Network Working Group
Request for Comments: 2536
Category: Standards Track

D. EastLake
IBM

March 1999

DSA 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

Abstract

A standard method for storing US Government Digital Signature Algorithm keys and 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 [RFC 2535]. Thus the DNS can now be secured and can be used for secure key distribution.

This document describes how to store US Government Digital Signature Algorithm (DSA) keys and signatures in the DNS. Familiarity with the US Digital Signature Algorithm is assumed [Schneier]. Implementation of DSA is mandatory for DNS security.

2. DSA KEY Resource Records

DSA public keys are stored in the DNS as KEY RRs using algorithm number 3 [RFC 2535]. The structure of the algorithm specific portion of the RDATA part of this RR is as shown below. These fields, from Q through Y are the "public key" part of the DSA KEY RR.

The period of key validity is not in the KEY RR but is indicated by the SIG RR(s) which signs and authenticates the KEY RR(s) at that domain name.

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 [FIPS 186] and [Schneier]: T is a key size parameter chosen such that 0 <= T <= 8. (The meaning for algorithm 3 if the T octet is greater than 8 is reserved and the remainder of the RDATA portion 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 so 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 FIPS 186 key generation algorithm [Schneier]. P is in the range 2**(511+64T) < P < 2**(512+64T) and so is 64 + 8*T octets long. G and Y are quantities modulus 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 SIG Resource Records

The signature portion of the SIG RR RDATA area, when using the US Digital Signature Algorithm, is shown below with fields in the order they occur. See [RFC 2535] for fields in the SIG RR RDATA which precede the signature itself.

Field	Size
T	1 octet
R	20 octets
S	20 octets

The data signed is determined as specified in [RFC 2535]. Then the following steps are taken, as specified in [FIPS 186], 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
```

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 the SIG 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 specified.

4. Performance Considerations

General signature generation speeds are roughly the same for RSA [RFC 2537] and DSA. 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 than RSA 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.

The key size limitation of a maximum of 1024 bits (T = 8) in the current DSA standard may limit the security of DSA. For particularly critical applications, implementors are encouraged to consider the range of available algorithms and key sizes.

DSA assumes the ability to frequently generate high quality random numbers. See [RFC 1750] for guidance. DSA is designed so that if manipulated rather than random numbers are used, very 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 requires an IETF standards actions. It is intended that values unallocated herein be used to cover future extensions of the DSS standard.

References

[FIPS 186] U.S. Federal Information Processing Standard: Digital Signature Standard.

[RFC 1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[RFC 1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[RFC 1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[RFC 2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC 2537] Eastlake, D., "RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)", RFC 2537, March 1999.

[Schneier] Schneier, B., "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", 1996.

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