BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

DNSSEC.vn

TÀI LIỆU

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC NHÀ ĐĂNG KÝ TÊN MIỀN

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

DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT

ccTLD	Country Code Top Level Domain
DNS	Domain Name System
DNSKEY	Domain Name System KEY
DNSSEC	Domain Name System Security Extensions
DS	Delegation Signer
EPP	Extensible Provisioning Protocol
gTLD	Generic Top-level Domain
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDC	Internet Data Center
IPv6	Internet Protocol Version 6
ISP	Doanh nghiệp Internet
KSK	Key Signing Key
NĐK	Nhà đăng ký
NSEC	Next Secure
RFC	Request for Comments
RRSIG	Resource Record Signature
SRS	Shared Registry System
TLD	Top Level Domain
VNNIC	Vietnam Internet Network Information Center
ZSK	Zone Signing Key

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Hệ thống DNS đóng vai trò dẫn đường trên Internet, được coi là một hạ tầng lõi trọng yếu của hệ thống Internet toàn cầu. Do tính chất quan trọng của hệ thống DNS, đã có nhiều cuộc tấn công, khai thác lỗ hổng của hệ thống này với quy mô lớn và tinh vi với mục đích làm tê liệt hệ thống này hoặc chuyển hướng một tên miền nào đó đến một địa chỉ IP khác. Trên thế giới từ nhiều năm đã có nhiều cuộc tấn công làm thay đổi dữ liệu tên miền, chuyển hướng website được thực hiện, gây hậu quả nghiêm trọng.

Để giải quyết các nguy cơ ở trên, ngay từ năm 1990, các giải pháp khắc phục đã được nghiên cứu. Năm 1995, giải pháp DNSSEC được công bố và tới năm 2001 thì được xây dựng thành các tiêu chuẩn RFC dự thảo, và cuối cùng được IETF chính thức công bố thành tiêu chuẩn RFC vào năm 2005.

DNSSEC dựa trên nền tảng mã hoá khoá công khai (PKI) tương tự hệ thống chứng thực điện tử (CA), thực hiện ký số trên các bản ghi DNS để đảm bảo tính xác thực, toàn vẹn của cặp ánh xạ tên miền – địa chỉ IP, tất cả các thay đổi bản ghi DNS đã được ký số sẽ được phát hiện.

Kể từ khi được chuẩn hoá năm 2005, DNSSEC đã nhanh chóng được triển khai rộng rãi trên mạng Internet. Tại Việt Nam, việc triển khai áp dụng tiêu chuẩn DNSSEC cho hệ thống máy chủ tên miền (DNS) ".VN" sẽ giúp đảm bảo chính xác, tin cậy việc sử dụng, truy vấn tên miền ".VN" trên Internet thông qua việc áp dụng thống nhất tiêu chuẩn DNSSEC đối với các hệ thống DNS ".VN". Đảm bảo kết nối liên thông theo tiêu chuẩn DNSSEC giữa hệ thống DNS quốc gia ".VN" với hệ thống máy chủ tên miền gốc (DNS ROOT) và các hệ thống DNS quốc tế. Đánh dấu bước chuyển biến quan trọng trong việc phát triển hạ tầng Internet tại Việt Nam, sẵn sàng đẩy mạnh phát triển các dịch vụ thương mại điện tử, chính phủ điện tử tại Việt Nam một cách an toàn nhất.

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC NĐK

1. Nhà đăng ký tên miền .VN:

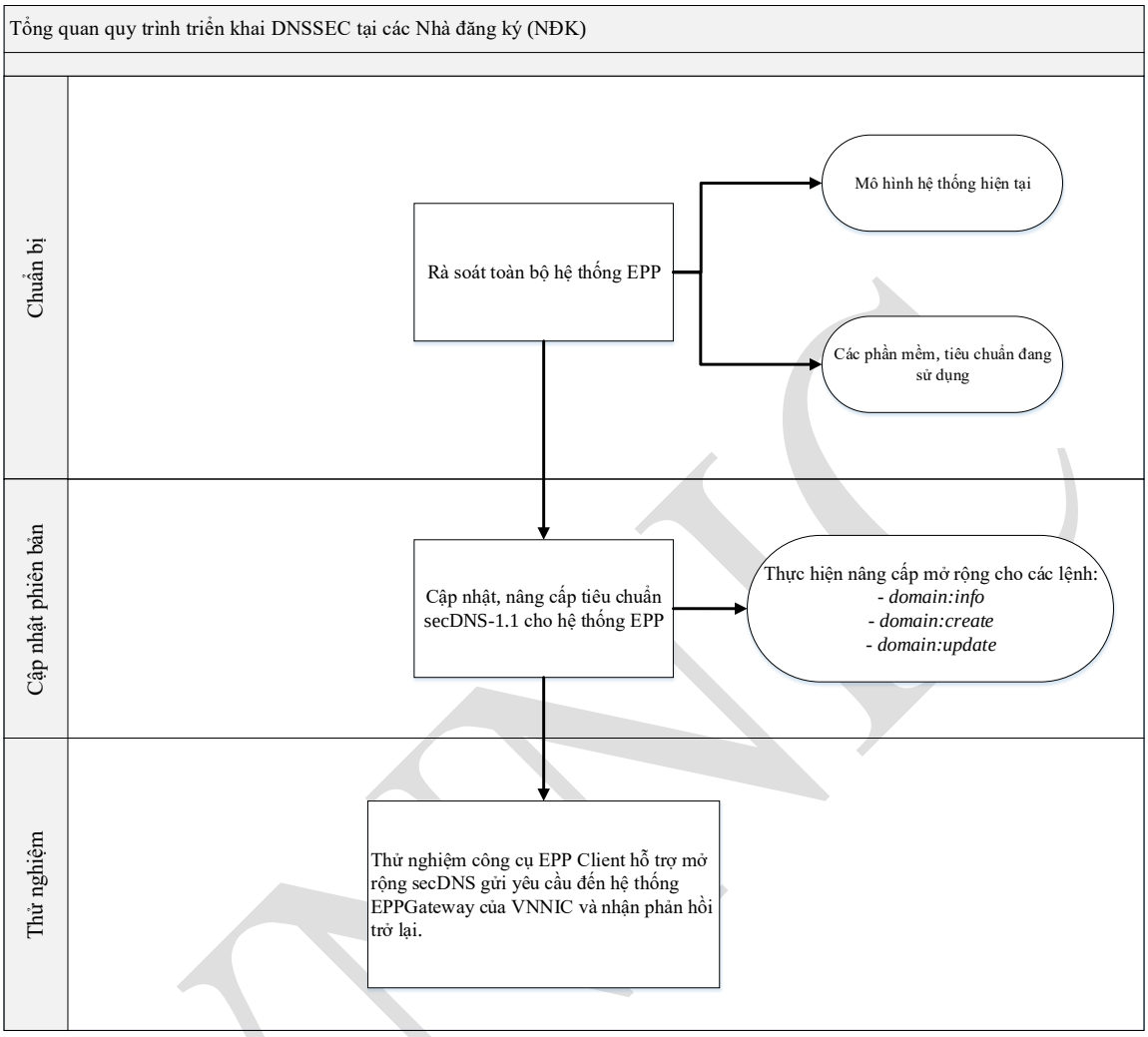
Các nhà đăng ký tên miền .VN là các đơn vị đã ký kết thỏa thuận với VNNIC cho dịch vụ đại lý đăng ký tên miền .VN. Các nhà đăng ký sẽ thực hiện các tác nghiệp liên quan đến cập nhật các bản ghi tên miền, đăng ký thông tin tên miền lên hệ thống quản lý của VNNIC. Trong triển khai DNSSEC, chủ yếu là cập nhật thông tin của bản ghi ký chuyển giao DS tương ứng trong zone VN.

2. Phân tích, đánh giá vai trò

Đối với các Nhà đăng ký tên miền ".VN", với vai trò được chia sẻ quyền quản lý đối với tên miền ".VN" theo mô hình Shared Registry System (SRS), sẽ cần thiết lập kênh kết nối liên thông để thực hiện cung cấp thông tin và tiến hành cập nhật bản ghi ký ủy quyền cho tên miền (DS) lên hệ thống DNS Quốc gia để tạo thành chuỗi tin cậy từ hệ thống DNS Root tới hệ thống DNS Quốc gia và máy chủ DNS của tên miền.

3. Quy trình triển khai DNSSEC

3.1. Tổng quan quy trình thực hiện



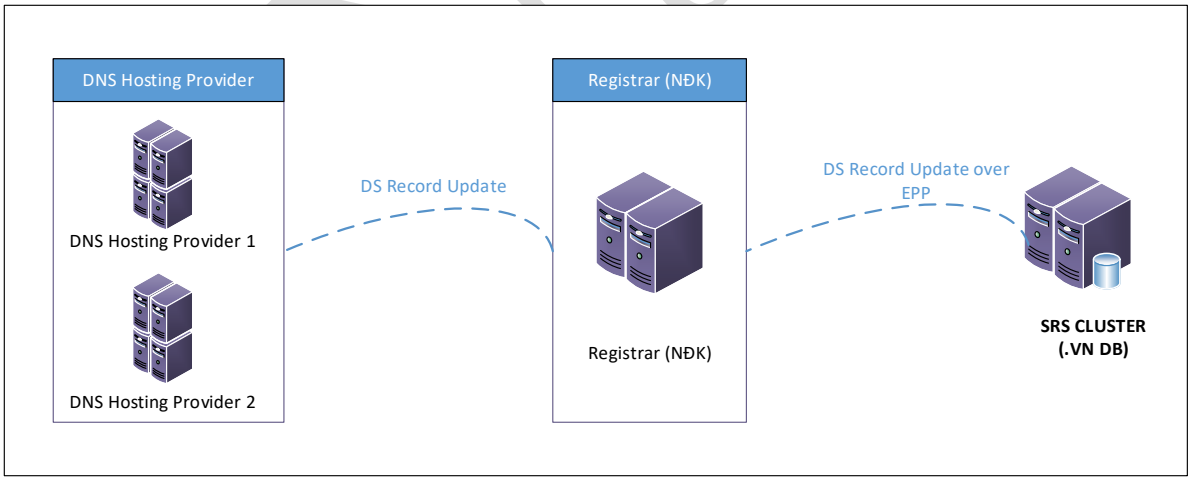
3.2. Các yêu cầu trước khi triển khai

Công việc chính của triển khai thử nghiệm DNSSEC trên hệ thống của các nhà đăng ký là nâng cấp phần mềm, giúp hỗ trợ quản lý và cập nhật bản ghi DS lên hệ thống DNS quốc gia, thông qua chuẩn giao thức EPP hoặc các kênh truyền bảo mật.

Đứng ở vai trò Nhà đăng ký và cũng là đơn vị cung cấp dịch vụ DNS Hosting, các hệ thống sẽ triển khai bao gồm:

- Hệ thống DNS: thực hiện việc ký zone tên miền đang quản lý, cập nhật bản ghi ký chuyển giao DS lên hệ thống DNS quốc gia, tiến hành thử nghiệm các tính năng như quản lý khóa, DNSSEC Inline-signing, key rollover.
- Hệ thống EPPClient: triển khai công cụ EPP Client hỗ trợ mở rộng secDNS để thực hiện gửi yêu cầu đến hệ thống EPPGateway của VNNIC và nhận phản hồi trở lại.
- Hệ thống EPPGateway: Hệ thống EPPGateway với vai trò tiếp nhận các xử lý các request từ các EPP Client của các DNS Hosting Provider sẽ phải thực hiện điều chỉnh:
    - Cập nhật cấu trúc CSDL để lưu trữ thêm các thông tin của tên miền liên quan đến bản ghi DS.
    - Cập nhật Module thực hiện validate dữ liệu bản tin EPP hỗ trợ mở rộng secDNS-1.1.
    - Cập nhật logic xử lý các lệnh bị thay đổi khi áp dụng mở rộng secDNS-1.1 và các lệnh sẽ sinh ra tác động lên DNS quốc gia bao gồm: domain:info, domain:create, domain:update và domain:delete.

3.3. Mô hình triển khai



Hình 1: Mô hình triển khai DNSSEC trên NĐK

Nguyên lý hoạt động:

Khi một tên miền được ký DNSSEC tại các DNS Hosting Provider hoặc trên hệ thống DNS của các nhà đăng ký, bản ghi DS cần được tạo ra và cập nhật gửi lên các nhà đăng ký. Nhà đăng ký giúp hỗ trợ quản lý và cập nhật bản ghi DS lên hệ thống DNS quốc gia, thông qua chuẩn giao thức EPP hoặc các kênh truyền bảo mật để hoàn thành chuỗi tin cậy.

3.4. Những thay đổi, ảnh hưởng

Mở rộng trên giao thức EPP dùng cho việc quản lý các thông tin của tên miền để hỗ trợ tiêu chuẩn DNSSEC được đặc tả trong tài liệu RFC 5910 được công bố vào tháng 5 năm 2010. Trong tài liệu RFC này, mở rộng secDNS phiên bản 1.1 được mô tả bao gồm các thông tin bổ sung cho đối tượng tên miền và các điều chỉnh đến các lệnh và phản hồi áp dụng đối với đối tượng tên miền đã được đặc tả tại RFC 5731. Tài liệu RFC 5910 ra đời để thay thế cho tài liệu RFC 4310 (đặc tả mở rộng secDNS phiên bản 1.0 áp dụng cho đối tượng tên miền trong RFC 3731) đã quá hạn.

Mở rộng secDNS-1.1 được sử dụng để thiết lập chứng thực giữa các zone dữ liệu của Registry và Registrar, theo đó thiết lập chuỗi tin cậy trong DNSSEC từ zone của Registry đến zone của Registrar, song song với việc chuyển giao DNS giữa 2 tổ chức này.

Để thực hiện được việc đó, mở rộng secDNS-1.1 bổ sung các thông tin liên quan đến bản ghi DS cho đối tượng tên miền và các thay đổi lên tập lệnh của đối tượng tên miền để tạo và quản lý các thông tin đó. Cụ thể mở rộng secDNS-1.1 đặc tả:

- Thông tin về bản ghi DS qua 2 hình thức: dữ liệu bản ghi DS và dữ liệu khóa công khai KSK.
- Thông tin về thời gian sống tối đa của chữ ký (maxSigLife): là thời gian tồn tại của bản ghi RRSIG ký trên bản ghi DS tại zone của Registry.
- Thay đổi đối với phản hồi của lệnh *domain:info*
- Thay đổi đối với lệnh *domain:create*
- Thay đổi đối với lệnh *domain:update*
- Các lệnh khác áp dụng cho đối tượng tên miền không bị thay đổi.

Để cung cấp thông tin về bản ghi DS cho tên miền, Registrar có thể sử dụng một trong hai hình thức:

- Thông tin dữ liệu bản ghi DS (DS Data Interface): với hình thức này, Registrar sẽ chịu trách nhiệm cho việc tạo bản ghi DS và cung cấp thông tin đó cho Registry. Cụ thể Registrar sẽ lựa chọn giải thuật băm và thực hiện giải thuật đó để lấy giá trị băm cho khóa công khai KSK của tên miền. Hình thức này cũng hỗ trợ việc Registrar cung cấp thêm thông tin về khóa công khai bên cạnh thông tin về bản ghi DS cho Registry.
- Thông tin dữ liệu khóa công khai (Key Data Interface): với hình thức này, Registrar sẽ chỉ cung cấp thông tin về khóa công khai cho Registry. Việc lựa chọn giải thuật băm và tiến hành giải thuật đó để có giá trị băm cho khóa công khai được Registry thực hiện.

Đặc tả secDNS-1.1 chỉ ra, Registry có thể hỗ trợ cả hai hình thức về thông tin dữ liệu cho bản ghi DS trên, tuy nhiên trong một lệnh hoặc phản hồi EPP thì chỉ sử dụng một hình thức. Ngoài ra, ngoại trừ trong quá trình chuyển đổi, Registry chỉ được hỗ trợ một trong hai hình thức trên đối với một đối tượng tên miền.

Mở rộng cho lệnh domain:create

Lệnh *domain:create* được sử dụng để tạo mới một đối tượng tên miền (nghiệp vụ đăng ký tên miền) với các thông tin được đặc tả trong RFC 5731. Mở rộng secDNS-1.1 bổ sung thêm thành phần secDNS:create để cung cấp các thông tin về bản ghi DS cho tên miền. Thành phần *secDNS:create* là thành phần con và bắt buộc của thành phần extension trong lệnh *domain:create.* Thành phần này bao gồm các thành phần con sau đây:

- Một thành phần không bắt buộc *secDNS:maxSigLife.* Trong trường hợp Registry không hỗ trợ thành phần *secDNS:maxSigLife* và trong lệnh *domain:create* của Registrar có thành phần này thì phản hồi với mã 2102 sẽ được trả lại.

- Không hoặc nhiều thành phần *secDNS:dsData* hoặc *secDNS:keyData,* tuy nhiên không được sử dụng cả 2 hình thức.

Mở rộng cho lệnh domain:update

Lệnh *domain:update* được sử dụng để thay đổi các thuộc tính của đối tượng domain. Bên cạnh các thành phần của lệnh được mô tả trong RFC 5721, mở rộng secDNS-1.1 bổ sung thành phần *secDNS:update,* là một thành phần bắt buộc của thành phần *extension* để thực hiện thay đổi các thông tin liên quan đến các bản ghi DS gắn với tên miền đó.

Thành phần *secDNS:update* có thể bao gồm các thành phần:

- *secDNS:add để* thêm bản ghi DS cho tên miền
- *secDNS:rem* để xóa bản ghi DS gắn với tên miền
- *secDNS:chg* để thay đổi thông tin về thời gian sống tối đa của chữ ký cho các bản ghi DS hiện tại.

Mở rộng cho lệnh domain:info

Khi một lệnh domain:info được thực hiện thành công, trong bản tin phản hồi của Registry, thành phần domain:resData phải chứa các thông tin về đối tượng tên miền như đặc tả trong RFC 5731. Thêm vào đó, mở rộng secDNS-1.1 sẽ bổ sung thêm thành phần mở rộng cho phản hồi này bằng việc cung cấp thành phần secDNS:infData để cung cấp thông tin về các bản ghi DS cho tên miền đó (nếu đã sử dụng DNSSEC) theo một trong hai hình thức được quy định bởi chính sách của Registry.

Thành phần secDNS:infData có chứa các thành phần con sau đây:

- Một thành phần không bắt buộc *secDNS:maxSigLife*
- Một hoặc nhiều các thành phần *secDNS:dsData* hoặc *secDNS:keyData* chứa thông tin về các bản ghi DS của tên miền đó. Tuy nhiên không được sử dụng cả 2 hình thức.

Nội dung của thành phần secDNS:dsData

Khi tạo hoặc thay đổi bản ghi DS cho một tên miền, thông tin các trường dưới đây phải được thiết lập trong thành phần secDNS:dsData cho mỗi bản ghi DS:

- keyTag: Giá trị Key Tag của bản ghi DS
- alg: Thuật toán được dùng trong bản ghi DS
- digestType: Định nghĩa các thuật toán được sử dụng để xây dựng trường Digest cho bản ghi DS
- digest: Chuỗi mã hóa của bản ghi DS

Các trường trên được mô tả chi tiết trong RFC 4034.

Nếu thông tin cung cấp về bản ghi DS không đầy đủ hoặc không chính xác, thì sẽ dẫn đến các hoạt động khởi tạo hoặc cập nhật tên miền bị thất bại và các thông báo lỗi sẽ chứa một mã lỗi chỉ ra các nguyên nhân gây ra lỗi trên.

3.5. Các bước triển khai, thử nghiệm

Trên hệ thống DNS của Nhà đăng ký:

- Tiến hành tạo zone cho tên miền example.vn.
- Tạo cặp khóa KSK và ZSK và cập nhật bản ghi DNSKEY tương ứng vào zone example.vn.
- Tiến hành ký zone với cặp khóa KSK và ZSK đã tạo.
- Tạo bản ghi DS từ zone example.vn.

Trên hệ thống Registrar Client của Nhà đăng ký:

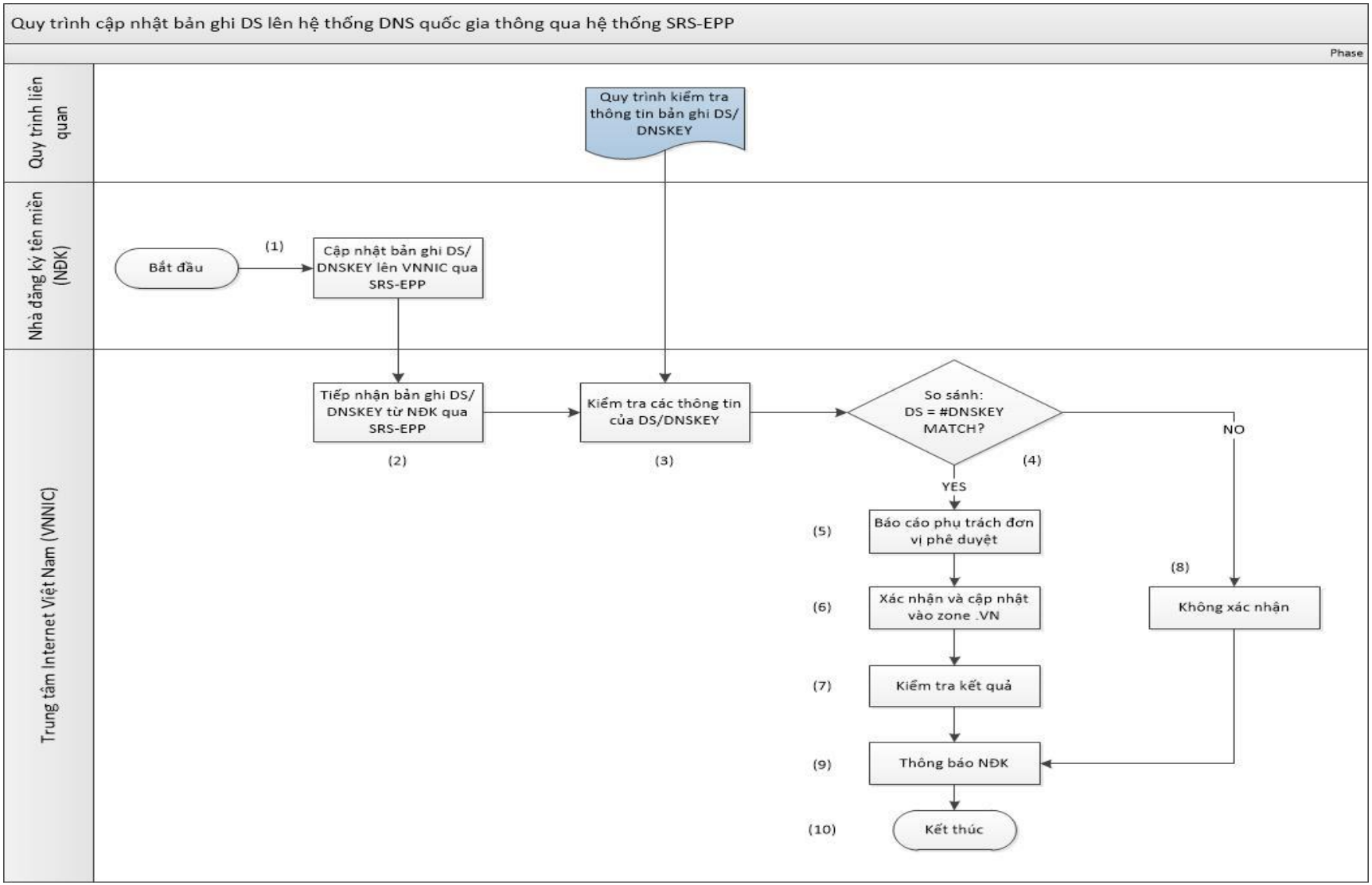
- Thực hiện tạo bản tin lệnh domain:create với thông tin bản ghi DS và DNSKEY lấy từ bước 1.
- Request lên hệ thống EPP Gateway Server.

3.6. Quy trình tiếp nhận, xử lý bản ghi DS

Việc cập nhật các bản ghi DS của tên miền trên hệ thống DNS quốc gia là một quá trình cần thực hiện cẩn thận, tuân thủ theo đúng quy trình, vì nếu dữ liệu sai lệch sẽ dẫn đến việc hoạt động của tên miền sẽ bị gián đoạn. Do đó, nhóm triển khai DNSSEC của VNNIC đã xây dựng lên một quy trình cho việc ký chuyển giao tên miền .vn lên hệ thống DNS quốc gia. Theo đó sau khi có được thông tin cập nhật từ phía Nhà đăng ký cho các dữ liệu bản ghi DS của tên miền, VNNIC sẽ tiến hành kiểm tra, xác thực và ký chuyển giao bản ghi DS do các nhà đăng ký gửi lên. Quá trình hoàn tất, các tên miền .vn mà đã gửi bản ghi chuyển giao DS lên DNS quốc gia sẽ được ký xác thực trên hệ thống.

3.6.1. Quy trình cập nhật bản ghi DS lên hệ thống DNS quốc gia thông qua hệ thống SRS-EPP

- Lưu đồ quy trình


Quy trình cập nhật bản ghi DS lên hệ thống DNS quốc gia thông qua hệ thống SRS-EPP
Phase
Quy trình liên quan
Nhà đăng ký tên miền (NĐK)
Trung tâm Internet Việt Nam (VNNIC)
Quy trình kiểm tra thông tin bản ghi DS/ DNSKEY
Bắt đầu
(1)
Cập nhật bản ghi DS/ DNSKEY lên VNNIC qua SRS-EPP
Tiếp nhận bản ghi DS/ DNSKEY từ NĐK qua SRS-EPP
(2)
Kiểm tra các thông tin của DS/DNSKEY
(3)
So sánh: DS = #DNSKEY MATCH?
(4)
NO
YES
(5)
Báo cáo phụ trách đơn vị phê duyệt
(6)
Xác nhận và cập nhật vào zone .VN
(7)
Kiểm tra kết quả
(8)
Không xác nhận
(9)
Thông báo NĐK
(10)
Kết thúc

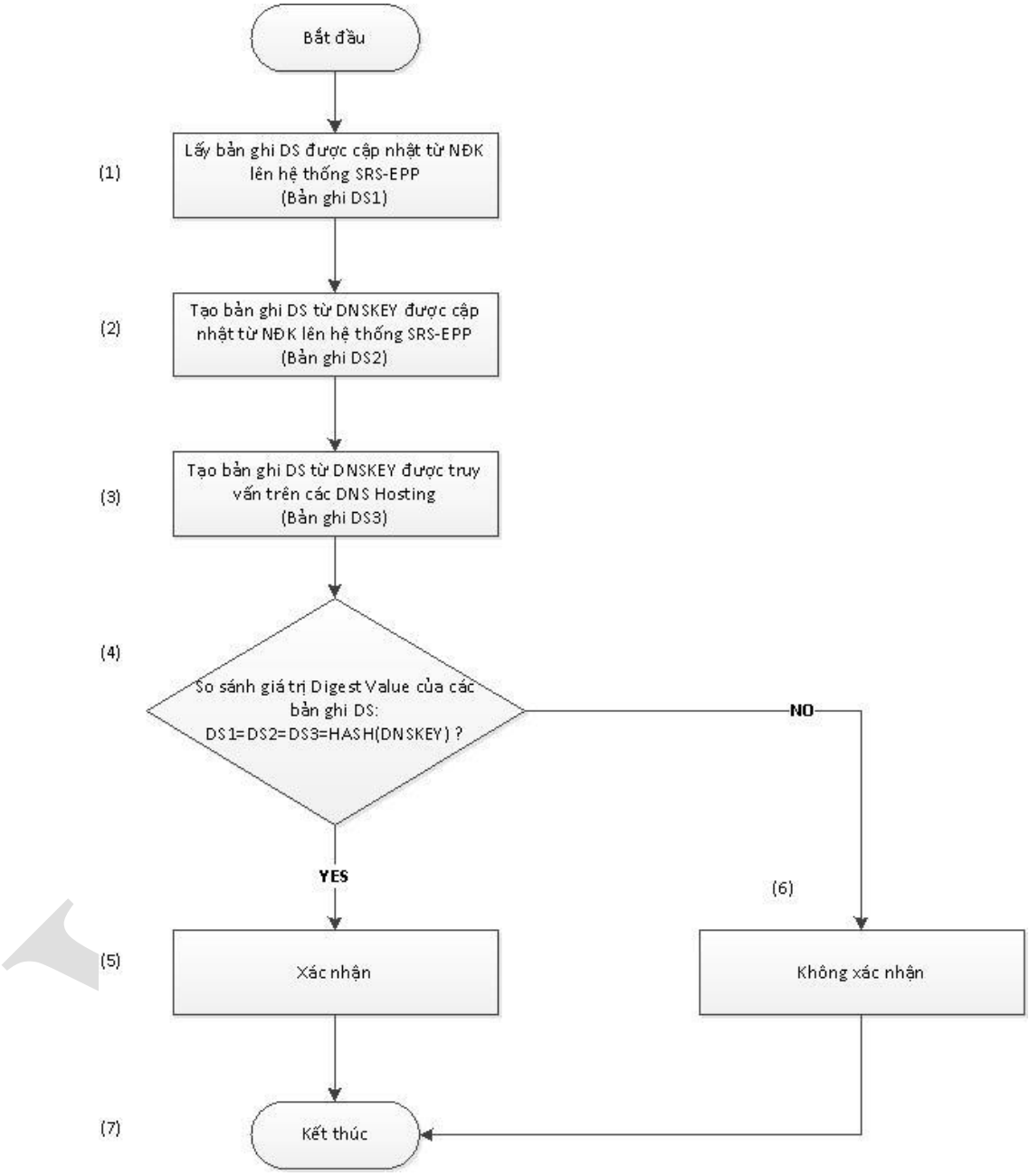
- Mô tả quy trình:

Bước	Nội dung	Người thực hiện	Thời gian	Hướng dẫn chi tiết
(1)	Cập nhật bản ghi DS/DNSKEY thông qua SRS-EPP	Các cán bộ quản trị hệ thống DNS của NĐK	Sau khi đã thực hiện ký DNSSEC trên DNS Hosting.	Thông tin yêu cầu cơ bản cần có khi cập nhật: - Bản ghi DS: + KeyTag + Alg + DigestType + DigestValue - Bản ghi DNSKEY: + KeyTag + KeyProtocol + Alg + KeyValue
(2)	Tiếp nhận các bản ghi DS/DNSKEY thông qua SRS-EPP	Hệ thống SRS-EPP tự động tiếp nhận các thông tin yêu cầu	Ngay khi NĐK gửi yêu cầu cập nhật bản ghi.	- Hệ thống sẽ gửi thông báo các quản trị hệ thống DNS quốc gia ngay khi có yêu cầu cập nhật bản ghi DS/DNSKEY
(3)	Kiểm tra các thông tin của các bản ghi DS/DNSKEY	Tool công cụ kiểm tra thông tin bản ghi DS/DNSKEY	Sau khi hệ thống đã tiếp nhận yêu cầu cập nhật bản ghi DS/DNSKEY	- Các bước thực hiện chi tiết trong quy trình "Quy trình kiểm tra thông tin các bản ghi DS/DNSKEY"
(4)	So sánh, xác thực chính xác các bản ghi DS/DNSKEY	Công cụ kiểm tra thông tin DS/DNSKEY	Sau khi hệ thống đã tiếp nhận yêu cầu cập nhật bản ghi DS/DNSKEY	Tiêu chí kiểm tra: - Kiểm tra các thông tin của bản ghi DS: + KeyTag + Alg + DigestType + DigestValue = HASH(DNSKEY) - Nếu trùng khớp chuyển sang bước (5)

Bước	Nội dung	Người thực hiện	Thời gian	Hướng dẫn chi tiết
				- Nếu không trùng khớp chuyển sang bước (8)
(5)	Báo cáo phụ Lãnh đạo phê duyệt cập nhật.	Cán bộ quản trị hệ thống DNS quốc gia	Sau khi kiểm tra, xác thực thông tin DS thành công	- Báo cáo Lãnh đạo đồng ý phê duyệt cập nhật bản ghi DS lên hệ thống DNS quốc gia.
(6)	Xác nhận, cập nhật DS vào zone .VN	Cán bộ quản trị hệ thống DNS quốc gia	Sau khi được phê duyệt	- Thực hiện thao tác confirm xác nhận thông tin bản ghi DS và cập nhật vào zone .VN
(7)	Kiểm tra kết quả	Các cán bộ quản trị hệ thống DNS	Sau khi cập nhật DS vào zone .VN	- Các cán bộ tiến hành các bước sau: + Truy vấn hỏi bản ghi DS của tên miền tương ứng trên hệ thống DNS quốc gia (truy vấn có DNSSEC) + Truy vấn hỏi DNSSEC Validation (DNS Cache Google, …) kiểm tra xác thực DNSSEC
(8)	Không xác nhận	Cán bộ quản trị hệ thống DNS quốc gia	Sau khi so sánh, xác thực chính xác các bản ghi DS/DNSKEY	
(9)	Thông báo NĐK	Cán bộ quản trị hệ thống DNS quốc gia	Sau các bước kiểm tra, xác thực thông tin bản ghi DS/DNSKEY	- Cán bộ quản trị thông báo cho NĐK: + Thông báo cập nhật thành công: Nếu cập nhật thành công bản ghi DS lên hệ thống DNS quốc gia, hoàn thành chuỗi xác thực DNSSEC. + Thông báo cập nhật thất bại: Nếu các thông tin bản ghi DS/DNSKEY không chính xác.
(10)	Kết thúc			

3.6.2. Quy trình kiểm tra các thông tin bản ghi DS/DNSKEY

- Lưu đồ quy trình



- Mô tả quy trình

Bước	Nội dung	Người thực hiện	Hướng dẫn chi tiết
(1)	Lấy thông tin bản ghi DS được cập nhật từ NĐK lên hệ thống SRS-EPP (DS1)	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	Thông tin bản ghi DS được cập nhật: + KeyTag + Alg + DigestType + DigestValue=DS1
(2)	Tạo bản ghi DS từ bản ghi DNSKEY được cập nhật lên hệ thống SRS-EPP	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	- Hệ thống sẽ thực hiện tạo bản ghi DS từ DNSKEY với các thuật toán: + SHA1 + SHA256 + SHA384
(3)	Tạo bản ghi DS từ bản ghi DNSKEY được truy vấn trên các DNS Hosting	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	- Truy vấn lấy thông tin bản ghi DNSKEY trên các DNS Hosting - Hệ thống sẽ thực hiện tạo bản ghi DS từ DNSKEY với các thuật toán: + SHA1 + SHA256 + SHA384
(4)	So sánh giá trị Digest Value của các bản ghi DS (DS1, DS2 và DS3)	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	- Hệ thống thực hiện kiểm tra tính trùng khớp của các bản ghi DS được tạo ra và giá trị hàm băm của DNSKEY (HASH) - Nếu trùng khớp chuyển sang bước (5) - Nếu không trùng khớp chuyển sang bước (6)
(5)	Xác nhận chính xác	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	- Hệ thống thông báo thông tin bản ghi DS chính xác, yêu cầu xác nhận
(6)	Không xác nhận	Công cụ kiểm tra, xác thực thông tin DS/DNSKEY	- Hệ thống thông báo thông tin bản ghi DS không chính xác, yêu cầu không xác nhận.
(7)	Kết thúc		

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