Internet-Draft
Expires: May 1, 2016

D. Bider
Bitvise Limited
November 1, 2015

Use of RSA and DSA Keys with SHA-2 256 in Secure Shell (SSH)
draft-rsa-dsa-sha2-256-00.txt

Abstract

This memo defines algorithm names, public key formats, and signature formats for use of RSA and DSA keys with SHA-2 256 for server and client authentication in SSH connections.

Status

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright

1. Overview and Rationale

Secure Shell (SSH) is a common protocol for secure communication on the Internet. In [RFC4253], SSH originally defined the signature methods "ssh-rsa" for server and client authentication using RSA with SHA-1, and "ssh-dss" using DSA according to the then-available version of the Digital Signature Standard [FIPS-186-2]. At that time, DSS specified a modulus of up to 1024 bits, with a subgroup size of 160 bits, using SHA-1 hashing.

A decade later, these signature methods are considered deficient. For US government use, NIST has disallowed 1024-bit RSA and DSA, and use of SHA-1 for signing [800-131A].

This memo defines new algorithm names allowing for interoperable use of RSA and DSA keys with SHA-2 256, and use of 2048 and 3072-bit DSA.

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Public Key Algorithms

This memo adopts the style and conventions of [RFC4253] in specifying how the use of a signature algorithm is indicated in SSH.

The following new signature algorithms are defined:

rsa-sha2-256	RECOMMENDED	sign	Raw RSA key
dsa-sha2-256	OPTIONAL	sign	Raw 2048- or 3072-bit DSA Key

Both signature algorithms are suitable for use both in the SSH transport layer [RFC4253] for server authentication, and in the SSH authentication layer [RFC4252] for client authentication.

2.1 rsa-sha2-256

Since RSA keys are not dependent on the choice of hash function, the algorithm "rsa-sha2-256" reuses the public key format of the existing "ssh-rsa" algorithm as defined in [RFC4253]:

```
string    "ssh-rsa"
mpint     e
mpint     n
```

All aspects of the "ssh-rsa" format are kept, including the encoded string "ssh-rsa", in order to allow users' existing RSA keys to be

used with the new signature format, without requiring re-encoding, or affecting already trusted key fingerprints.

Signing and verifying using this algorithm is performed according to the RSASSA-PSS scheme in [RFC3447] using SHA-2 256 [FIPS-180-3] as hash; MGF1 as mask function; and salt length equal to hash size.

The resulting signature is encoded as follows:

```
string    "rsa-sha2-256"
string    rsa_signature_blob
```

The value for 'rsa_signature_blob' is encoded as a string containing S - an octet string which is the output of RSASSA-PSS, of length equal to the length in octets of the RSA modulus.

2.2 dsa-sha2-256

Keys used with this signature algorithm MUST use one of the following FIPS 186-4 options for modulus size (L) and subgroup size (N):

```
L = 2048, N = 256
L = 3072, N = 256
```

At least one major platform is currently known to support large DSA keys only with these parameters. To help interoperability, applications MUST NOT use options not listed.

Applications that wish to implement DSA key sizes or parameters other than those specified herein MUST use different algorithm names for such extensions. This is necessary to allow effective algorithm negotiation, and ensure interoperability between applications that may support varying sets of parameters and key sizes.

This key format has the following public key encoding:

```
string    "dsa-sha2-256"
mpint     p
mpint     q
mpint     g
mpint     y
```

Signing and verifying using this key format is done according to the Digital Signature Standard [FIPS-186-4] using a 256-bit SHA-2 hash [FIPS-180-3].

The resulting signature is encoded as follows:

```
string    "dsa-sha2-256"
string    dsa_signature_blob
```

The value for 'dsa_signature_blob' is encoded as a string containing

r, followed by s (which are 256-bit integers, without lengths or padding, unsigned, and in network byte order).

3. IANA Considerations

This document augments the Public Key Algorithm Names in [RFC4253] and [RFC4250].

IANA is requested to update the "Secure Shell (SSH) Protocol Parameters" registry with the following entries:

Public Key Algorithm Name	Reference	Note
rsa-sha2-256	[this document]	Section 2.1
dsa-sha2-256	[this document]	Section 2.2

4. Security Considerations

The security considerations of [RFC4253] apply to this document.

The National Institute of Standards and Technology (NIST) Special Publication 800-131A [800-131A] suggests that RSA keys shorter than 2048 bits; and DSA keys shorter than 2048 bits, and with subgroup sizes under 224 bits; have an encryption strength less than 112 bits. It disallows them for US government use after 2013. RSA key sizes of 2048 bits or more; and DSA key sizes of 2048 bits or more, and with subgroup sizes of 224 bits or more; are considered acceptable.

The same document disallows the SHA-1 hash function, as used in the "ssh-dss" algorithm, for digital signature generation after 2013. The SHA-2 family of hash functions, as used with the algorithm defined in this document, is considered acceptable.

4.1 Generation of "k" in DSA Signing

DSA private keys are vulnerable to biases in random generation of the "k" parameter during signing. A small bias permits discovery of the private key after observing a sufficient number of signatures. Reuse of the same "k" for only two different messages is sufficient to completely compromise the key. This can be induced, for example, by resuming saved virtual machine state. On the contrary, a DSA private key is immune to these attacks if "k" is generated deterministically, based only on the private key and message.

Applications that are able to do so SHOULD use a deterministic "k" as specified in [RFC6979]. Applications that cannot do this SHOULD feed the entropy of the message being signed into the PRNG mechanism used to generate "k" immediately before signing.

5. References

5.1. Normative References

[FIPS-180-3]
National Institute of Standards and Technology (NIST), United States of America, "Secure Hash Standard (SHS)", FIPS PUB 180-3, October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

[FIPS-186-4]
National Institute of Standards and Technology (NIST), United States of America, "Digital Signature Standard (DSS)", FIPS Publication 186-4, July 2013, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[RFC6979] Pornin, T., "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 6979, August 2013.

5.2. Informative References

[800-131A] National Institute of Standards and Technology (NIST), "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A, January 2011, <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>.

[FIPS-186-2]
National Institute of Standards and Technology (NIST), United States of America, "Digital Signature Standard (DSS)", FIPS Publication 186-2 (with Change Notice 1), October 2001, <http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2-change1.pdf>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH)

Authentication Protocol", RFC 4252, January 2006.

Author's Address

Denis Bider
Bitvise Limited
Suites 41/42, Victoria House
26 Main Street
GI

Phone: +506 8315 6519
EMail: ietf-ssh3@denisbider.com
URI: https://www.bitvise.com/

Acknowledgments

Thanks to Jeffrey Hutzelman for comments and suggestions to initial drafts.

Thanks to participants on the SSH and CFRG mailing lists for additional comments and suggestions.