TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12044:2017

CÁC YÊU CẦU BẢO MẬT DNS (DNSSEC)

DNS Security requirements

HÀ NỘI - 2017

Mục lục

Lời nói đầu

TCVN 12044:2017 được xây dựng trên cơ sở tham khảo các tiêu chuẩn RFC 4033 (03-2005), RFC 6014 (10-2010) và RFC 6840 (02-2013) của IETF.

TCVN 12044:2017 do Viện Khoa học Kỹ thuật Bưu điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Các yêu cầu bảo mật DNS (DNSSEC)

DNS Security Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra các yêu cầu và hướng dẫn đối với phần mở rộng bảo mật hệ thống tên miền (DNSSEC).

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả sửa đổi, bổ sung (nếu có).

RFC 1034, Domain names - concepts and facilities (11-1987) *(Tên miền – Các khái niệm và tính năng).*

RFC 2538, Storing Certificates in the Domain Name System (DNS) (03-1999) *(Lưu trữ chứng chỉ trong hệ thống tên miền (DNS).*

RFC 2181, Clarifications to the DNS Specification (06-1997) *(Làm rõ đặc tính DNS).*

RFC 2671, Extension Mechanisms for DNS (EDNS0) (08-1999) *(Cơ chế mở rộng cho DNS (EDNS0)).*

RFC 2845, Secret Key Transaction Authentication for DNS (TSIG) (05-2000) *(Xác thực giao dịch khóa riêng cho DNS (TSIG).*

RFC 2931, DNS Request and Transaction Signatures (SIG(0)s) (11-2000) *(Yêu cầu và các chữ ký giao dịch DNS (SIG(0)s)).*

RFC 3225, Indicating Resolver Support of DNSSEC (12- 2001) *(Hỗ trợ Resolver chỉ thị của DNSSEC).*

RFC 3226, DNSSEC and IPv6 A6 aware server/Resolver message size requirements (12-2001) *(DNSSEC và Các yêu cầu kích thước thông báo sever/resolver aware).*

RFC 3755, Legacy Resolver Compatibility for Delegation Signer (DS)", (05-2004) – *(Khả năng tương thích Resolver kế thừa cho ký ủy quyền).*

RFC 3833, Threat Analysis of the Domain Name System (DNS) (08-2004) *(Các phân tích mối đe dọa của hệ thống tên miền).*

RFC 4034, Resource Records for DNS Security Extensions (03-2005) *(Bản ghi tài nguyên cho phần mở rộng bảo mật DNS).*

RFC 4035, Protocol Modifications for the DNS Security Extensions (03-2005) *(Các sửa đổi giao thức cho phần mở rộng bảo mật DNS).*

RFC 4305, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", (12-2005) *(Các yêu cầu cài đặt thuật toán mã cho đóng gói tải bảo mật (ESP) và tiêu đề xác thực (AH)).*

RFC 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs) (05-2006) *(Sử dụng SHA-256 trong ký ủy quyền DNSSEC (DS) Tập bản ghi tài nguyên (RRs).*

RFC 5115, Telephony Routing over IP (TRIP) Attribute for Resource Priority (01-2008) *(Định tuyến thoại qua IP (TRIP) Chỉ định cho ưu tiên tài nguyên).*

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1 Định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau đây:

3.1.1

Bản ghi khóa công khai DNS (DNSKEY – DNS Public Key)

Bản ghi sử dụng để chứng thực zone dữ liệu.

3.1.2

Bản ghi chữ ký tài nguyên (RRSIG – Resource Record Signature)

Bản ghi sử dụng để chứng thực cho các bản ghi tài nguyên trong zone dữ liệu.

3.1.3

Bản ghi bảo mật kế tiếp (NSEC – Next Secure)

Bản ghi sử dụng trong quá trình xác thực đối với các bản ghi có cùng sở hữu tập các bản ghi tài nguyên hoặc bản ghi CNAME, kết hợp với RRSIG để xác thực cho zone dữ liệu.

3.1.4

Bản ghi ký chuyển giao (DS – Delegation Signer)

Bản ghi sử dụng để cấu hình chứng thực giữ các zone dữ liệu, sử dụng trong việc ký xác thực trong quá trình chuyển giao DNS.

3.1.5

Vùng (Zone)

Nơi lưu trữ thông tin tên miền và dữ liệu tương ứng với thông tin tên miền.

3.1.6

Bộ phân giải (Resolvers)

Các chương trình người dùng truy cập máy chủ tên miền thông qua các giao thức chuẩn.

3.1.7

Bộ phân giải sơ khai (Stub Resolver)

Một chương trình người dùng truy cập máy chủ tên miền không hỗ trợ các truy vấn đệ quy, chương trình chỉ làm việc với một DNS.

3.1.8

Bộ phân giải Security-Aware (Security-Aware Resolver)

Một thực thể hoạt động trong vai trò của một Resolver, có khả năng nhận biết các phần mở rộng bảo mật DNS được quy định trong tiêu chuẩn này. Đặc biệt, một Security-Aware Resolver là một phần tử gửi truy vấn DNS, nhận hồi đáp DNS, hỗ trợ phần mở rộng kích thước thông báo EDNS0 và bit DO, nó thể hiện năng lực sử dụng các loại bản ghi và bit tiêu đề thông báo để cung cấp các chỉ dẫn DNSSEC.

3.1.9

Máy chủ tên miền Security-Aware (Security-Aware Name Server)

Một thực thể hoạt động trong vai trò của một máy chủ tên miền, nó có khả năng nhận biết các phần mở rộng bảo mật DNS được quy định trong tiêu chuẩn này. Đặc biệt, máy chủ tên miền Security-Aware là một phần tử nhận các truy vấn DNS, gửi các hồi đáp DNS, hỗ trợ EDNS0 và bit DO, và hỗ trợ các loại bản ghi và các bit tiêu đề thông báo được quy định trong tiêu chuẩn này.

3.1.10

Máy chủ tên miền đệ quy Security-Aware (Security-Aware Recursive Name Server)

Một thực thể hoạt động cả trong vai trò máy chủ tên miền Security-Aware và vai trò Security-Aware Resolver.

3.1.11

Bộ phân giải Security-Aware sơ khai (Security-Aware Stub Resolver)

Một thực thể hoạt động trong vai trò của một Stub Resolver có thể nhận biết các phần mở rộng bảo mật DNS để cung cấp các chỉ dẫn kèm theo. Các chỉ dẫn này không có sẵn trong Security-Olivious Stub Resolver. Các Security-Aware Stub Resolver có thể là "Validating" hoặc "Non-Validating", tùy thuộc vào việc Stub Resolver cố gắng xác minh chữ ký DNSSEC trên nó hoặc tin tưởng một Security-Aware khác.

3.1.12

Xác nhận bộ phân giải Security-Aware sơ khai (Validating Security-Aware Stub Resolver)

Một Security-Aware Stub Resolver gửi truy vấn ở chế độ đệ quy nhưng thực hiện xác thực chữ ký của riêng nó thay vì tin cậy vào máy chủ tên miền đệ quy Security-Aware.

3.1.13

Xác nhận bộ phân giải sơ khai (Validating Stub Resolver)

Một thuật ngữ khác để mô tả một Validating Security-Aware Stub Resolver.

3.1.14

Không xác nhận bộ phân giải Security-Aware sơ khai (Non-Validating Security-Aware Stub Resolver)

Một Security-Aware Stub Resolver tin cậy một hoặc nhiều máy chủ tên miền đệ quy Security-Aware thực hiện hầu hết các công việc trên đại diện của nó. Nói chung, một Non-Validating Security-Aware Stub Resolver sẽ gửi truy vấn DNS, nhận hồi đáp DNS, và có khả năng cấu hình một kênh được bảo mật phù hợp với một máy chủ tên miền đệ quy Security-Aware cung cấp các chỉ dẫn trên đại diện của Security-Aware Stub Resolver này.

3.1.15

Không xác nhận bộ phân giải sơ khai (Non-Validating Stub Resolver)

Một thuật ngữ khác để mô tả một Non-Validating Security-Aware Stub Resolver.

3.1.16

Security-Oblivious < ... >

Là khái niệm trái ngược với Security-Aware, nghĩa là không biết, không hỗ trợ Security-Aware đối với DNSSEC.

3.1.17

Chuỗi xác thực (Authentication Chain)

Một dãy xen kẽ tập bản ghi DNSKEY và tập bản ghi DS, nhận được từ một chuỗi dữ liệu được ký. Một bản ghi DNSKEY sử dụng xác thực chữ ký bao gồm một bản ghi DS và chấp nhận cho phép việc bản ghi DS đã được xác thực. Bản ghi DS bao gồm một mã Hash của một bản ghi DNSKEY khác và bản ghi DNSKEY mới này được xác thực bằng việc trùng mã Hash của bản ghi DS này. Bản ghi DNSKEY mới này lần lượt xác thực một tập bản ghi DNSKEY khác, kết quả là, một số bản ghi DNSKEY trong tập này có thể được sử dụng để xác thực một bản ghi DS khác, cho đến khi chuỗi cuối cùng kết thúc với một bản ghi DNSKEY tương ứng việc khóa riêng ký dữ liệu DNS mong muốn.

Ví dụ, tập bản ghi DNSKEY gốc có thể được sử dụng để xác thực một tập bản ghi DS "example.". Tập bản ghi DS "example." này bao gồm một mã Hash phù hợp với DNSKEY "example.", và một khoá riêng tương ứng của DNSKEY này ký một tập bản ghi DNSKEY "example.". Những bản sao khoá riêng của tập bản ghi DNSKEY "example." ký các bản ghi dữ liệu "www.example." và các bản ghi DS đối với các chuyển giao "subzone.example.".

3.1.18

Khóa xác thực (Authentication Key)

Khóa công khai sử dụng để xác thực dữ liệu và được Security-Aware Resolver xác thực. Một Security-Aware Resolver có thể nhận được các khóa xác thực theo ba cách sau đây:

- Cách thứ nhất, Resolver được cấu hình để hiểu ít nhất về một khóa công khai; dữ liệu được cấu hình này là khóa công khai của nó hoặc mã Hash của khóa công khai được tìm thấy trong bản ghi DS.
- Thứ hai, Resolver có thể sử dụng một khóa công khai được xác thực để xác minh một bản ghi DS và một bản ghi DNSKEY mà bản ghi DS chỉ dẫn đến.
- Thứ ba, Resolver có thể xác định một khóa công khai mới đã được ký bởi khóa riêng rằng Resolver đã xác minh, khoá riêng này tương ứng với một khóa công khai khác. Lưu ý rằng, Resolver này phải tuân thủ một chính sách nội bộ khi quyết định xác thực một khóa công khai mới, thậm chí, nếu chính sách nội bộ này đơn giản chỉ để xác thực bất kỳ khóa công khai mới thì Resolver có thể xác thực chữ ký.

3.1.19

Tập bản ghi thẩm quyền (Authoritative RRset)

Một tập bản ghi "thẩm quyền" nếu và chỉ nếu tên miền này nằm trong tập con của không gian tên miền tại hoặc dưới điểm Zone Apex và tại hoặc trên điểm phân tách zone con và zone cha (nếu có).

Tất cả các tập bản ghi tại điểm Zone Apex là tập bản ghi thẩm quyền, trừ các bản ghi thuộc về zone cha tại tên miền này (nếu có). Tập bản ghi này có thể bao gồm một tập bản ghi DS, tập bản ghi NSEC

tham chiếu của tập bản ghi DS này ("NSEC cha") và các bản ghi RRSIG được liên kết với các tập bản ghi này, tất cả các tập bản ghi này đều là tập bản ghi thẩm quyền trong zone cha.

Tương tự, nếu zone này bao gồm các điểm chuyển giao bất kỳ, duy nhất một tập bản ghi NSEC cha, các tập bản ghi DS và các tập bản ghi RRSIG bất kỳ được liên kết với các tập bản ghi này đều là tập bản ghi thẩm quyền đối với zone này.

3.1.20

Zone cut

Ranh giới giữa các zone. Ranh giới chia tách zone con (ở bên dưới ranh giới) và zone cha (ở bên trên ranh giới).

3.1.21

Điểm Zone Apex (Zone Apex)

Tên tại phía zone con tại một zone cut.

3.1.22

Điểm chuyển giao (Delegation Point)

Tên tại phía cha của một zone cut. Điểm chuyển giao đối với "foo.example" là nút foo.example trong zone "example" (không phải điểm Zone Apex của zone "foo.example").

3.1.23

Island of Security

Zone được ký, được ủy quyền nhưng không có chuỗi xác thực từ zone cha của nó, không có bản ghi DS chứa mã Hash của một bản ghi DNSKEY cho phần riêng biệt được zone cha ủy quyền (xem [RFC 4034]). Một Island of Security được cấp phát bởi các máy chủ tên miền Security-Aware, có thể cung cấp các chuỗi xác thực cho các zone con bất kỳ được ủy quyền. Hồi đáp từ một Island of Security hoặc phần con của nó chỉ được xác thực nếu có một phương pháp đáng tin cậy ngoài băng từ giao thức DNS xác thực các khóa xác thực của nó.

3.1.24

Neo tin cậy (Trust Anchor)

Một bản ghi DNSKEY được cấu hình hoặc mã Hash bản ghi DS của một bản ghi DNSKEY. Một Validating Security-Aware Stub Resolver sử dụng khóa công khai hoặc mã Hash làm điểm bắt đầu cho việc xây dựng chuỗi xác thực cho một hồi đáp DNS được ký. Nhìn chung, một Validating Resolver sẽ phải có được giá trị ban đầu của Neo tin cậy thông qua một số phương pháp bảo mật hoặc tin cậy bên ngoài giao thức DNS. Giá trị Neo tin cậy này thể hiện rằng Resolver kỳ vọng zone có các điểm Neo tin cậy được ký.

3.1.25

Khóa ký khóa (KSK) (Key Signing Key (KSK))

Một khóa xác thực tương ứng với một khoá riêng được sử dụng để ký một hoặc nhiều khóa xác thực khác nhau cho một zone nhất định. Thông thường, khoá riêng tương ứng với KSK sẽ dùng để ký ZSK (có khoá riêng tương ứng sẽ dùng để ký các dự liệu zone). Chính sách nội bộ có thể yêu cầu ZSK thay đổi thường xuyên, trong khi KSK có thể có thời hạn hiệu lực dài hơn để cung cấp các điểm an toàn ổn định hơn trong zone. Kết quả là, chỉ định một khóa xác thực như một KSK: xác minh DNSSEC không

phân biệt giữa KSK và các khóa xác thực khác, và nó có thể sử dụng một khóa duy nhất cho cả KSK và ZSK. Xem [RFC 3757].

3.1.26

Khóa ký zone (ZSK) (Zone Signing Key (ZSK))

Một khoá xác thực có khoá riêng tương ứng sẽ dùng để ký zone. Thông thường, một ZSK sẽ là một phần của tập bản ghi DNSKEY, như là khoá riêng tương ứng của KSK dùng để ký tập bản ghi DNSKEY này; nhưng ZSK được sử dụng cho mục đích khác và có thể khác KSK ở một số thông tin (ví dụ TTL). Việc chỉ định một khoá xác thực ZSK hoàn toàn là do vấn đề trong vận hành; quá trình xác thực DNSSEC không phân biệt giữa ZSK và các khoá xác thực khác, nó có thể sử dụng một khoá duy nhất cho cả KSK và ZSK.

3.1.27

Zone được ký (Signed Zone)

Một zone có các tập bản ghi được ký và chứa DNSKEY, RRSIG, NSEC và DS.

3.1.28

Zone không được ký (Unsigned Zone)

Một zone có các tập bản ghi không được ký hoặc không chứa DNSKEY, RRSIG, NSEC hoặc DS.

3.2 Chữ viết tắt

Theo mục đích của tiêu chuẩn này, các chữ viết tắt sau đây được áp dụng:

AD	Authenticated Data	Dữ liệu được xác thực
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
CD	Checking Disabled	Kiểm tra vô hiệu hóa
CNAME	Canonical Name	Tên chính tắc
DNAME	Delegation Name	Tên chuyển giao
DNS	Domain Name System	Hệ thống tên miền
DNSSEC	Security Extensions DNS	Phần mở rộng bảo mật hệ thống tên miền
DNSKEY	DNS Public Key	Bản ghi khóa công khai DNS
DO	DNSSEC OK	Hỗ trợ DNSSEC
DoS	Denial of Service Attack	Tấn công từ chối dịch vụ
DS	Delegation Signer	Bản ghi ký chuyển giao
EDNS	Extension Mechanisms for DNS	Cơ chế mở rộng cho DNS
IANA	Internet Assigned Numbers Authority	Tổ chức cấp phát số hiệu Internet

NAT	Network address translation	Biên dịch địa chỉ mạng
NSEC	Next Secure	Bản ghi bảo mật kế tiếp
NSEC3	Next Secure 3	Bản ghi bảo mật kế tiếp 3
NSEC3PARAM		Bản ghi NSEC3PARAM
RR	Resource Record	Bản ghi tài nguyên
RRset	Resource Record set	Tập bản ghi tài nguyên
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng
TTL	Time To Live	Thời gian hợp lệ
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải
TSIG	Transaction SIGnature	Chữ ký giao dịch

4 Dịch vụ cung cấp bởi bảo mật DNS

Phần mở rộng bảo mật DNS cung cấp cơ chế xác thực nguồn gốc và đảm bảo toàn vẹn dữ liệu cho dữ liệu DNS, bao gồm các cơ chế để xác thực việc từ chối tồn tại của dữ liệu DNS, Các cơ chế này được mô tả như sau:

- Các cơ chế yêu cầu thay đổi giao thức DNS: DNSSEC thêm bốn loại bản ghi tài nguyên mới là RRSIG, DNSKEY, DS và NSEC và hai bit tiêu đề thông báo mới CD và AD. DNSSEC yêu cầu hỗ trợ EDNS0 (xem [RFC 3225]) để đáp ứng việc tăng kích thước thông báo DNS do thêm các bản ghi DNSSEC. Cuối cùng, DNSSEC cũng yêu cầu hỗ trợ bit tiêu đề EDNS DNSSEC OK (DO) (xem [RFC 3225]), vì vậy, trong truy vấn của Security-Aware Resolver cho biết rằng Security-Aware Resolver này mong muốn nhận được các bản ghi DNSSEC trong thông báo Answer.
- Các chỉ dẫn bảo vệ hệ thống DNS chống lại các mối đe dọa được mô tả trong [RFC 3833]. Xem mục 13 mô tả những hạn chế của các phần mở rộng.

4.1 Xác thực nguồn gốc dữ liệu và toàn vẹn dữ liệu

DNSSEC cung cấp xác thực bằng cách kết hợp chữ ký số được mã hóa với các tập bản ghi DNS. Những chữ ký số được lưu trữ trong một bản ghi tài nguyên mới, bản ghi RRSIG. Việc ký dữ liệu của zone do một khoá riêng duy nhất thực hiện, tuy nhiên, việc ký dữ liệu này cũng có thể do nhiều khóa thực hiện. Ví dụ, có thể dùng nhiều khóa đối với mỗi chuỗi các thuật toán ký số khác nhau. Nếu một Security-Aware Resolver chắc chắn biết được một khóa công khai của zone, nó có thể xác thực dữ liệu của zone đã được ký. Trong DNSSEC, khoá ký dữ liệu zone sẽ được liên kết với zone của chính nó và máy chủ thẩm quyền của zone đó (các khoá công khai của cơ chế xác thực tiến trình DNS có thể xuất hiện trong zone, như mô tả trong [RFC 2931], nhưng DNSSEC chỉ liên quan đến bảo mật các đối tượng trong dữ liệu DNS, không liên quan đến bảo mật tiến trình DNS. Các khoá được liên kết với bảo mật tiến trình có thể được lưu trữ trong các loại bản tin tài nguyên khác như mô tả trong [RFC 3755].

Một Security-Aware Resolver có thể nhận biết được khóa công khai của zone thông qua Neo tin cậy được cấu hình trong Resolver hoặc bằng quá trình phân giải DNS thông thường. Cho phép sau này, các khóa công khai được lưu trữ trong một loại bản ghi tài nguyên mới, bản ghi DNSKEY. Lưu ý, các khoá riêng sử dụng ký dữ liệu zone phải được giữ an toàn và được lưu trữ ngoại tuyến khi thực hiện.

Để phát hiện một khóa công khai tin cậy thông qua bộ phân giải DNS, khóa công khai của nó phải được ký bởi một khóa xác thực đã cấu hình từ trước. Security-Aware Resolver xác thực thông tin zone bằng cách tạo ra một chuỗi xác thực từ một khóa công khai mới được nhận biết theo chiều ngược lại một khóa công khai xác thực được biết đến từ trước, nghĩa là một trong hai khóa đã được cấu hình trong Resolver hoặc phải được nhận biết và xác thực trước đó. Do đó, Resolver phải được cấu hình với ít nhất một Neo tin cậy.

Nếu Neo tin cậy được cấu hình là một ZSK, nó sẽ xác thực zone được liên kết; nếu khóa được cấu hình là một KSK, nó sẽ xác thực một ZSK. Nếu Neo tin cậy được cấu hình là mã Hash của một khóa hay đúng hơn khóa của chính nó, Resolver có thể nhận được khóa thông qua truy vấn DNS. Để trợ giúp các bộ Security-Aware Resolver cấu hình chuỗi xác thực này, các Recurity-Aware Name Server gửi (các) chữ ký xác thực một khóa công khai của (các) zone trong thông báo hồi đáp DNS cùng với khóa công khai của nó và cung cấp không gian sẵn có trong thông điệp.

Bản ghi DS làm đơn giản hóa một số thủ tục định sẵn trong việc ký chuyển giao bằng các giới hạn nhất định. Tập bản ghi DS lưu trú tại một điểm ủy quyền trong một zone cha và chỉ định (các) khóa công khai tương ứng với khoá riêng được sử dụng để tự ký tập bản ghi DNSKEY tại Apex của zone con được ủy quyền. Quản trị của zone con, lần lượt sử dụng (các) khoá riêng tương ứng với một hoặc một vài khóa công khai trong tập bản ghi DNSKEY này để ký dữ liệu của zone con. Chuỗi xác thực điển hình là DNSKEY->[DS->DNSKEY]*->tập bản ghi, trong đó "*" bao hàm không hoặc nhiều chuỗi phụ DS->DNSKEY. DNSSEC cho phép nhiều chuỗi xác thực phức tạp, chẳng hạn như lớp bổ sung của bản ghi DNSKEY ký với bản ghi DNSKEY khác trong một zone.

Một Security-Aware Resolver tạo chuỗi xác thực này từ root của hệ thống phân cấp DNS đến zone dựa trên nhận biết được cấu hình trong khóa công khai từ root này. Chính sách nội bộ cho phép Security-Aware Resolver sử dụng một hoặc nhiều khóa công khai được cấu hình (hoặc mã Hash của các khóa công khai) hơn là một khóa công khai của root, chính sách này có thể không cung cấp một nhận biết được cấu hình về khóa công khai của root, hoặc có thể ngăn chặn Resolver sử dụng khóa công khai một cách tùy ý, ngay cả khi các khóa công khai được ký đúng cách với chữ ký xác minh. DNSSEC cung cấp cơ chế để Security-Aware Resolver có thể xác định một chữ ký của tập bản ghi "hợp lệ". Trong phân tích cuối cùng, chính sách nội bộ xác thực các khóa DNS và dữ liệu, khi đó có thể mở rộng hoặc ghi đè các phần mở rộng giao thức được quy định trong tiêu chuẩn này. Xem tại mục 6.

4.2 Tên xác thực và loại không tồn tại xác thực

Cơ chế bảo mật được mô tả trong mục 4.1 chỉ cung cấp phương pháp cho việc ký các tập bản ghi đã có sẵn trong một zone, việc cung cấp các hồi đáp từ chối với mức xác thực và mức toàn vẹn sử dụng của một loại bản ghi tài nguyên mới, bản ghi NSEC. NSEC cho phép Security-Aware Resolver xác thực một hồi đáp từ chối cho tên xác thực hoặc loại không tồn tại xác thực. Với các hồi đáp DNS khác, Security-Aware Resolver sử dụng các cơ chế tương tự. Việc sử dụng NSEC yêu cầu một đại diện chuẩn và sắp xếp thứ tự các tên miền trong các zone. Các chuỗi của NSEC mô tả rõ các khoảng trống hoặc "không gian trống" giữa các tên miền trong một zone và danh sách các loại tập bản ghi hiện diện tại các tên miền hiện có. Mỗi NSEC được ký và được xác thực bằng cách sử dụng các cơ chế được mô tả trong mục 4.1.

5 Dịch vụ không cung cấp bởi bảo mật DNS

DNS ban đầu được thiết kế với giả định rằng DNS sẽ trả lại cho cùng câu trả lời cho các truy vấn bất kỳ mà không quan tâm đến người thực hiện truy vấn đó, và tất cả dữ liệu trong DNS đều có thể truy vấn được. Theo đó, DNSSEC không được thiết kế để cung cấp tính năng bảo mật, danh sách kiểm soát truy nhập, hoặc phương pháp phân biệt giữa các đối tượng thực hiện truy vấn.

DNSSEC không cung cấp cơ chế bảo vệ chống lại các tấn công từ chối dịch vụ. Các Security-Aware Resolver và các máy chủ tên miền Security-Aware dễ bị tấn công từ một loại bổ sung của tấn công từ chối dịch vụ dựa trên các hoạt động mã hóa (mô tả trong mục 13).

Phần mở rộng bảo mật DNS cung cấp dữ liệu và xác thực gốc cho dữ liệu DNS. Các cơ chế nêu trên không được thiết kế cho các hoạt động bảo vệ cũng như chuyển zone và cập nhật động ([RFC 2136], [RFC 3007]). Việc xác thực thông báo được mô tả trong [RFC 2845] và [RFC 2931] hoạt động bảo mật địa chỉ liên quan đến nghiệp vụ này.

6 Phạm vi của DNSSEC

Các chỉ tiêu kỹ thuật trong tiêu chuẩn này định nghĩa phương thức xử lý cho các chữ ký zone và các máy chủ tên miền Security-Aware và các Resolver theo phương pháp các đối tượng xác minh có thể xác định rõ trạng thái của dữ liệu.

Một Validating Resolver có thể xác định bốn trạng thái sau đây:

- An toàn: Validating Resolver có một Neo tin cậy, có một chuỗi điểm tin cậy, và có thể xác minh tất cả các chữ ký trong các hồi đáp.
- Không an toàn: Validating Resolver có một Neo tin cậy, có một chuỗi điểm tin cậy, và tại một điểm ủy quyền, được ký chứng minh không tồn tại của một bản ghi DS. Điều này chỉ ra các nhánh tiếp theo của cây là không an toàn. Một validating Resolver có thể có chính sách nội bộ để đánh dấu các phần của không gian miền là không an toàn.
- Không có thật: Validating Resolver có một Neo tin cậy và ủy quyền an toàn chỉ ra dữ liệu phụ trợ đã được ký nhưng hồi đáp không thể xác minh đối với một số lý do: thiếu chữ ký, ký quá hạn, ký với các thuật toán không được hỗ trợ, mất dữ liệu các bản ghi NSEC liên quan hiện diện, ...
- Không xác định: Không có Neo tin cậy chỉ ra một phần cụ thể của cây là an toàn. Đây là chế độ hoạt động mặc định.

Đặc tính kỹ thuật này chỉ quy định các Recurity-Aware Name Server có thể ký với các Non-Validating Stub Resolver rằng dữ liệu được tìm thấy không có thật (sử dụng RCODE=2, "Server Failure"; mô tả trong [RFC4035]).

Đây là cơ chế cho các máy chủ tên miền Recurity-Aware ký với các Security-Aware Stub Resolver thông báo dữ liệu được tìm thấy là an toàn (sử dụng bit AD, được mô tả trong [RFC 4035]).

Đặc tính này không định nghĩa định dạng cho thông tin trả lời vì sao hồi đáp được tìm thấy là không có thật hoặc được đánh dấu không an toàn. Cơ chế ký hiện hành không phân biệt giữa zone xác định và zone không an toàn.

Một phương pháp sử dụng cho việc truyền tín hiệu mã lỗi tiên tiến và các chính sách giữa một Security-Aware Stub Resolver và các máy chủ tên miền đệ quy Security-Aware là vấn đề được nghiên cứu trong tương lai, như giao diện giữa một Security-Aware Resolver và các ứng dụng mà nó sử dụng. Lưu ý, việc không đáp ứng đầy đủ các đặc tính của thông tin không ngăn cấm trong việc triển khai các zone đã được ký hoặc việc triển khai các Security Aware Recursive Name Server nhưng ngăn cấm việc lan truyền dữ liệu không có thật cho các ứng dụng.

7 Các yêu cầu đối với Resolver

Một Security-Aware Resolver phải có khả năng thực hiện các chức năng mã hóa cần thiết để xác minh ký số bằng cách sử dụng ít nhất một thuật toán mandatory-to-implement (xem [RFC 4305]). Các Security-Aware Resolver phải có khả năng tạo ra một chuỗi xác thực từ một zone mới được biết từ một khóa xác thực. Việc xử lý này có thể yêu cầu truy vấn thêm vào các zone DNS trung gian để thu được

các bản ghi DNSKEY, DS và RRSIG cần thiết. Một Security-Aware Resolver nên được cấu hình với ít nhất một điểm Neo tin cậy, và coi như điểm bắt đầu cho việc cấu hình chuỗi xác thực.

Trong trường hợp, Security-Aware Resolver được tách ra từ các máy chủ có thẩm quyền liên quan bởi các máy chủ tên miền đệ quy hoặc bất kỳ thiết bị trung gian hoạt động như một proxy của DNS. Nếu Recursive Name Server hoặc thiết bị trung gian này không có chức năng Security-Aware thì Security-Aware Resolver có thể không có khả năng hoạt động trong một chế độ an toàn. Ví dụ, nếu các gói tin của Security-Aware Resolver được chuyển qua một thiết bị địa chỉ mạng (NAT) bao gồm một proxy không có chức năng Security-Aware, Security-Aware Resolver có thể gặp khó khăn trong việc tìm kiếm cũng như không có khả năng nhận hoặc xác thực dữ liệu DNS được ký. Security-Aware Resolver có thể phải mất thời gian để nhận được các bản ghi DS trong trường hợp như vậy, bản ghi DS không thực hiện theo các quy tắc DNS thông thường đối với quyền sở hữu của bản ghi tại các zone cut. Chú ý rằng, vấn đề này không đặc trưng cho NAT: bất kỳ phần mềm Security-Obliviou DNS của bất kỳ loại nào giữa Security-Aware Resolver và các máy chủ có thẩm quyền sẽ giao tiếp với DNSSEC.

Nếu một Security-Aware Resolver phải tin cậy vào một zone không được ký hoặc một máy chủ tên miền không có Security-Aware, Resolver có thể không có khả năng xác thực hồi đáp DNS, khi đó cần một chính sách nội bộ về việc có nên chấp nhận hồi đáp chưa được xác thực hay không.

Một Security-Aware Resolver đòi hỏi một khoảng thời gian cho việc xác minh chữ ký khi xác định TTL của dữ liệu trong bộ nhớ đệm của nó, tránh việc dữ liệu trong bộ nhớ đệm được ký sau thời gian xác minh chữ ký. Tuy nhiên, nó cũng cho phép khả năng đồng hồ của Security-Aware Resolver bị sai. Vì vậy, một Security-Aware Resolver là một phần của một máy chủ tên miền đệ quy Security-Aware phải chú ý đến bit CD "kiểm tra vô hiệu hóa" trong DNSSEC ([RFC 3034]). Điều này tránh tình trạng chữ ký hợp lệ bị chặn bởi các Security-Aware Resolvers khác là các máy khách của máy chủ tên miền đệ quy này. Việc một Secure Recursive Server xử lý truy vấn với cấu hình bit CD được mô tả trong [RFC 4035].

8 Các yêu cầu đối với Stub Resolver

Giao thức không đưa ra các yêu cầu, tuy nhiên, hầu hết các truy vấn DNS có nguồn gốc từ các Stub Resolver. Các Stub Resolver là các DNS Resolver tối giản và sử dụng chế độ truy vấn đệ quy để giảm tải cho các công việc của bộ phân tích DNS đến một máy chủ tên miền đệ quy. Cấu trúc của DNSSEC ghi chép các stub Resolver vào một bảng kê để đáp ứng việc sử dụng rộng rãi các stub Resolver này, nhưng các đặc tính bảo mật cần thiết trong một Stub Resolver và các đặc tính bảo mật trong một Security-Aware Iterative Resolver hoàn toàn khác nhau.

Thậm chí, một Security-Oblivious Stub Resolver có lợi từ DNSSEC nếu các máy chủ tên miền đệ quy được sử dụng là Security-Aware, nhưng nếu Stub Resolver tin tưởng vào các chỉ dẫn DNSSEC, Stub Resolver phải tin cậy vào cả máy chủ tên miền đệ quy trong câu hỏi và các kênh thông tin giữa nó và các máy chủ tên đó. Vấn đề đầu tiên là chính sách nội bộ: về bản chất, một Security-Oblivious Stub Resolver không thực hiện việc kiểm tra hiệu lực DNSSSEC mà tin tưởng vào máy chủ tên miền đệ quy nó sử dụng. Vấn đề thứ hai quy định một số loại cơ chế bảo mật kênh; việc sử dụng hợp lý các cơ chế xác thực giao dịch DNS như SIG(0) ([RFC 2931]) hoặc TSIG ([RFC 2845]), hay sử dụng thích hợp của IPsec. Các bổ sung chi tiết có thể có những lựa chọn có sẵn, chẳng hạn như các cơ chế truyền tin liên

quá trình đặc tính hệ thống điều hành. Các kênh này không cần bảo mật, nhưng tính toàn vẹn dữ liệu và xác thực thông báo cần được bảo mật.Một Security-Aware Stub Resolver tin tưởng vào máy chủ tên miền đệ quy và kênh thông tin để có thể lựa chọn và kiểm tra việc cấu hình bit AD trong tiêu đề thông báo của thông báo hồi đáp nó nhận được. Stub Resolver có thể sử dụng bit flag này để tìm máy chủ tên miền đệ quy đã có chữ ký xác minh đối với tất cả dữ liệu trong phần quyền hạn và trả lời của các hồi đáp.

Nếu vì bất kỳ lý do gì, Security-Aware Stub Resolver không có khả năng cấu hình một mối quan hệ độ tin cậy cần thiết với các máy chủ tên miền đệ quy mà nó sử dụng: nó có thể thực hiện xác minh chữ ký của mình bằng cách cấu hình bit CD trong các thông báo truy vấn. A validating Stub Resolver coi các chữ kỹ DNSSEC như các quan hệ tin cậy giữa các quản trị zone và Stub Resolver của nó.

9 Các yêu cầu đối với zone

Sự khác biệt giữa zone được ký và zone không được ký. Một zone đã được ký bao gồm các bản ghi bảo mật bổ sung (RRSIG, DNSKEY, DS và các NSEC). Các bản ghi RRSIG và NSEC có thể được tạo ra trong quá trình ký trước khi được sử dụng. Các bản ghi RRSIG kèm theo dữ liệu zone đã được xác định khởi đầu và cấu hình thời hạn có hiệu lực cho các chữ ký và dữ liệu zone.

9.1 Các giá trị TTL so với thời gian hiệu lực của RRSIG

Sự khác biệt giữa giá trị TTL của tập bản ghi và thời gian hiệu lực được ký quy định bởi sự bao phủ bản ghi RRSIG là tập bản ghi. DNSSEC không thay đổi định nghĩa hoặc chức năng của giá trị TTL, với mục đích duy trì sự liên kết cơ sở dữ liệu trong các bộ đệm. Một Resolver loại trừ các tập bản ghi từ bộ nhớ đệm của nó trước điểm kết thúc của hiệu lực thời gian được quy định bởi các trường TTL của các tập bản ghi, kể cả khi Resolver này là Security-Aware.

Các trường bắt đầu và kết thúc trong bản ghi RRSIG ([RFC 4034]) chỉ định chu kỳ thời gian chữ ký có thể được sử dụng để xác định tập bản ghi. Các chữ ký được liên kết với dữ liệu zone được ký chỉ có hiệu lực trong chu kỳ thời gian được quy định bởi các trường trong bản ghi RRSIG trong câu hỏi. Các giá trị TTL không thể kéo dài thời gian hiệu lực của tập bản ghi được ký trong bộ đệm của Resolver, nhưng Resolver có thể sử dụng thời gian còn lại trước khi kết thúc thời hạn hiệu lực chữ ký của một tập bản ghi được ký, việc kết thúc là bắt buộc đối với TTL của tập bản ghi đã được ký và được liên kết với bản ghi RRSIG trong bộ đệm của Resolver.

9.2 Các yêu cầu mới về phụ thuộc thời gian trong các zone

Thông tin trong một zone được ký tạm thời nhưng không tồn tại trong giao thức DNS gốc. Việc bảo trì zone được ký phải thường xuyên để đảm bảo mỗi tập bản ghi trong zone có một giá trị hiện hành bản ghi RRSIG. Thời gian hiệu lực chữ ký của một bản ghi RRSIG là khoảng thời gian có hiệu lực diễn ra việc ký nhận đối với mỗi tập bản ghi, và việc ký của các tập bản ghi khác nhau trong một zone có thể hết hiệu lực tại các thời điểm khác nhau. Việc ký lại một hoặc nhiều tập bản ghi sẽ thay đổi một hoặc nhiều bản ghi RRSIG, việc này làm tăng số dãy SOA của zone và cho biết đã xảy ra sự thay đổi zone và ký lại tập bản ghi SOA của chính nó. Do đó, việc ký lại bất kỳ tập bản ghi trong một zone có thể gây ra thông báo DNS NOTIFY và các hoạt động chuyển giao zone.

10 Các yêu cầu đối với máy chủ tên miền

Một máy chủ tên miền Recurity-Aware bao gồm các bản ghi DNSSEC thích hợp (RRSIG, DNSKEY, DS, và NSEC) trong tất cả các hồi đáp cho các truy vấn từ các Resolver và báo hiệu việc sẵn sàng nhận các bản ghi thông qua sử dụng bit DO trong tiêu đề EDNS, tùy thuộc vào giới hạn kích thước thông báo. Bởi vì, tập hợp của các bản ghi DNSSEC này có thể dễ dàng gây ra sự cắt xén thông báo UDP và dự phòng tới TCP, một máy chủ tên miền Recurity-Aware phải hỗ trợ cơ chế "tải UDP của người gửi" EDNS.

Nếu có thể, một nửa của mỗi khóa DNSSEC nên được giữ ngoại tuyến, nhưng không áp dụng cho zone cập nhật động DNS đã được kích hoạt. Trong trường hợp cập nhật động, Primary Master Server của zone ký lại zone khi được cập nhật, vì vậy khóa chính tương ứng với ZSK phải được giữ trực tuyến.

DNSSEC không thể đảm bảo tính toàn vẹn của toàn bộ zone trong suốt các hoạt động chuyển zone, vì vậy một zone được ký vẫn có thể chứa phần chưa được ký, dữ liệu chưa xác thực nếu zone đó không có zone con. Do đó, hoạt động bảo trì zone đòi hỏi một số cơ chế bổ sung (như hình thức bảo mật kênh TSIG, SIG(0) hoặc IPsec).

11 Họ tài liệu bảo mật DNS

Tập hợp tài liệu về DNSSEC có thể được phân chia thành nhiều nhóm chính, dưới sự bảo trợ của các tài liệu giao thức cơ sở DNS.

"Tập tài liệu giao thức DNSSEC" đề cập đến ba tài liệu là chính của phần mở rộng bảo mật DNS:

1) Các yêu cầu và hướng dẫn bảo mật DNS ([RFC 4033]).
2) Bản ghi tài nguyên cho phần mở rộng bảo mật DNS ([RFC 4034]).
3) Các thay đổi trong giao thức cho phần mở rộng bảo mật DNS ([RFC 4035]).

Ngoài ra, bất kỳ tiêu chuẩn nào được thêm vào hoặc thay đổi tài liệu chính của phần mở rộng bảo mật DNS sẽ nằm trong nhóm này. Điều này bao gồm bất cứ việc làm trong tương lai liên quan đến giao tiếp giữa Security-Aware Stub Resolvers và máy chủ tên miền đệ quy Security-Aware ngược tuyến.

Nhóm các tiêu chuẩn "Chỉ tiêu kỹ thuật thuật toán ký số" mô tả cụ thể các thuật toán ký số cần được thực hiện để phù hợp với các định dạng bản ghi tài nguyên DNSSEC. Mỗi tài liệu này là một thuật toán ký số cụ thể. Phụ lục "Các loại thuật toán và phân loại DNS" mô tả trong [RFC 4034] cung cấp danh sách các thuật toán được định nghĩa khi các chỉ tiêu kỹ thuật chính này được xây dựng. "Giao thức xác thực giao dịch" đề cập đến giải quyết xác thực thông báo DNS bao gồm cấu hình khóa riêng và xác thực.

Tiêu chuẩn cuối cùng "Sử dụng bảo mật mới" đề cập tới các tiêu chuẩn tìm cách sử dụng đề xuất các phần mở rộng bảo mật DNS đối với các bảo mật khác có liên quan. DNSSEC không cung cấp bất kỳ bảo mật trực tiếp nào đối với các bảo mật mới này nhưng có thể được sử dụng để hỗ trợ. Các tài liệu này nằm trong nhóm mô tả việc sử dụng DNS trong lưu trữ và phân phối chứng chỉ [RFC2538].

12 Các yêu cầu của IANA

Các yêu cầu của IANA được đề cập trong [RFC 4034].

13 Các yêu cầu đối với bảo mật

Tiêu chuẩn này giới thiệu phần mở rộng bảo mật DNS và mô tả tập tài liệu có chứa các bản ghi bảo mật mới và các thay đổi trong giao thức DNS. Phần mở rộng cung cấp xác thực dữ liệu gốc và toàn vẹn dữ liệu bằng cách sử dụng ký số trên các tập bản ghi tài nguyên.

Mục này đưa ra các hạn chế của phần mở rộng.

Để một Security-Aware Resolver xác minh một hồi đáp DNS, tất cả các zone dọc theo đường dẫn từ điểm bắt đầu được tin cậy tại zone chứa các zone hồi đáp phải được ký, và tất cả máy chủ tên miền và các Resolver liên quan trong quá trình phân tích phải là Security-Aware như mô tả trong tiêu chuẩn này. Một Security-Aware Resolver không thể xác thực nguồn gốc hồi đáp từ một zone không được ký, từ zone không được chỉ dẫn bởi một máy chủ tên miền Recurity-Aware, hoặc từ bất kỳ dữ liệu DNS không được nhận biết thông qua máy chủ tên miền đệ quy Security-Aware. Nếu chuỗi xác thực bị phá vỡ thì Security-Aware Resolver không thể xác minh các khóa xác thực cần thiết, sau đó Security-Aware Resolver này không thể xác minh dữ liệu DNS bị hư hỏng.

Tiêu chuẩn này đưa ra các phương pháp bảo mật bổ sung cho một truy vấn DNS, ví dụ sử dụng một kênh được bảo mật bởi IPsec hoặc sử dụng một cơ chế xác thực giao dịch DNS như TSIG ([RFC 2845]) hoặc SIG(0) ([RFC 2931]), nhưng bảo mật giao dịch không phải là một phần của DNSSEC.

Một non-validating Security-Aware Stub Resolver không thực hiện việc xác minh chữ ký DNSSEC trên chính nó, do đó, nó dễ bị ảnh hưởng khi bị tấn công vào máy chủ tên miền đệ quy Security-Aware do việc thực hiện kiểm tra trên đại diện của nó và bị tấn công vào giao tiếp của nó với các máy chủ tên miền đệ quy Security-Aware. Các Non-validating Security-Aware Stub Resolver nên sử dụng một số hình thức bảo mật kênh để chống lại các mối đe dọa sau này. Security-Aware Stub Resolver chống lại các mối đe dọa thông qua việc xác minh chữ ký của nó, lúc này nó sẽ không còn là Non-Validating Security-Aware Stub Resolver.

DNSSEC không bảo vệ chống lại tấn công từ chối dịch vụ (DoS). DNSSEC làm cho DNS dễ bị ảnh hưởng đến một loại mới của DoS dựa trên hoạt động mã hóa chống lại các Security-Aware Resolver và các máy chủ tên miền Recurity-Aware, ví dụ, kẻ tấn công có thể cố gắng sử dụng các cơ chế DNSSEC để tiêu hao tài nguyên của đối tượng bị tấn công. Loại tấn công này tồn tại ít nhất hai hình thức. Kẻ tấn công có thể tiêu hao mã xác minh chữ ký của một Security-Aware Resolver bằng cách giả mạo các thông báo hỏi đáp trong các bản ghi RRSIG hoặc bằng cách tạo ra các chuỗi chữ kỹ phức tạp. Kẻ tấn công có thể tiêu thụ các tài nguyên trong một máy chủ tên miền Recurity-Aware hỗ trợ cập nhật động DNS, bằng cách gửi một dòng thông báo cập nhật, bắt buộc máy chủ tên miền Recurity-Aware ký lại các tập bản ghi trong zone với tần suất bất thường.

Một thiết kế có lựa chọn là DNSSEC không cung cấp bảo mật.

DNSSEC giới thiệu một khả năng cho kẻ tấn công để liệt kê tất cả các tên miền trong zone bởi một chuỗi NSEC sau đây. NSEC xác minh rằng tên miền không tồn tại trong một zone bởi các liên kết từ tên đã tạo sẵn đến tên đã tạo sẵn theo một trật tự chuẩn của tất cả các tên miền trong một zone. Do đó, kẻ tấn công có thể truy vấn các bản ghi NSEC trong dãy để thu được tất cả các tên miền trong zone. Mặc dù, không tấn công vào DNS của chính nó, nó có thể cho phép kẻ tấn công sắp xếp các network host hoặc các tài nguyên khác bằng cách liệt kê các nội dung của một zone.

DNSSEC không bảo vệ chống giả mạo với dữ liệu zone không được ký. Dữ liệu không được xác thực tại các zone cut (các bản ghi NS trong zone con) không được ký. Việc này không xảy ra vấn đề khi xác minh chuỗi xác thực, nhưng nó có nghĩa là dữ liệu "non-authoritative" của nó dễ bị xáo trộn trong suốt các hoạt động chuyển zone. Do đó, trong khi DNSSEC có thể cung cấp xác thực nguồn gốc dữ liệu và toàn vẹn dữ liệu đối với các tập bản ghi, nó không thể làm như vậy đối với các zone, và các cơ chế khác (như TSIG, SIG (0), hoặc IPsec) phải được sử dụng để bảo vệ các hoạt động chuyển giao zone. (xem [RFC 4034] và [RFC 4035] đối với các yêu cầu bảo mật bổ sung).

Phụ lục A

(Quy định)

Các RFC cập nhật

Phụ lục này chỉ trình bày các thông tin được cập nhật cho tiêu chuẩn này.

A.1 RFC 6014 "Cryptographic Algorithm Identifier Allocation for DNSSEC" - RFC 6014 "Định dạng các thuật toán mã hóa dùng cho DNSSEC" (11-2010)

RFC 6014 (11-2010) thay đổi yêu cầu về ký từ một RFC tiêu chuẩn tham chiếu sang một RFC được xuất bản dưới bất kỳ loại nào.

Trong Mục "2. Các yêu cầu về ấn định trong việc ký số thuật toán bảo mật DNS" tại Trang 3 của RFC 6014 (11-2010):

Có hai lý do để quy định yêu cầu là:

- Có một số thuật toán có ích không thể nằm trong một RFC tiêu chuẩn tham chiếu. Vì các lý do nào đó, một thuật toán có thể đã không được đánh giá đủ kỹ lưỡng để có thể thành một tiêu chuẩn tham chiếu. Hoặc là thuật toán đó có thể có quyền sở hữu trí tuệ không rõ ràng đã ngăn cản thuật toán này được xây dựng thành một tiêu chuẩn tham chiếu.
- Mặc dù không gian ký bị hạn chế (khoảng 250 số), các thuật toán mới được đề xuất không thường xuyên. Nó có thể kéo dài nhiều thập kỷ trước khi có một lý do nào đó để xem xét lại việc hạn chế được ký. Một số nhà phát triển sẽ quan tâm đến mức tiêu chuẩn của các RFC trong việc ký. Việc ký đã được cập nhật để phản ánh mức tiêu chuẩn hiện tại của từng thuật toán được liệt kê.

Để giải quyết những lo ngại về việc đầy ký số, IETF nên đánh giá lại các yêu cầu đối với ký số khi ký số được ấn định xấp xỉ 120. Việc đánh giá này có thể dẫn đến những hạn chế chặt chẽ hơn hoặc một cơ chế mới để mở rộng không gian ký. Để việc đánh giá khả thi hơn, IANA đã đánh dấu khoảng một nửa ký số khả dụng là "dự phòng" để việc đánh giá lại này có thời gian rõ ràng hơn.

Các giá trị 253 và 254 vẫn được dành cho các nhà phát triển muốn kiểm tra các thuật toán không nằm trong một RFC. Tiêu chuẩn này không làm thay đổi cú pháp của hai giá trị này.

A.2 RFC 6840 "Clarifications and Implementation Notes for DNS Security (DNSSEC)" - RFC 6840 "Các chú ý làm rõ và thực hiện đối với bảo mật DNS (DNSSEC)" (02-2013)

Trong Mục "2. Những bổ sung quan trọng DNS" tại Trang 4 của RFC 6840 (02-2013) liệt kê các tài liệu được coi là cốt lõi của các tài liệu giao thức DNS không được chỉ ra tại mục 11 của tiêu chuẩn này.

A.2.1 Hỗ trợ NSEC3

RFC 5155 mô tả việc sử dụng và xử lý các bản ghi NSEC3 và NSEC3 PARAM đối với chứng cứ không tồn tại đã bị làm hỏng. Những bổ sung hợp lý này được khuyến khích trong đó bao gồm hỗ trợ cho NSEC3 bởi vì một số zone có thể xác định được sử dụng nó. Những bổ sung không hỗ trợ xác minh hồi đáp bằng các sử dụng NSEC3 bị ngăn cản trong việc xác thực phần lớn không gian DNS.

[RFC 5155] xem xét phần họ tiêu chuẩn bảo mật DNS được mô tả tại mục 11 của tiêu chuẩn này đối với việc hỗ trợ NSEC3.

A.2.2 Hỗ trợ SHA-2

[RFC 4509] mô tả việc sử dụng SHA-256 bằng thuật toán phân loại trong các bản ghi DS. [RFC 5702] mô tả việc sử dụng thuật toán RSASHA256 và SRASHA512 trong các bản ghi DNSKEY và RRSIG.

Những bổ sung hợp lý này được khuyến khích bao gồm hỗ trợ cho các thuật toán các bản ghi DS, DNSKEY và RRSIG.

[RFC 4509] và [RFC 5702] xem xét phần Họ tiêu chuẩn bảo mật DNS được mô tả tại mục 11 của tiêu chuẩn này đối với việc hỗ trợ SHA-2.

Thư mục tài liệu tham khảo

[1] [RFC 4033] "DNS Security Introduction and Requirements", (03-2005).

[2] [RFC 6014] "Cryptographic Algorithm Identifier Allocation for DNSSEC", (10-2010).

[3] [RFC 6840] "Clarifications and Implementation Notes for DNS Security (DNSSEC)", (02-2013).