DSA Keying and Signature Information in the DNS

<draft-ietf-dnsext-rfc2536bis-dsa-08.txt>
Donald E. Eastlake 3rd

Status of This Document

Abstract

The standard method of encoding US Government Digital Signature Algorithm keying and signature information for use in the Domain Name System is specified.

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 [RFC1034], [RFC1035]. The DNS has been extended to include digital signatures and cryptographic keys as described in [RFC4033], [RFC4034], [RFC4035] and there is additional work which would use the storage of keying information in the DNS such as IPSECKEY [RFC4025]. This document does not change the wire format of KEY RR's but extends the use of DSA DNS keys to cover the DNSKEY RR.

This document describes how to encode US Government Digital Signature Algorithm (DSA) keys and signatures in the DNS. Familiarity with the US Digital Signature Algorithm is assumed [FIPS186-2], [Schneier].

2. DSA Keying Information

When DSA public keys are stored in the DNS, the structure of the relevant part of the RDATA part of the RR (currently KEY and DNSKEY) being used is the fields listed below in the order given.

The period of key validity is not included in this data but is indicated separately, for example by an RR such as RRSIG which signs and authenticates the RR containing the keying information.

Field	Size
T	1 octet
Q	20 octets
P	64 + T*8 octets
G	64 + T*8 octets
Y	64 + T*8 octets

As described in [FIPS186-2] and [Schneier], T is a key size parameter chosen such that 0 <= T <= 8. (The meaning if the T octet is greater than 8 is reserved and the remainder of the data may have a different format in that case.) Q is a prime number selected at key generation time such that 2**159 < Q < 2**160. Thus Q is always 20 octets long and, as with all other fields, is stored in "big-endian" network order. P, G, and Y are calculated as directed by the [FIPS186-2] key generation algorithm [Schneier]. P is in the range 2**(511+64*T) < P < 2**(512+64*T) and thus is 64 + 8*T octets long. G and Y are quantities modulo P and so can be up to the same length as P and are allocated fixed size fields with the same number of octets as P.

During the key generation process, a random number X must be generated such that 1 <= X <= Q-1. X is the private key and is used

in the final step of public key generation where Y is computed as

```
Y = G**X mod P
```

3. DSA Signature Information

The portion of the RDATA area used for US Digital Signature Algorithm signature information is shown below with fields in the order they are listed and the contents of each multi-octet field in "big-endian" network order.

Field	Size
T	1 octet
R	20 octets
S	20 octets

First, the data signed must be determined. Then the following steps are taken, as specified in [FIPS186-2], where Q, P, G, and Y are as specified in the public key [Schneier]:

```
hash = SHA-1 ( data )

Generate a random K such that 0 < K < Q.

R = ( G**K mod P ) mod Q

S = ( K**(-1) * (hash + X*R) ) mod Q
```

For information on the SHA-1 hash function see [FIPS180-2] and [RFC3174].

Since Q is 160 bits long, R and S can not be larger than 20 octets, which is the space allocated.

T is copied from the public key. It is not logically necessary in an RRSIG but is present so that values of T > 8 can more conveniently be used as an escape for extended versions of DSA or other algorithms as later standardized.

4. Performance Considerations

General signature generation speeds are roughly the same for RSA [RFC3110] and DSA. With sufficient pre-computation, signature generation with DSA is faster than RSA. Key generation is also faster for DSA. However, DSA signature verification is an order of magnitude slower than RSA when the RSA public exponent is chosen to

be small, as is recommended for some applications.

Current DNS implementations are optimized for small transfers, typically less than 512 bytes including DNS overhead. Larger transfers will perform correctly and extensions have been standardized [RFC2671] to make larger transfers more efficient, it is still advisable at this time to make reasonable efforts to minimize the size of RR sets containing keying and/or signature information consistent with adequate security.

5. Security Considerations

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 security policy.

The key size limitation of a maximum of 1024 bits (T = 8) in the referenced DSA standard [FIPS186-2] may limit the security of DSA. For particular applications, implementers are encouraged to consider the range of available algorithms and key sizes.

DSA assumes the ability to frequently generate high quality random numbers. See [RFC4086] for guidance. DSA is designed so that if biased rather than random numbers are used, high bandwidth covert channels are possible. See [Schneier] and more recent research. The leakage of an entire DSA private key in only two DSA signatures has been demonstrated. DSA provides security only if trusted implementations, including trusted random number generation, are used.

6. IANA Considerations

Allocation of meaning to values of the T parameter that are not defined herein (i.e., > 8) requires an IETF standards actions. It is intended that values unallocated herein be used to cover future extensions of the DSS standard.

Appendix A: Example RRs

This section provides an example DNSKEY and corresponding RRSIG RR. All numbers below in this Appendix are in hexadecimal.

The elements of the DSA key are as follows:

```
   T = 00
   Q = c773218c 737ec8ee 993b4f2d ed30f48e dace915f
   P = 8df2a494 492276aa 3d25759b b06869cb eac0d83a fb8d0cf7
       cbb8324f 0d7882e5 d0762fc5 b7210eaf c2e9adac 32ab7aac
       49693dfb f83724c2 ec0736ee 31c80291
   G = 626d0278 39ea0a13 413163a5 5b4cb500 299d5522 956cefcb
       3bff10f3 99ce2c2e 71cb9de5 fa24babf 58e5b795 21925c9c
       c42e9f6f 464b088c c572af53 e6d78802
   Y = 19131871 d75b1612 a819f29d 78d1b0d7 346f7aa7 7bb62a85
       9bfd6c56 75da9d21 2d3a36ef 1672ef66 0b8c7c25 5cc0ec74
       858fba33 f44c0669 9630a76b 030ee333
```

Based on this, the RDATA portion of a zone signing DSNKEY RR would be as show below where "F" is the flags field, "p" is the "protocol" field, and "a" is the algorithm field.

```
          01 00030300 c773218c 737ec8ee 993b4f2d ed30f48e
          F>   p>a>T> Q>
    dace915f 8df2a494 492276aa 3d25759b b06869cb eac0d83a
             P>
    fb8d0cf7 cbb8324f 0d7882e5 d0762fc5 b7210eaf c2e9adac
    32ab7aac 49693dfb f83724c2 ec0736ee 31c80291 626d0278
                                                G>
    39ea0a13 413163a5 5b4cb500 299d5522 956cefcb 3bff10f3
    99ce2c2e 71cb9de5 fa24babf 58e5b795 21925c9c c42e9f6f
    464b088c c572af53 e6d78802 19131871 d75b1612 a819f29d
                               Y>
    78d1b0d7 346f7aa7 7bb62a85 9bfd6c56 75da9d21 2d3a36ef
    1672ef66 0b8c7c25 5cc0ec74 858fba33 f44c0669 9630a76b
    030ee333
```

The Key Tag for the above DNSKEY RDATA, whose RDLENGTH is 00d9, is 19a3.

Assume that the hash of the DNS data being signed is

```
      a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```

the resulting signature value would be

```
   T = 00
   R = 8bac1ab6 6410435c b7181f95 b16ab97c 92b341c0
   S = 41e2345f 1f56df24 58f426d1 55b4ba2d b6dcd8c8
```

Based on this, the RDATA portion of an RRSIG with this hash is shown below assuming the following other parameters: the RRSIG signs "A" records; its validity time is from 00112233 seconds after the 1 January 1970 00:00:00 UTC through 00123456 seconds after that time; the signer name of "xx."; the original TTL was one hour or 0e10 seconds; and the number of labels in the original owner name was 05. "a" is the algorithm number for DSA and "l" is the "Labels" field.

```
0001 03 05 00000e10 00123456 00112233 19a3 02787800
```

```
      Type a> l> OrigTTL  expire   incept   ktag signer
      00 8bac1ab6 6410435c b7181f95 b16ab97c 92b341c0
      T> R>
         41e2345f 1f56df24 58f426d1 55b4ba2d b6dcd8c8
         S>
```

All numbers above in this Appendix are in hexadecimal.

Appendix B: Changes from RFC 2536

When [RFC2536] was published, keys and signatures in the DNS appeared only in KEY and SIG resource records. As described in [RFC3755], due to a revision in DNS data origin authentication security, the recommended RRs were changed to DNSKEY and RRSIG which are described in [RFC4034]; however, SIG continues to be used in transaction authentication, SIG(0) [RFC2931], and KEY continue to be used in connection with TKEY [RFC2930].

Thus the primary change from RFC 2536 in this document is to eliminate the tie to the KEY and SIG RRs. In addition, many references have been updated and example DNSKEY and RRSIG RRs using the DSA algorithm have been included.

Copyright, Disclaimer, and Additional IPR Provisions

found in BCP 78 and BCP 79.

Normative References

[FIPS186-2] - U.S. Federal Information Processing Standard: Digital Signature Standard, 27 January 2000.

[RFC4034] - Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

Informative References

[FIPS180-2] - U.S. Federal Information Processing Standard: Secure Hash Standard, 1 August 2002.

[RFC1034] - "Domain names - concepts and facilities", P. Mockapetris, 11/01/1987.

[RFC1035] - "Domain names - implementation and specification", P. Mockapetris, 11/01/1987.

[RFC2536] - "DSA KEYs and SIGs in the Domain Name System (DNS)", D. Eastlake, March 1999.

[RFC2671] - "Extension Mechanisms for DNS (EDNS0)", P. Vixie, August 1999.

[RFC2930] - Eastlake 3rd, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC2931] - Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3110] - "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", D. Eastlake 3rd. May 2001.

[RFC3174] - "US Secure Hash Algorithm 1 (SHA1)", D. Eastlake, P. Jones, September 2001.

[RFC3755] - Weiler, S., "Legacy Resolver Compatibility for Delegation Signer (DS)", May 2004.

[RFC4025] - "A Method for Storing IPsec Keying Material in DNS", M. Richardson, March 2005.

[RFC4033] - Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4035] - Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4086] - Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

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

Author's Address

Donald E. Eastlake 3rd
Motorola Labortories
155 Beaver Street
Milford, MA 01757 USA

Telephone: +1-508-786-7554(w)
EMail: Donald.Eastlake@motorola.com

Expiration and File Name

This draft expires in April 2007.

Its file name is draft-ietf-dnsext-rfc2536bis-dsa-08.txt.