RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)

Donald E. Eastlake 3rd

Status of This Document

[Changes from the previous draft: change date, update author info, add RFC 2119 reference]

Abstract

A standard method for storing RSA keys and and RSA/MD5 based signatures in the Domain Name System is described which utilizes DNS KEY and SIG resource records.

Table of Contents

1. Introduction

The Domain Name System (DNS) is the global hierarchical replicated distributed database system for Internet addressing, mail proxy, and other information. The DNS has been extended to include digital signatures and cryptographic keys as described in [draft-ietf-dnssec-secext2-*]. Thus the DNS can now be secured and used for secure key distribution.

This document describes how to store RSA keys and and RSA/MD5 based signatures in the DNS. Familiarity with the RSA algorithm is assumed [Schneier]. Implementation of the RSA algorithm in DNS is recommended.

The key words "MUST", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in RFC 2119.

2. RSA Public KEY Resource Records

RSA public keys are stored in the DNS as KEY RRs using algorithm number 1 [draft-ietf-dnssec-secext2-*]. The structure of the algorithm specific portion of the RDATA part of such RRs is as shown below.

```
     Field             Size
     -----             ----
     exponent length   1 or 3 octets (see text)
     exponent          as specified by length field
     modulus           remaining space
```

For interoperability, the exponent and modulus are each currently limited to 4096 bits in length. The public key exponent is a variable length unsigned integer. Its length in octets is represented as one octet if it is in the range of 1 to 255 and by a zero octet followed by a two octet unsigned length if it is longer than 255 bytes. The public key modulus field is a multiprecision unsigned integer. The length of the modulus can be determined from the RDLENGTH and the preceding RDATA fields including the exponent. Leading zero octets are prohibited in the exponent and modulus.

3. RSA/MD5 SIG Resource Records

The signature portion of the SIG RR RDATA area, when using the RSA/MD5 algorithm, is calculated as shown below. The data signed is determined as specified in [draft-ietf-dnssec-secext2-*]. See [draft-ietf-dnssec-secext2-*] for fields in the SIG RR RDATA which precede the signature itself.

```
hash = MD5 ( data )

signature = ( 01 | FF* | 00 | prefix | hash ) ** e (mod n)
```

where MD5 is the message digest algorithm documented in [RFC 1321], "|" is concatenation, "e" is the private key exponent of the signer, and "n" is the modulus of the signer's public key. 01, FF, and 00 are fixed octets of the corresponding hexadecimal value. "prefix" is the ASN.1 BER MD5 algorithm designator prefix specified in PKCS1, that is,

hex 3020300c06082a864886f70d020505000410 [NETSEC].

This prefix is included to make it easier to use RSAREF (or similar packages such as EuroRef). The FF octet MUST be repeated the maximum number of times such that the value of the quantity being exponentiated is one octet shorter than the value of n.

(The above specifications are identical to the corresponding part of Public Key Cryptographic Standard #1 [PKCS1].)

The size of n, including most and least significant bits (which will be 1) MUST be not less than 512 bits and not more than 4096 bits. n and e SHOULD be chosen such that the public exponent is small.

Leading zero bytes are permitted in the RSA/MD5 algorithm signature.

A public exponent of 3 minimizes the effort needed to verify a signature. Use of 3 as the public exponent is weak for confidentiality uses since, if the same data can be collected encrypted under three different keys with an exponent of 3 then, using the Chinese Remainder Theorem [NETSEC], the original plain text can be easily recovered. This weakness is not significant for DNS security because we seek only authentication, not confidentiality.

4. Performance Considerations

General signature generation speeds are roughly the same for RSA and DSA [RFC xDSA]. With sufficient pre-computation, signature generation with DSA is faster than RSA. Key generation is also faster for DSA. However, signature verification is an order of magnitude slower with DSA when the RSA public exponent is chosen to be small as is recommended for KEY RRs used in domain name system (DNS) data authentication.

Current DNS implementations are optimized for small transfers, typically less than 512 bytes including overhead. While larger transfers will perform correctly and work is underway to make larger transfers more efficient, it is still advisable at this time to make reasonable efforts to minimize the size of KEY RR sets stored within the DNS consistent with adequate security. Keep in mind that in a secure zone, at least one authenticating SIG RR will also be returned.

5. Security Considerations

Many of the general security consideration in [draft-ietf-dnssec-secext2-*] apply. Keys retrieved from the DNS should not be trusted unless (1) they have been securely obtained from a secure resolver or independently verified by the user and (2) this secure resolver and secure obtainment or independent verification conform to security policies acceptable to the user. As with all cryptographic algorithms, evaluating the necessary strength of the key is essential and dependent on local policy.

For interoperability, the RSA key size is limited to 4096 bits. For particularly critical applications, implementors are encouraged to consider the range of available algorithms and key sizes.

References

[NETSEC] - Network Security: PRIVATE Communications in a PUBLIC World, Charlie Kaufman, Radia Perlman, & Mike Speciner, Prentice Hall Series in Computer Networking and Distributed Communications, 1995.

[PKCS1] - PKCS #1: RSA Encryption Standard, RSA Data Security, Inc., 3 June 1991, Version 1.4. [there is an ID on this and any resulting RFC could be substitutes if available in time]

[RFC 1034] - P. Mockapetris, "Domain names - concepts and facilities", 11/01/1987.

[RFC 1035] - P. Mockapetris, "Domain names - implementation and specification", 11/01/1987.

[RFC 1321] - R. Rivest, "The MD5 Message-Digest Algorithm", April 1992.

[draft-ietf-dnssec-secext2-*] - Domain Name System Security Extensions, D. Eastlake, C. Kaufman, January 1997.

[RFC xDSA] - draft-ietf-dnssec-dss-*.txt

[Schneier] - Bruce Schneier, "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", 1996, John Wiley and Sons, ISBN 0-471-11709-9.

Author's Address

Donald E. Eastlake 3rd
IBM
318 Acton Street
Carlisle, MA 01741 USA

Telephone: +1-978-287-4877
+1-914-784-7913
FAX: +1-978-371-7148
EMail: dee3@us.ibm.com

Expiration and File Name

This draft expires in April 1999.

Its file name is draft-ietf-dnssec-rsa-01.txt.