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

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

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

Table of Contents

Abstract...................................................1
1. Introduction..........................................1
2. RSA Public KEY Resource Records....................2
3. RSA/MD5 SIG Resource Records.......................2
4. Performance Considerations.........................3
5. Security Considerations.............................4
References...............................................4
Author’s Address........................................5
Full Copyright Statement..............................6

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 [RFC 2535]. 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 [RFC 2535]. The structure of the algorithm specific portion of the RDATA part of such RRs is as shown below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>exponent length</td>
<td>1 or 3 octets (see text)</td>
</tr>
<tr>
<td>exponent</td>
<td>as specified by length field</td>
</tr>
<tr>
<td>modulus</td>
<td>remaining space</td>
</tr>
</tbody>
</table>

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 RDLLENGTH 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 [RFC 2535]. See [RFC 2535] for fields in the SIG RR RDATA which precede the signature itself.

\[
\text{hash} = \text{MD5} (\text{data})
\]

\[
\text{signature} = (00 | 01 | \text{FF}^* | 00 | \text{prefix} | \text{hash})^{\ast\ast\ast} \text{e (mod n)}
\]
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 [RFC
2437], that is,

    hex 3020300c06082a864886f70d0205050010 [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 the same length in octets as the value of n.

(The above specifications are identical to the corresponding part of
Public Key Cryptographic Standard #1 [RFC 2437].)

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 2536].  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 [RFC 2535] 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


Author’s Address

Donald E. Eastlake 3rd
IBM
65 Shindegan Hill Road, RR #1
Carmel, NY 10512

Phone: +1-914-276-2668(h)
      +1-914-784-7913(w)
Fax:   +1-914-784-3833(w)
EMail: dee3@us.ibm.com
Full Copyright Statement

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

This document and translations of it may be copied and furnished to
others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published
and distributed, in whole or in part, without restriction of any
kind, provided that the above copyright notice and this paragraph are
included on all such copies and derivative works. However, this
document itself may not be modified in any way, such as by removing
the copyright notice or references to the Internet Society or other
Internet organizations, except as needed for the purpose of
developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be
followed, or as required to translate it into languages other than
English.

The limited permissions granted above are perpetual and will not be
revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an
"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING
TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION
HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.