[redacted] Ask

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.

VIRNETX EXHIBIT 2016

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

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.