BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

DNSSEC.vn

TÀI LIỆU

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC ISP

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
4.0	20/4/2020	Cập nhật lần 3

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
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISP	Doanh nghiệp Internet
KSK	Key Signing Key
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

DANH MỤC BẢNG BIỂU

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 ISP

1. Định nghĩa về ISP (Internet Service Provider)

Là đơn vị, doanh nghiệp quản lý, vận hành các hệ thống máy chủ tên miền đệm (DNS Recursive Caching), cung cấp dịch vụ truy vấn/ phản hồi truy vấn tên miền cho khách hàng, người dùng Internet. ISP là cầu nối để khách hàng và người dùng Internet có thể kết nối đến các hệ thống DNS khác. Thông thường trong triển khai DNSSEC, các ISP sẽ không thuộc nhóm Signing (quản lý và ký số tên miền, trừ đối với các tên miền tự quản lý), mà các ISP thuộc nhóm Validation (xác thực) sẽ đóng vai trò xác thực DNSSEC, đảm bảo các câu trả lời từ các hệ thống hỗ trợ DNSSEC là hợp lệ và toàn vẹn.

2. Phân tích, đánh giá vai trò

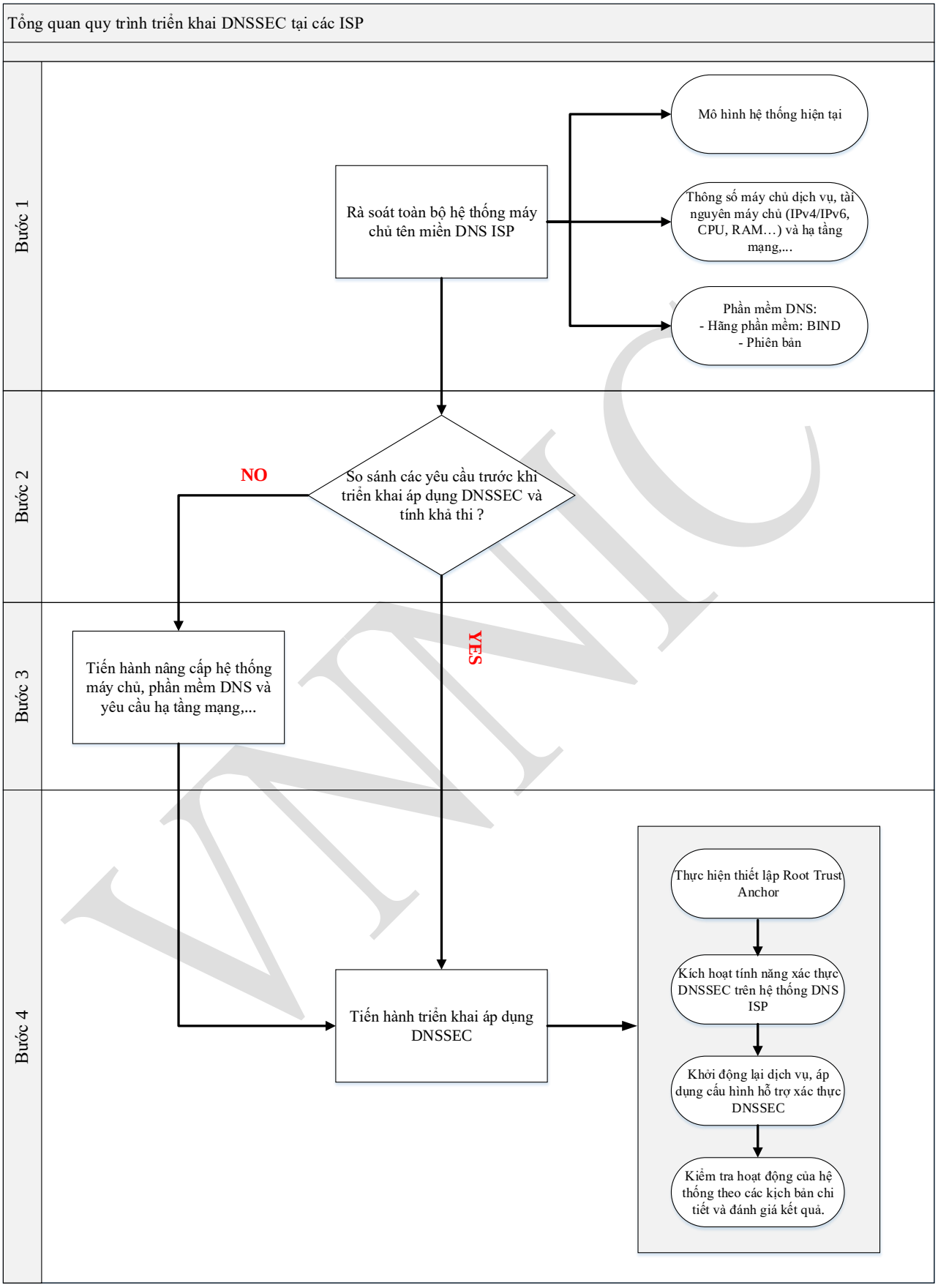
Việc triển khai xác thực DNSSEC trên các hệ thống DNS của các ISP có vai trò rất quan trọng, với vai trò là hệ thống xác thực các phản hồi truy vấn DNS/DNSSEC, điều này sẽ giúp bảo vệ người sử dụng, chống lại sự giả mạo các phản hồi truy vấn DNS. Việc giả mạo các phản hồi truy vấn DNS có thể gây ra các hậu quả nghiêm trọng về cả vấn đề kinh tế (lợi nhuận, làm giảm sự uy tín của thương hiệu, tổ chức) và các vấn đề an ninh cho cả người dùng (đánh cắp thông tin người dùng) và đối với các doanh nghiệp (chuyển hướng các luồng dữ liệu đến các đích có chứa mã độc hại, lừa đảo, hoặc chặn/bắt các gói tin).

Khi một ISP hỗ trợ DNSSEC, đồng nghĩa với việc ISP cung cấp cho người dùng cuối của họ gia tăng tính bảo mật, an toàn trên Internet bởi các máy chủ DNS với khả năng xác thực tên miền và đảm bảo rằng các DNS không bị thay đổi sai lệch, hay bị chuyển hướng luồng dữ liệu

Các tính năng quan trọng nhất của DNSSEC là nó thêm các cơ chế để xác minh tính xác thực của các đáp ứng DNS. Để đạt được điều này, chữ ký số DNSSEC trên các bản ghi DNS phải có trong câu trả lời. Những đối tượng nhận dữ liệu truy vấn DNS như máy chủ tên miền đệm có thể xác nhận chữ ký số DNSSEC và điều này có thể chứng minh được rằng các dữ liệu DNS đã được xác thực.

3. Quy trình triển khai DNSSEC

3.1. Tổng quan quy trình thực hiện


Tổng quan quy trình triển khai DNSSEC tại các ISP
Bước 1
Bước 2
Bước 3
Bước 4
Rà soát toàn bộ hệ thống máy chủ tên miền DNS ISP
Mô hình hệ thống hiện tại
Thông số máy chủ dịch vụ, tài nguyên máy chủ (IPv4/IPv6, CPU, RAM…) và hạ tầng mạng,...
Phần mềm DNS:
- Hãng phần mềm: BIND
- Phiên bản
So sánh các yêu cầu trước khi triển khai áp dụng DNSSEC và tính khả thi ?
NO
YES
Tiến hành nâng cấp hệ thống máy chủ, phần mềm DNS và yêu cầu hạ tầng mạng,...
Tiến hành triển khai áp dụng DNSSEC
Thực hiện thiết lập Root Trust Anchor
Kích hoạt tính năng xác thực DNSSEC trên hệ thống DNS ISP
Khởi động lại dịch vụ, áp dụng cấu hình hỗ trợ xác thực DNSSEC
Kiểm tra hoạt động của hệ thống theo các kịch bản chi tiết và đánh giá kết quả.

Giải thích quy trình:

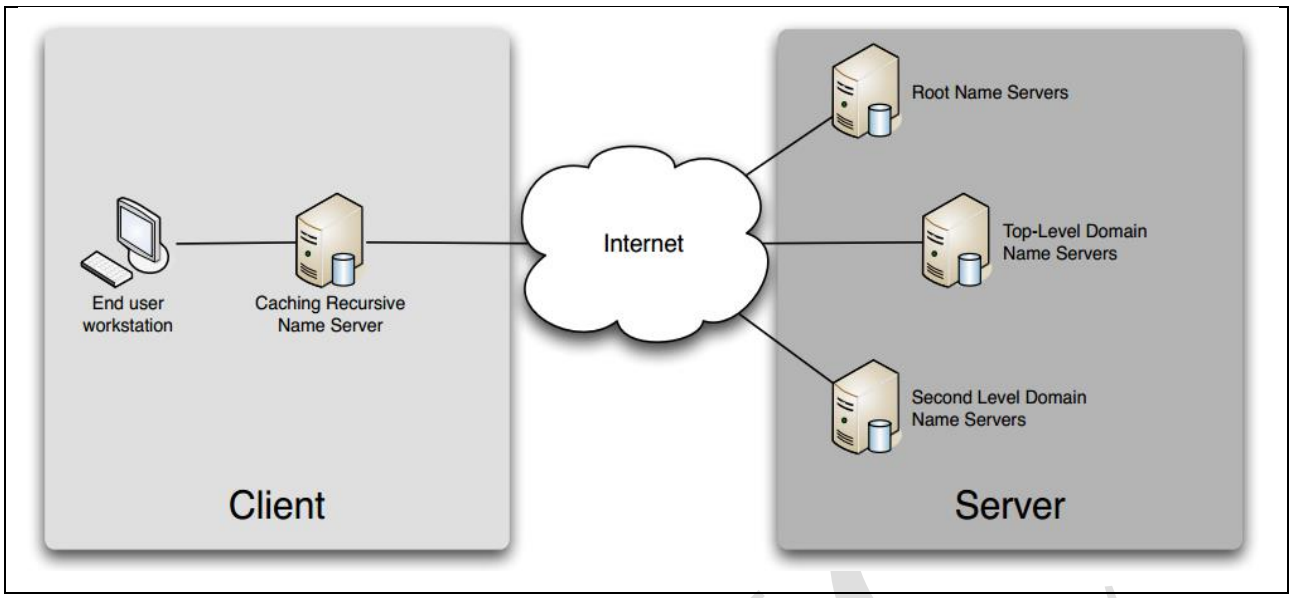
Hệ thống DNS ISP thông thường là các hệ thống máy chủ DNS Recursive Caching, sẽ đóng vai trò xác thực (validation) trong DNSSEC. Việc triển khai DNSSEC sẽ thực hiện theo quy trình các bước dưới đây:

- **Bước 1:** Trước hết cần thực hiện rà soát hệ thống máy chủ DNS Recusive Caching của chính ISP; bao gồm mô hình hệ thống hiện tại, các thông số máy chủ, hạ tầng mạng và phiên bản phần mềm DNS đang được sử dụng, để có thể nhìn một cách tổng quát về hệ thống thực tại.
- **Bước 2:** Đánh giá mức độ ảnh hưởng và tính khả thi khi áp dụng triển khai DNSSEC đối với hệ thống hiện tại dựa trên các thông số đã rà soát ở bước trên và các yêu cầu trước khi triển khai áp dụng DNSSEC.
    - Nếu hệ thống chưa đáp ứng được các yêu cầu trước khi triển khai áp dụng DNSSEC thì chuyển sang Bước 3.
    - Nếu hệ thống hoàn toàn có thể đáp ứng mọi yêu cầu, chuyển sang Bước 4.
- **Bước 3:** Tiến hành nâng cấp hệ thống máy chủ DNS, phần mềm DNS hay hạ tầng mạng tại các ISP để đáp ứng các yêu cầu đặt ra, và chuyển qua Bước 4 để tiến hành triển khai áp dụng DNSSEC.
- **Bước 4:** Trong bước này sẽ thực hiện chi tiết các công việc, và kiểm tra theo các kịch bản thử nghiệm, đưa ra đánh giá hoạt động của hệ thống.

3.2. Rà soát hệ thống máy chủ

3.2.1. Mô hình hiện tại

Mô hình hệ thống tên miền bộ nhớ đệm (DNS Recursive Caching) phổ biến tại các ISP:



Hình 1: Mô hình nguyên lý tổng quan của hệ thống DNS

3.2.2. Thông số máy chủ dịch vụ, hạ tầng mạng và phần mềm DNS

Tiến hành rà soát toàn bộ các thông số máy chủ dịch vụ và hạ tầng mạng tại chính đơn vị ISP dựa theo bảng check list dưới đây:

Nội dung rà soát	Tiêu chí	Kết quả
Thông số máy chủ dịch vụ DNS ISP	Tên máy chủ, chủng loại	
	Địa chỉ IV4/IPv6	
	Bộ nhớ RAM	
	Dung lượng ổ bộ nhớ	
	CPU	
Hạ tầng mạng có thể đáp ứng các yêu cầu DNSSEC	Cho phép DNS over TCP	☐
	Cho phép các gói tin UDP kích thước lớn	☐
Phần mềm DNS	Hãng phần mềm	
	Phiên bản	

Bảng 1: Check list các công việc rà soát trước khi triển khai

3.3. Các yêu cầu trước khi triển khai

3.3.1. Yêu cầu về phần mềm

- Phần mềm BIND:

BIND (the Berkeley Internet Name Daemon) là phần mềm DNS phổ biến nhất trên Internet, và được phát hành bởi ISC (the Internet System Consortium, http://www.isc.org).

BIND đã hỗ trợ DNSSEC cho tất cả các phiên bản của BIND9. Nếu phiên bản BIND hiện đang sử dụng không sẵn sàng hỗ trợ DNSSEC hoặc có hỗ trợ nhưng phiên bản cũ, khuyến nghị nên nâng cấp lên từ phiên bản BIND 9.7 trở lên hoặc mới nhất BIND 9.17 để có thêm nhiều tính năng hỗ trợ DNSSEC tốt hơn (Xem phụ lục Các tính năng mới của BIND 9.11 trở lên)

3.3.2. Năng lực máy chủ hệ thống

Việc kích hoạt xác thực DNSSEC trên máy chủ tên miền bộ nhớ đệm (ISP DNS Server) tạo cho nó một trình phân giải xác thực. Công việc của một trình phân giải xác thực là lấy thêm thông tin có thể được sử dụng để tính toán, xác minh các câu trả lời. Dưới đây là các yêu cầu về phần cứng của các máy chủ vật lý cũng như các máy chủ xây dựng trên nền tảng ảo hóa để đáp ứng việc phân giải xác thực:

- CPU:

Một trình phân giải xác thức thực hiện chức năng mã hóa rất nhiều các câu trả lời, điều này thường dẫn đến gia tăng việc sử dụng CPU, trừ khi máy chủ DNS đệ quy đã được xây dựng tích hợp trong phần cứng để thực hiện các tính toán mật mã mã hóa.

- Bộ nhớ hệ thống:

Việc kích hoạt DNSSEC dẫn đến các câu trả lời có kích thước lớn hơn, và sẽ chiếm không gian bộ nhớ lớn hơn.

3.3.3. Hạ tầng mạng

Khi triển khai áp dụng xác thực DNSSEC trên máy chủ tên miền bộ nhớ đệm (ISP DNS Server), DNSSEC sẽ đính kèm chữ ký số vào gói tin phản hồi truy vấn DNS, điều này làm tăng kích thước của gói tin.

Với các phản hồi truy vấn đối với DNS thông thường, kích thước gói tin không vượt quá 512 byte. Đối với DNSSEC, kích thước các gói tin có thể lớn hơn nhiều và thường xuyên vượt quá 1500 byte. Do vậy cần phải đảm bảo rằng cơ sở hạ tầng mạng là phù hợp và đáp ứng tốt.

Dưới đây là một số yêu cầu về hạ tầng mạng cần đáp ứng để có thể triển khai DNSSEC:

- DNS over TCP:

Theo truyền thống, DNS hoạt động dựa trên giao thức UDP để truyền tải các truy và trả lời. Tuy nhiên trong một số trường hợp, các đáp ứng DNS có kích thước gói tin vượt quá mức tối đa dẫn đến việc đưa giao thức TCP sử dụng là hoàn toàn có thể.

Do vậy cần phải cho phép, kiểm tra kết nối mạng qua giao thức TCP port 53 trên hệ thống hạ tầng mạng để đảm bảo rằng "DNS over TCP" được phép hoạt động.

- Kích thước gói UDP:

DNSSEC hoạt động cũng một phần dựa trên giao thức mở rộng của DNS được gọi là EDNS0. Với giao thức này sẽ làm cho DNS có thể sử dụng gói tin lớn hơn 512 byte để truyền tải đáp ứng truy vấn DNS. Nhiều phần mềm DNS (trong đó có BIND) được cấu hình quy định kích thước gói EDNS0 là 4KB, điều này có nghĩa rằng các máy chủ DNS có thể nhận được các gói tin với kích thước lên đến 4KB.

Các vấn đề như là hệ quả của việc trên:

- Một số hệ thống tường lửa (firewall) được cấu hình loại bỏ các gói tin UDP DNS có kích thước lớn hơn 512 byte vì được xem như một cuộc tấn công.

- Một số hệ thống tường lửa cũng từ chối chấp nhận các gói tin UDP phân mảnh, và đây cũng có thể được cho là dấu hiệu của tấn công.

Do vậy, trong cả hai trường hợp đó, cần phải thực hiện cấu hình lại tường lửa dỡ bỏ các hạn chế, để đảm bảo hệ thống mạng có khả năng xử lý các gói tin UDP lớn (>512 byte, ≤4000 byte).

3.3.3. Checklist kết quả so sánh yêu cầu

Bảng dưới đây là một checklist có thể tham khảo để lập kế hoạch triển khai:

Yêu cầu	Check
Phần mềm hỗ trợ DNSSEC	
Nếu sử dụng phần mềm BIND: BIND phiên bản 9.7 trở lên, hoặc mới nhất BIND 9.17	☐
Các máy chủ hệ thống đủ năng lực đáp ứng	☐
Hạ tầng mạng có thể đáp ứng các yêu cầu DNSSEC	
Cho phép DNS over TCP	☐
Cho phép các gói tin UDP kích thước lớn	☐

Bảng 2: Checklist các yêu cầu triển khai DNSSEC đối với các ISP

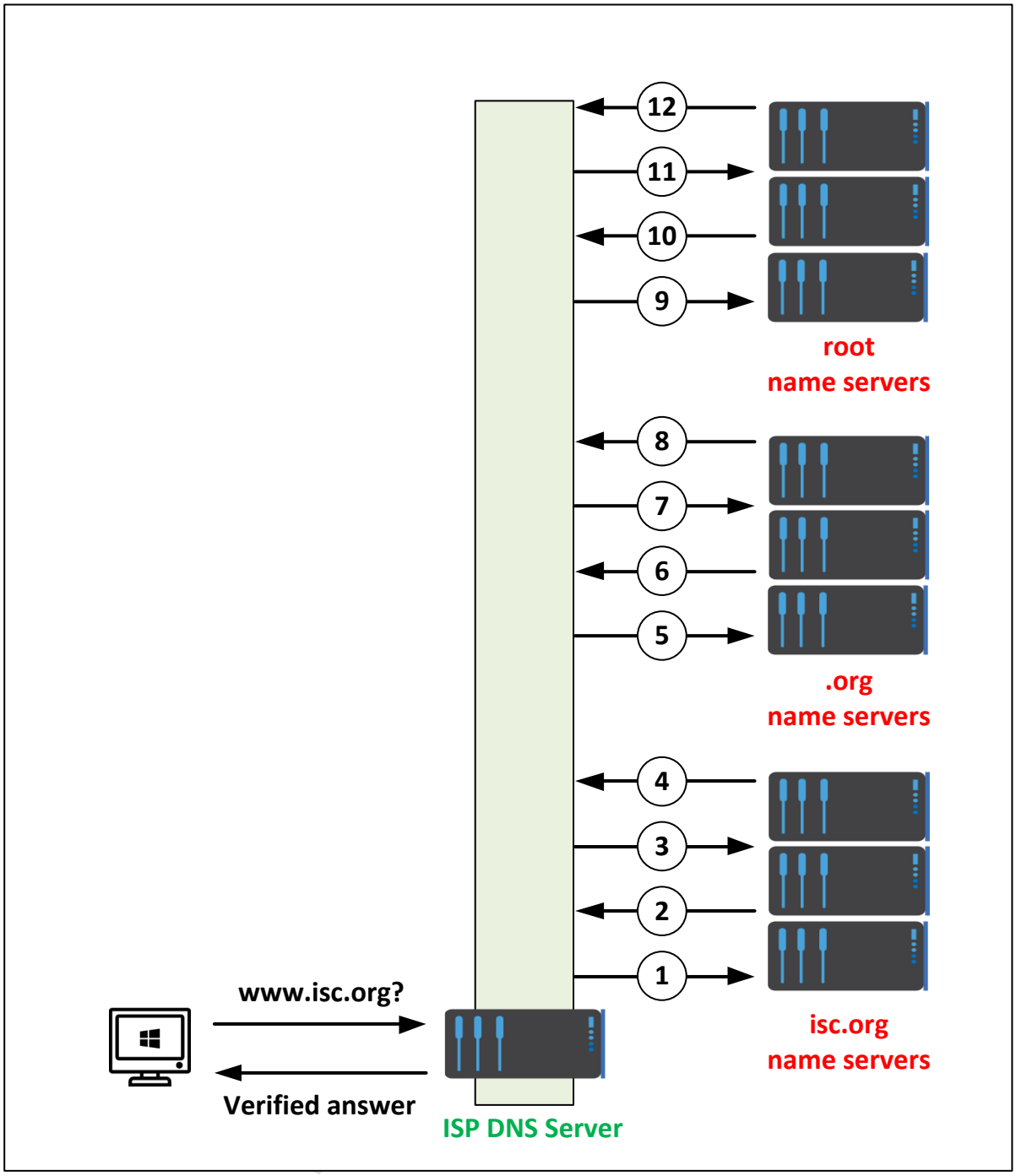
3.4. Mô hình triển khai

Việc triển khai DNSSEC đối với hệ thống DNS Caching trên các ISP sẽ không làm thay đổi mô hình hệ thống hiện tại của ISP.

3.4.1. Nguyên lý hoạt động

- Quá trình truy vấn và được xác thực với DNSSEC

Dưới đây là sơ đồ thể hiện quá trình truy vấn và trả lời truy vấn dối với DNS có DNSSEC:



Hình 2: Quá trình truy vấn có xác thực DNSSEC

Mô tả:

Đối với quá trình truy vấn có DNSSEC, các bước thực hiện truy vấn sẽ theo trình tự như đối với các truy vấn DNS thông thường. Và sau khi máy chủ tên miền đệm (ISP DNS

Server) nhận được câu trả lời cuối cùng về thông tin máy chủ tên miền cần truy vấn từ máy chủ có thẩm quyền. Máy chủ tên miền đệm (ISP DNS Server) sẽ thực hiện chức năng xác thực DNSSEC.

1. Máy chủ DNS của ISP gửi yêu cầu truy vấn bản ghi A của tên miền www.isc.org đến các máy chủ tên miền isc.org.

2. Máy chủ DNS của ISP đó sẽ phản hồi lại bằng câu trả lời kèm theo bản ghi tài nguyên RRSIG (chữ ký số) của bản ghi A.

3. Máy chủ DNS của ISP tiếp tục truy vấn bản ghi tài nguyên DNSKEY của tên miền isc.org lên chính các máy chủ tên miền isc.org

4. Máy chủ tên miền isc.org sẽ phản hồi lại câu trả lời kèm theo các bản ghi DNSKEY và RRSIG của bản ghi DNSKEY.

5. Máy DNS của ISP truy vấn bản ghi DS của isc.org đến máy chủ tên miền .org

6. Máy chủ tên miền .org phản hồi lại bản ghi DS và RRSIG của tên miền isc.org.

7. Máy chủ DNS của ISP truy vấn bản ghi DNSKEY của tên miền .org đến chính các máy chủ tên miền .org

8. Máy chủ tên miền .org sẽ phản hồi lại bản ghi DNSKEY và RRSIG của DNSKEY.

9. Máy chủ DNS của ISP truy vấn bản ghi DS của tên miền .org lên các máy chủ ROOT.

10. Máy chủ ROOT sẽ phản hồi lại bản ghi DS kèm theo chữ ký RRSIG của DS.

11. Máy chủ DNS của ISP tiếp tục hỏi bản ghi DNSKEY của tên miền cấp cao nhất "." lên chính các máy chủ ROOT.

12. Máy chủ ROOT sẽ phản hồi lại bản ghi DNSKEY của tên miền "." kèm theo bản ghi RRSIG của DNSKEY.

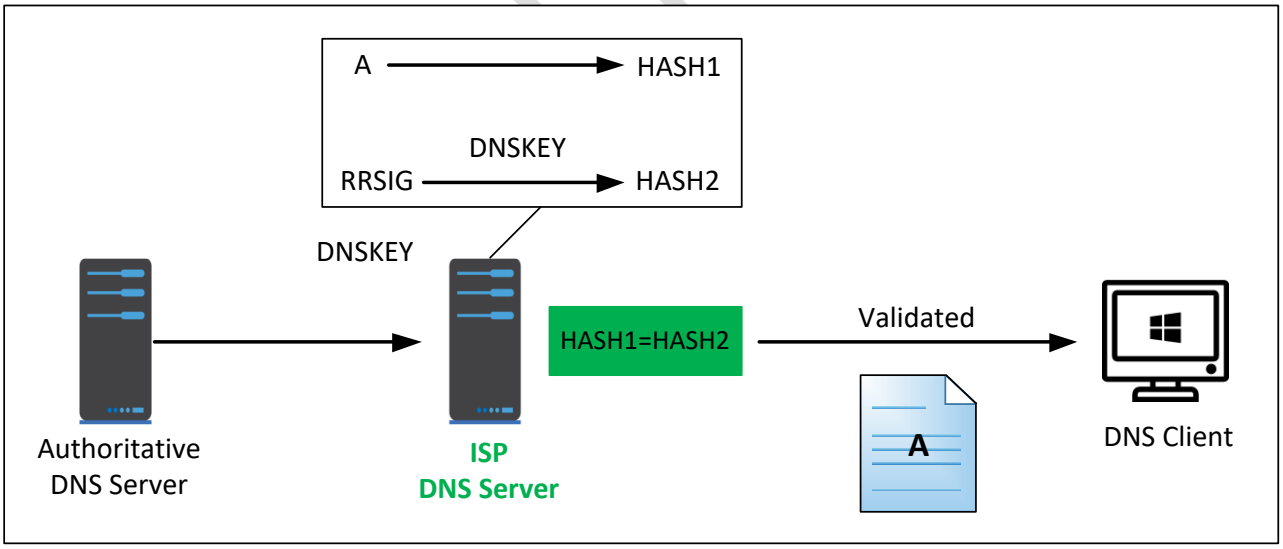
Sau khi xác minh được câu trả lời cuối dùng đã được xác thực, máy chủ DNS của ISP sẽ gửi lại thông tin câu trả lời cho Client.

Đối với các truy vấn có yêu cầu xác thực lần đầu tiên, quá trình thực hiện và phản hồi truy vấn sẽ tốn nhiều thời gian, băng thông và hiệu năng xử lý của máy chủ hơn so với truy vấn DNS thông thường. Nhưng đối với những truy vấn tiếp theo, do các câu trả lời đã được lưu trong bộ nhớ cache của các máy chủ DNS của các ISP nên sẽ chỉ thực hiện truy vấn và trả lời từ bộ nhớ cache của máy chủ, do đó sẽ không ảnh hưởng đến hiệu năng xử lý cũng như thời gian truy vấn của các máy chủ này.

3.4.2. Phân tích sự xác thực

Một máy chủ DNS đệ quy sử dụng các bản ghi tài nguyên DNSKEY để xác nhận các phản hồi từ máy chủ DNS có thẩm quyền bằng cách giải mã các chữ ký số được chứa trong các bản bản ghi tài nguyên DNSSEC liên quan, và sau đó tính toán và so sánh giá trị băm (HASH). Nếu giá trị băm là như nhau, nó sẽ cung cấp một câu trả lời cho Client DNS với các dữ liệu DNS mà Client đó đã yêu cầu, chẳng hạn như một bản ghi tài nguyên (A). Nếu giá trị hash là không giống nhau, nó sẽ trả lời một thông điệp "SERVFAIL".

Hình dưới đây cho thấy sự xác thực câu trả lời trên máy chủ DNS đệ quy của ISP:



Hình 3: Mô tả sự xác thực trên máy chủ DNS đệ quy của ISP

Khi một máy chủ DNS đệ quy (ISP DNS Server) thực hiện phân giải xác thực truy vấn bản ghi A của một tên miền bất kỳ từ Client yêu cầu, nó sẽ thực hiện truy vấn đến máy chủ có thẩm quyền của tên miền đó về bản ghi A, và nó sẽ nhận được cả bản ghi A và bản ghi RRSIG. Máy chủ DNS đệ quy này sẽ cho bản ghi A qua một hàm băm và nhận được kết quả là HASH1. Nó cũng lấy về bản ghi DNSSEC tương ứng để giải mã chữ ký số, và kết quả của việc giải mã băm được giá trị HASH2. Nếu giá trị HASH1 và HASH2 giống hệt nhau và thời gian là chính xác thì câu trả lời sẽ được xác thực. Điều này có nghĩa là chúng ta biết câu trả lời đến từ máy chủ có thẩm quyền (xác thực), và nội dung vẫn còn nguyên vẹn, không bị thay đổi trong quá trình phản hồi (tính toàn vẹn).

3.5. Các bước triển khai

3.5.1. Điều kiện tiên quyết:

Trước khi thực hiện theo các bước hướng dẫn để cấu hình BIND 9.x cho các máy chủ tên miền bộ nhớ đệm (ISP DNS Server) cho phép xác thực DNSSEC, cần đảm bảo các điều kiện cần thiết sau:

- Phiên bản BIND từ 9.7 trở lên (nên cập nhật lên phiên bản BIND 9.11)
- Được cấu hình và cài đặt đúng với chức năng của một máy chủ tên miền bộ nhớ đệm

3.5.2. Thêm neo tin cậy ROOT (ROOT trust anchor)

Thực hiện lấy neo tin cậy ROOT bằng cách DIG bản ghi DNSKEY:

```
# dig @8.8.8.8 DNSKEY . | grep 257
.                       172800  IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=
```

Mở chỉnh sửa tập tin cấu hình của BIND (thường là *named.conf*) và thêm các phần sau đây:

```
trusted-keys   {
     . 257 3 8 "<root-trust-anchor-data>;
```

Trong đó *root-trust-anchor-data* chính là phần dữ liệu DNSKEY của DNS ROOT, thường bắt đầu bằng: "AwEAAagAIKlVZrp…"

Sao chép phần dữ liệu DNSKEY của DNS ROOT vừa truy vấn ở bước trên vào phần *root-trust-anchor-data*, và lưu cấu hình chỉnh sửa.

3.5.3. Kích hoạt sự xác thực

Thêm các cấu hình sau và trong phần *"option"* của tập tin cấu hình BIND (*named.conf*):

```
dnssec-enable yes;
dnssec-validation yes; # enable DNSSEC validation
```

Lưu tập tin cấu hình và đóng trình soạn thảo.

3.5.4. Khởi động lại BIND

Thực hiện kiểm tra lại tập tin cấu hình và khởi động lại BIND để áp dụng cấu hình:

```
# named-checkconf /etc/named.conf
# /etc/init.d/named restart
```

Kiểm tra thông tin log để đảm bảo rằng BIND khởi động một cách chính xác. Và có thể thấy những cảnh báo như: không tồn tại tập tin *"managed keys"*; Điều này là bình thường vì lần đầu tiên khởi động lại BIND. Tập tin *"managed keys"* sẽ được tự động tạo ra.

3.5.5. Kiểm tra cài đặt

Tham khảo phần "***3.6. Các kịch bản thử nghiệm***"

3.6. Các kịch bản thử nghiệm

3.6.1. Thử nghiệm bằng trình duyệt và các tiện ích

Có một số trang web cung cấp tính năng để kiểm tra DNSSEC có được kích hoạt hay không.

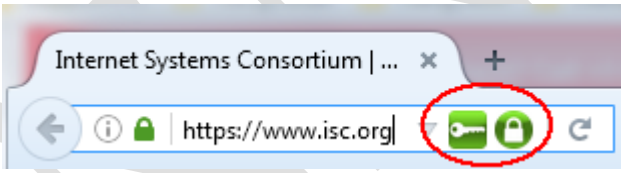
Ví dụ như một số web như:

http://dnssectest.sidn.nl/test.php

http://www.nic.cz/dnssec/

http://dnssec.vs.uni-due.de/

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.



Hình 4: Kết quả xác thực DNSSEC trên trình duyệt Firefox

3.6.2. Sử dụng công cụ dòng lệnh DIG để kiểm chứng

3.6.2.1. Kiểm tra với các kết quả có xác thực

Mục tiêu thử nghiệm này là để chứng minh rằng trình xác thực của máy chủ tên miền bộ nhớ đệm (DNS Caching) xác thực một cách chính xác các câu trả lời DNS cho các tên miền được ký DNSSEC.

Trong quá trình thử nghiệm, thực hiện truy vấn bản ghi A cho tên miền *www.isc.org* và kiểm tra bằng cách xác định giá trị cờ (flags) được phản hồi lại,

Thực hiện lệnh sau:

```
# dig @192.168.1.7 www.isc.org. A +dnssec +multiline

; <<>> DiG 9.10.0-P2 <<>> @192.168.1.7 www.isc.org. A +dnssec
+multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32472
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.           IN A

;; ANSWER SECTION:
www.isc.org.           4 IN A    149.20.64.69
www.isc.org.           4 IN RRSIG A 5 3 60 (
                       20141029233238 20140929233238 4521 isc.org.
                       DX5BaGVd4KzU2AIH911Kar/UmdmkARyPhJVLr0oyPZaq

5zoobGqFI4efvzL0mcpncuUg3BSU5Q48WdBu92xinMdb

E75zl+adgEBOsFgFQR/zqM3myt/8SngWm4+TQ3XFh9eN
                       jqExHZZuZ268NtlxqgF9OmKRRv8X8YigaPShuyU= )

;; Query time: 3 msec
;; SERVER: 192.168.1.7#53(192.168.1.7)
;; WHEN: Fri Oct 03 16:40:04 CST 2014
;; MSG SIZE  rcvd: 223
```

Nếu sau khi thực hiện lệnh trên nhận được kết quả với:

- Cờ AD (Authenticated Data) được thiết lập trong quá trình truy vấn DNS/DNSSEC
- Cờ DO (DNSSEC OK) được thiết lập, cho thấy máy chủ DNS Caching có thể nhận thực DNSSEC
- Bản ghi tài nguyên RRSIG được đính kèm trong câu trả lời, với tên miền giống như các bản ghi A.

Thì tức là dữ liệu đã được xác thực với DNSSEC.

3.6.2.2. Kiểm tra với các kết quả KHÔNG xác thực:

Mục tiêu của thử nghiệm này là để chứng minh rằng trình xác thực của máy chủ tên miền bộ nhớ đệm (DNS Caching) sẽ loại bỏ dữ liệu tên miền cùng với chữ ký số.

Trong thử nghiệm này, thực hiện gửi một truy vấn bản ghi A cho tên miền www.rhybar.cz và kiểm tra xem rằng các máy chủ không cung cấp câu trả lời và trả về đúng mã lỗi.

Thực hiện bằng dòng lệnh sau:

```
# dig +dnssec +noauthority +noadditional A www.rhybar.cz
; <<>> DiG 9.10.0-P2 <<>> +dnssec +noauthority +noadditional A
www.rhybar.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32343
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.rhybar.cz.     IN  A
;; Query time: 4 msec
;; SERVER: 145.100.188.188#53(145.100.188.188)
;; WHEN: Fri Jun 17 17:02:47 2011
;; MSG SIZE rcvd: 42
As you can see in the example output, no a
```

Dựa vào kết quả trên có thể thấy, không có câu trả lời được cung cấp cho các truy vấn và các máy chủ trả về mã lỗi "SERVFAIL" (phần in đậm màu vàng).

3.6.2.3. Phát hiện lỗi của quá trình xác thực

Khi nhận được một kết quả với mã lỗi "SERVFAIL" như trường hợp trên, đây cũng có thể là một lỗi liên quan đến trình xác thực. Để kiểm chứng, bằng cách thêm cờ *"+cd"* (checking disable) để vô hiệu hóa DNSSEC trong lệnh dig.

Nếu khi thêm cờ *"+cd"* trả về kết quả truy vấn thành công, tiếp tục thực hiện với việc không thêm cờ *"+cd"*, nếu cuối cùng thu được phản hồi "SERVFAIL" đồng nghĩa với trình xác thực gặp vấn đề.

```
$ dig @192.168.1.7 www.isc.org. A +cd

; <<>> DiG 9.10.1 <<>> @192.168.1.7 www.isc.org. A +cd
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33590
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.isc.org.                IN   A

;; ANSWER SECTION:
www.isc.org.         30    IN   A    149.20.64.69
```

3.6.3. Sử dụng công cụ dòng lệnh delv để kiểm chứng

Đối với các phiên bản BIND từ 9.10 trở lên, có thể sử dụng Domain Entity Lookup & Validation (***delv***) để thực hiện xác thực các cài đặt. Công cụ này tương tự công cụ ***dig***, nhưng nó được thiết kế đặc biệt cho DNSSEC.

Nếu không có DNSSEC:

```
# delv @192.168.1.7 www.isc.org. A
;; no valid RRSIG resolving 'org/DS/IN': 192.168.1.7#53
;; no valid DS resolving 'www.isc.org/A/IN': 192.168.1.7#53
;; resolution failed: no valid DS
```

Khi chưa kích hoạt xác thực DNSSEC, kết quả nhận được

Sau khi kích hoạt xác thực DNSSEC:

```
# delv @192.168.1.7 www.isc.org. A +multiline
; fully validated
www.isc.org.         60 IN A   149.20.64.69
www.isc.org.         60 IN RRSIG A 5 3 60 (
```

```
                    20141029233238 20140929233238 4521 isc.org.
                    DX5BaGVd4KzU2AIH911Kar/UmdmkARyPhJVLr0oyPZaq
                    5zoobGqFI4efvzL0mcpncuUg3BSU5Q48WdBu92xinMdb
                    E75zl+adgEBOsFgFQR/zqM3myt/8SngWm4+TQ3XFh9eN
                    jqExHZZuZ268NtlxqgF9OmKRRv8X8YigaPShuyU= )
```

Nếu sử dụng lệnh trên và thêm vào thông số *+rtrace* có thể xem được quá trình thực hiện xác thực câu trả lời:

```
# delv @192.168.1.7 www.isc.org +rtrace +multiline
;; fetch: www.isc.org/A
;; fetch: isc.org/DNSKEY
;; fetch: isc.org/DS
;; fetch: org/DNSKEY
;; fetch: org/DS
;; fetch: ./DNSKEY
www.isc.org.        60 IN A   149.20.64.69
www.isc.org.        60 IN RRSIG A 5 3 60 (
                    20141029233238 20140929233238 4521 isc.org.
                    DX5BaGVd4KzU2AIH911Kar/UmdmkARyPhJVLr0oyPZaq
                    5zoobGqFI4efvzL0mcpncuUg3BSU5Q48WdBu92xinMdb
                    E75zl+adgEBOsFgFQR/zqM3myt/8SngWm4+TQ3XFh9eN
                    jqExHZZuZ268NtlxqgF9OmKRRv8X8YigaPShuyU= )
```

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