant>
S:        <domain:contact type="admin">sh8013</domain:contact>
S:        <domain:contact type="tech">sh8013</domain:contact>
S:        <domain:ns>
S:          <domain:hostObj>ns1.example.com</domain:hostObj>
S:          <domain:hostObj>ns2.example.com</domain:hostObj>
S:        </domain:ns>
S:        <domain:host>ns1.example.com</domain:host>
S:        <domain:host>ns2.example.com</domain:host>
S:        <domain:clID>ClientX</domain:clID>
S:        <domain:crID>ClientY</domain:crID>
S:        <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:        <domain:upID>ClientX</domain:upID>
S:        <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
S:        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
S:        <domain:trDate>2000-04-08T09:00:00.0Z</domain:trDate>
S:        <domain:authInfo>
S:          <domain:pw>2fooBAR</domain:pw>
S:        </domain:authInfo>
S:      </domain:infData>
S:    </resData>
S:    <extension>
S:      <secDNS:infData
S:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
S:        <secDNS:maxSigLife>604800</secDNS:maxSigLife>
S:        <secDNS:dsData>
S:          <secDNS:keyTag>12345</secDNS:keyTag>
S:          <secDNS:alg>3</secDNS:alg>
S:          <secDNS:digestType>1</secDNS:digestType>
S:          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
S:          <secDNS:keyData>
S:            <secDNS:flags>257</secDNS:flags>
S:            <secDNS:protocol>3</secDNS:protocol>
S:            <secDNS:alg>1</secDNS:alg>
S:            <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
S:          </secDNS:keyData>
S:        </secDNS:dsData>
S:      </secDNS:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
```

```
S:</epp>
```

Ví dụ về một phản hồi cho lệnh *domain:info* với hình thức dữ liệu khóa công khai:

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
S:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
S:        <domain:name>example.com</domain:name>
S:        <domain:roid>EXAMPLE1-REP</domain:roid>
S:        <domain:status s="ok"/>
S:        <domain:registrant>jd1234</domain:registrant>
S:        <domain:contact type="admin">sh8013</domain:contact>
S:        <domain:contact type="tech">sh8013</domain:contact>
S:        <domain:ns>
S:          <domain:hostObj>ns1.example.com</domain:hostObj>
S:          <domain:hostObj>ns2.example.com</domain:hostObj>
S:        </domain:ns>
S:        <domain:host>ns1.example.com</domain:host>
S:        <domain:host>ns2.example.com</domain:host>
S:        <domain:clID>ClientX</domain:clID>
S:        <domain:crID>ClientY</domain:crID>
S:        <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:        <domain:upID>ClientX</domain:upID>
S:        <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
S:        <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
S:        <domain:trDate>2000-04-08T09:00:00.0Z</domain:trDate>
S:        <domain:authInfo>
S:          <domain:pw>2fooBAR</domain:pw>
S:        </domain:authInfo>
S:      </domain:infData>
S:    </resData>
S:    <extension>
S:      <secDNS:infData
S:       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
S:        <secDNS:keyData>
S:          <secDNS:flags>257</secDNS:flags>
S:          <secDNS:protocol>3</secDNS:protocol>
S:          <secDNS:alg>1</secDNS:alg>
S:          <secDNS:pubKey>AQPJ////4Q==</secDNS:pubKey>
S:        </secDNS:keyData>
S:      </secDNS:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

3. Những câu hỏi thường gặp về DNSSEC

3.1. DNSSEC là gì?

Trả lời: DNSSEC là công nghệ an toàn mở rộng cho hệ thống DNS. Trong đó DNSSEC sẽ cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau và xác thực cho từng zone dữ liệu để đảm bảo toàn vẹn dữ liệu và tăng tính an toàn cho các hoạt động như các trình duyệt Internet và Email, DNSSEC đảm bảo rằng bạn sẽ truy cập vào đúng tên miền mà bạn thực sự muốn, ngăn chặn các hoạt động độc hại nguy hiểm đến dữ liệu DNS.

3.2. Nguyên lý hoạt động của DNSSEC?

Trả lời: DNSSEC sử dụng cơ chế mã hóa khóa bất đối xứng (cặp khóa công cộng/khóa riêng) để ký dữ liệu DNS, tất cả các bản ghi tài nguyên tên miền trong các Zone DNS được ký số và công khai cùng với các chữ ký của chúng. Các khóa công cộng được công khai trên hệ thống DNS.

DNSSEC sử dụng một mô hình tin cậy và chuỗi tin cậy này đi từ zone cha đến các zone con. Các zone cấp cao (zone cha) ký hay xác minh cho các khóa công cộng của các zone cấp dưới (zone con), các máy chủ tên miền có thẩm quyền đối với các zone này có thể được quản lý bởi các NĐK, ISP, DNS Hosting, …

Khi một người dùng cuối muốn truy cập vào một trang web, một trình phân giải trên máy tính người dùng sẽ yêu cầu bản ghi tên miền đến máy chủ đệ quy (đặt tại ISP). Sau khi máy chủ yêu cầu bản ghi này, nó cũng yêu cầu "khóa" DNSSEC liên quan đến zone đó. "Khóa" này cho phép các máy chủ sử dụng để xác minh các thông tin mà nó nhận được là giống với các bản ghi trên máy chủ tên miền có thẩm quyền.

Nếu máy chủ đệ quy xác nhận rằng các bản ghi tên miền đã được gửi đi bởi các máy chủ có thẩm quyền và không bị thay đổi trong quá trình vận chuyển, nó sẽ phân giải tên miền và người dùng có thể truy cập vào trang web. Quá trình này được gọi là quá trình xác thực, và nếu bản ghi tài nguyên bị thay đổi hoặc từ nguồn không xác định, máy chủ đệ quy sẽ không cho phép người dùng truy cập vào địa chỉ giả mạo đó. DNSSEC cũng có thể chứng mình rằng một tên miền không tồn tại.

3.3. DNSSEC có mã hóa các phản hồi truy vấn hay không?

Trả lời: DNSSEC không mã hóa các phản hồi truy vấn DNS, nó chỉ thêm một chữ ký được mã hóa và được xác mình bằng cách sử dụng hệ thống khóa riêng và khóa công khai.

3.4. Các lợi ích của DNSSEC?

Trả lời: DNSSEC đã được phát triển để cung cấp chứng thực và toàn vẹn dữ liệu cho DNS giảm thiểu các mối đe dọa như DNS giả mạo, đầu độc bộ nhớ cache, các phân giải chứa mã độc hại, sửa đổi làm sai lệch dữ liệu DNS.

Một ví dụ về những lợi ích mà DNSSEC cung cấp là các chủ sở hữu của các trang web và các máy chủ Mail đã triển khai DNSSEC, sẽ đạt được mực độ an toàn cao hơn và chắc chắn rằng khi truy cập vào trang web hay email của họ sẽ không bị chuyển hướng đến nơi khác. Do vậy việc triển khai DNSSEC sẽ mang lại một số lợi ích khác như:

- Giúp bảo vệ, xây dựng thương hiệu và tăng sự uy tín của bạn đối với người sử dụng.
- Bảo vệ chính công việc của bạn bằng cách tăng cường độ tin cậy trong Internet.
- Cung cấp dịch vụ Internet an toàn hơn cho người dùng.

3.5. DNSSEC bảo vệ người dùng Internet như thế nào?

Trả lời: DNSSEC được thiết kế để bảo vệ người dùng trên Internet từ những dữ liệu DNS giả mạo, ví dụ như những địa chỉ đích không chính xác hoặc chữa mã độc hại. Đây là sự khác biệt giữa truy vấn có nhận thực DNSSEC và không nhận thực DNSSEC.

3.6. DNSSEC có làm tăng số lượng truy vấn?

Trả lời: DNSSEC có thể làm tăng số lượng truy vấn, do thực hiện quá trình phân giải tìm kiếm thông tin xác nhận của các tên miền con trong chuỗi xác thực.

3.7. DNSSEC có làm ảnh hưởng đến tốc độ truy vấn tên miền?

Trả lời: Truy vấn có DNSSEC phải thực hiện thêm quá trình xác thực, do vậy làm cho tốc độ truy vấn tên miền bị ảnh hưởng và tốn nhiều thời gian hơn. Nhưng đối với những hệ thống có Cache (bộ nhớ đệm) thì DNSSEC ảnh hưởng đến quá trình truy vấn lần đầu

tiên, còn đối với những lần truy vấn tiếp theo (chưa bị xóa cache) sẽ không ảnh hưởng đến tốc độ truy vấn do lấy thông tin từ bộ nhớ đệm.

3.8. Các đối tượng nào trong triển khai DNSSEC?

Trả lời: Các đối tượng trong triển khai DNSSEC:

- Nhà quản lý, cấp phát tên miền (Registries)
- Các nhà đăng ký tên miền (Registrars)
- Các nhà cung cấp dịch vụ Internet (ISPs)
- Các nhà cung cấp dịch vụ DNS Hosting, Web Hosting
- Các nhà cung cấp phần cứng và phần mềm
- Các cơ quan chính phủ
- Người dùng Internet

3.9. Làm sao để triển khai DNSSEC cho tên miền của tôi?

Trả lời: Khi bạn triển khai DNSSEC cho tên miền của bạn, nó được gọi là "ký" tên miền. Bạn có thể liên hệ đến NĐK tên miền .vn của bạn để xem nếu họ cung cấp dịch vụ DNSSEC, hoặc bạn có thể liên hệ với một tổ chức điều hành DNS bên thứ 3 có thể cung cấp dịch vụ DNSSEC.

3.10. Chi phí để triển khai DNSSEC như thế nào?

Trả lời:

- Đối với các nhà cung cấp dịch vụ DNS (như DNS Hosting, Resgistrars, Registries): Để triển khai DNSSEC thường chiếm chi phí lớn hơn, do có thể phải đầu tư vào các thiết bị, phần mềm dùng để "ký" và vận hành DNSSEC, cũng như việc tăng cường nâng cấp về hạ tầng mạng và các máy chủ dịch vụ để đảm bảo yêu cầu tốc độ xử lý cao hơn, băng thông lớn hơn và dung lượng bộ nhớ lớn hơn.
- Đối với các nhà cung cấp dịch vụ Internet (ISP): Việc triển khai DNSSEC trên các ISP (sự xác thực DNSSEC) thường chiếm chi phí là thấp đến rất thấp. Nó đòi hỏi ít hoặc không cần thiết phải đầu tư nhiều về phần cứng hay phần mềm, mà chỉ đòi hỏi một sự đầu tư nhỏ về thời gian cho bộ phận quản trị hệ thống của các ISP. Và đảm bảo một số yêu cầu về hạ tầng mạng và các máy chủ dịch vụ để đảm bảo yêu cầu tốc độ xử lý cao hơn, băng thông lớn hơn và dung lượng bộ nhớ lớn hơn.

3.11. Người dùng có cần cài đặt phần mềm nào để dùng được DNSSEC?

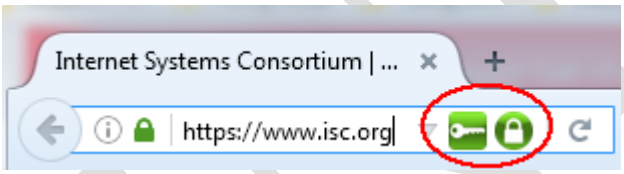
Trả lời: Người dùng nên cài đặt thêm một phần mềm "plug in" trên các trình duyệt của mình để xác thực dữ liệu DNSSEC.

- Ví dụ: Trình duyệt Mozilla Firefox có "plug in" tạo ra một trình duyệt có khả năng nhận thực DNSSEC là DNSSEC/TLSA Validator

3.12. Làm thế nào để biết tên miền của tôi đã được ký DNSSEC?

Trả lời: Để kiểm tra tên miền của bạn đã được ký DNSSEC hay chưa thì có thể sử dụng một số cách sau:

- Kiểm tra trực tuyến trên trang web: http://dnssec-debugger.verisignlabs.com/
- Kiểm tra bằng trình duyệt Firefox: khi sử dụng "plug in" DNSSEC/TLSA Validator, nếu tên miền của bạn đã được ký DNSSEC thì sẽ xuất hiện một biểu tượng nhỏ "chìa khóa màu xanh" trên trình duyệt.



3.13. Các thuật ngữ thường được sử dụng trong DNSSEC

Trả lời:

- DNSSEC (Domain Name System Security Extensions)
- DNSKEY (DNS Public Key): Bản ghi khóa công cộng DNS
- DS (Delegation Signer): Bản ghi ký ủy quyền
- KSK (Key Signing Key): Khóa sử dụng để ký khóa ZSK
- ZSK (Zone Signing Key): Khóa sử dụng để ký Zone
- NSEC (Next Secure): Bản ghi bảo mật kế tiếp
- RRSIG (Resource Record Signature): Bản ghi chữ ký tài nguyên.

Chỉ đạo biên soạn:

Ông Nguyễn Hồng Thắng – Phó Giám đốc VNNIC

Nhóm biên soạn:

Ông Nguyễn Trường Thành – Trưởng phòng Kỹ thuật

Ông Nguyễn Trung Kiên – Phó trưởng phòng Kỹ thuật

Ông Nguyễn Huy Bắc – Chuyên viên

Ông Nguyễn Văn Trí – Chuyên viên