

Network Working Group
Request for Comments: 2535
Obsoletes: 2065
Updates: 2181, 1035, 1034
Category: Standards Track

D. Eastlake
IBM
March 1999

Domain Name System Security Extensions

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

Extensions to the Domain Name System (DNS) are described that provide data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can also be provided through non-security aware DNS servers in some cases.

The extensions provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution services as well as DNS security. The stored keys enable security aware resolvers to learn the authenticating key of zones in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. Provision is made for a variety of key types and algorithms.

In addition, the security extensions provide for the optional authentication of DNS protocol transactions and requests.

This document incorporates feedback on RFC 2065 from early implementers and potential users.

Acknowledgments

The significant contributions and suggestions of the following persons (in alphabetic order) to DNS security are gratefully acknowledged:

- James M. Galvin
- John Gilmore
- Olafur Gudmundsson
- Charlie Kaufman
- Edward Lewis
- Thomas Narten
- Radia J. Perlman
- Jeffrey I. Schiller
- Steven (Xunhua) Wang
- Brian Wellington

Table of Contents

Abstract.....1

Acknowledgments.....2

1. Overview of Contents.....4

2. Overview of the DNS Extensions.....5

2.1 Services Not Provided.....5

2.2 Key Distribution.....5

2.3 Data Origin Authentication and Integrity.....6

2.3.1 The SIG Resource Record.....7

2.3.2 Authenticating Name and Type Non-existence.....7

2.3.3 Special Considerations With Time-to-Live.....7

2.3.4 Special Considerations at Delegation Points.....8

2.3.5 Special Considerations with CNAME.....8

2.3.6 Signers Other Than The Zone.....9

2.4 DNS Transaction and Request Authentication.....9

3. The KEY Resource Record.....10

3.1 KEY RDATA format.....10

3.1.1 Object Types, DNS Names, and Keys.....11

3.1.2 The KEY RR Flag Field.....11

3.1.3 The Protocol Octet.....13

3.2 The KEY Algorithm Number Specification.....14

3.3 Interaction of Flags, Algorithm, and Protocol Bytes...15

3.4 Determination of Zone Secure/Unsecured Status.....15

3.5 KEY RRs in the Construction of Responses.....17

4. The SIG Resource Record.....17

4.1 SIG RDATA Format.....17

4.1.1 Type Covered Field.....18

4.1.2 Algorithm Number Field.....18

4.1.3 Labels Field.....18

4.1.4 Original TTL Field.....19

4.1.5 Signature Expiration and Inception Fields.....	19
4.1.6 Key Tag Field.....	20
4.1.7 Signer's Name Field.....	20
4.1.8 Signature Field.....	20
4.1.8.1 Calculating Transaction and Request SIGs.....	21
4.2 SIG RRs in the Construction of Responses.....	21
4.3 Processing Responses and SIG RRs.....	22
4.4 Signature Lifetime, Expiration, TTLs, and Validity....	23
5. Non-existent Names and Types.....	24
5.1 The NXT Resource Record.....	24
5.2 NXT RDATA Format.....	25
5.3 Additional Complexity Due to Wildcards.....	26
5.4 Example.....	26
5.5 Special Considerations at Delegation Points.....	27
5.6 Zone Transfers.....	27
5.6.1 Full Zone Transfers.....	28
5.6.2 Incremental Zone Transfers.....	28
6. How to Resolve Securely and the AD and CD Bits.....	29
6.1 The AD and CD Header Bits.....	29
6.2 Staticly Configured Keys.....	31
6.3 Chaining Through The DNS.....	31
6.3.1 Chaining Through KEYs.....	31
6.3.2 Conflicting Data.....	33
6.4 Secure Time.....	33
7. ASCII Representation of Security RRs.....	34
7.1 Presentation of KEY RRs.....	34
7.2 Presentation of SIG RRs.....	35
7.3 Presentation of NXT RRs.....	36
8. Canonical Form and Order of Resource Records.....	36
8.1 Canonical RR Form.....	36
8.2 Canonical DNS Name Order.....	37
8.3 Canonical RR Ordering Within An RRset.....	37
8.4 Canonical Ordering of RR Types.....	37
9. Conformance.....	37
9.1 Server Conformance.....	37
9.2 Resolver Conformance.....	38
10. Security Considerations.....	38
11. IANA Considerations.....	39
References.....	39
Author's Address.....	41
Appendix A: Base 64 Encoding.....	42
Appendix B: Changes from RFC 2065.....	44
Appendix C: Key Tag Calculation.....	46
Full Copyright Statement.....	47

1. Overview of Contents

This document standardizes extensions of the Domain Name System (DNS) protocol to support DNS security and public key distribution. It assumes that the reader is familiar with the Domain Name System, particularly as described in RFCs 1033, 1034, 1035 and later RFCs. An earlier version of these extensions appears in RFC 2065. This replacement for that RFC incorporates early implementation experience and requests from potential users.

Section 2 provides an overview of the extensions and the key distribution, data origin authentication, and transaction and request security they provide.

Section 3 discusses the KEY resource record, its structure, and use in DNS responses. These resource records represent the public keys of entities named in the DNS and are used for key distribution.

Section 4 discusses the SIG digital signature resource record, its structure, and use in DNS responses. These resource records are used to authenticate other resource records in the DNS and optionally to authenticate DNS transactions and requests.

Section 5 discusses the NXT resource record (RR) and its use in DNS responses including full and incremental zone transfers. The NXT RR permits authenticated denial of the existence of a name or of an RR type for an existing name.

Section 6 discusses how a resolver can be configured with a starting key or keys and proceed to securely resolve DNS requests. Interactions between resolvers and servers are discussed for various combinations of security aware and security non-aware. Two additional DNS header bits are defined for signaling between resolvers and servers.

Section 7 describes the ASCII representation of the security resource records for use in master files and elsewhere.

Section 8 defines the canonical form and order of RRs for DNS security purposes.

Section 9 defines levels of conformance for resolvers and servers.

Section 10 provides a few paragraphs on overall security considerations.

Section 11 specified IANA considerations for allocation of additional values of parameters defined in this document.

Appendix A gives details of base 64 encoding which is used in the file representation of some RRs defined in this document.

Appendix B summarizes changes between this memo and RFC 2065.

Appendix C specified how to calculate the simple checksum used as a key tag in most SIG RRs.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Overview of the DNS Extensions

The Domain Name System (DNS) protocol security extensions provide three distinct services: key distribution as described in Section 2.2 below, data origin authentication as described in Section 2.3 below, and transaction and request authentication, described in Section 2.4 below.

Special considerations related to "time to live", CNAMEs, and delegation points are also discussed in Section 2.3.

2.1 Services Not Provided

It is part of the design philosophy of the DNS that the data in it is public and that the DNS gives the same answers to all inquirers. Following this philosophy, no attempt has been made to include any sort of access control lists or other means to differentiate inquirers.

No effort has been made to provide for any confidentiality for queries or responses. (This service may be available via IPSEC [RFC 2401], TLS, or other security protocols.)

Protection is not provided against denial of service.

2.2 Key Distribution

A resource record format is defined to associate keys with DNS names. This permits the DNS to be used as a public key distribution mechanism in support of DNS security itself and other protocols.

The syntax of a KEY resource record (RR) is described in Section 3. It includes an algorithm identifier, the actual public key parameter(s), and a variety of flags including those indicating the type of entity the key is associated with and/or asserting that there is no key associated with that entity.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.