Use of the SHA-256 Algorithm with RSA,
Digital Signature Algorithm (DSA),
and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records

Abstract

This document updates the IANA registries in RFC 4255, which defines
SSHFP, a DNS Resource Record (RR) that contains a standard Secure
Shell (SSH) key fingerprint used to verify SSH host keys using DNS
Security Extensions (DNSSEC). This document defines additional
options supporting SSH public keys applying the Elliptic Curve
Digital Signature Algorithm (ECDSA) and the implementation of
fingerprints computed using the SHA-256 message digest algorithm in
SSHFP Resource Records.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force
(IETF). It represents the consensus of the IETF community. It has
received public review and has been approved for publication by the
Internet Engineering Steering Group (IESG). Further information on
Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata,
and how to provide feedback on it may be obtained at

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ..........................................................3
2. Requirements Language ................................................4
3. SSHFP Resource Records ..............................................4
   3.1. SSHFP Fingerprint Type Specification .......................4
      3.1.1. SHA-256 SSHFP Fingerprint Type Specification .......4
   3.2. SSHFP Algorithm Number Specification ......................4
      3.2.1. ECDSA SSHFP Algorithm Number Specification .......4
4. Implementation Considerations .......................................4
   4.1. Support for SHA-256 Fingerprints ............................4
   4.2. Support for ECDSA ............................................4
5. Examples ......................................................................5
   5.1. RSA Public Key ................................................5
      5.1.1. RSA Public Key with SHA1 Fingerprint .................5
      5.1.2. RSA Public Key with SHA-256 Fingerprint ............5
   5.2. DSA Public Key ................................................6
      5.2.1. DSA Public Key with SHA1 Fingerprint .................6
      5.2.2. DSA Public Key with SHA-256 Fingerprint ............6
   5.3. ECDSA Public Key .............................................6
      5.3.1. ECDSA Public Key with SHA1 Fingerprint ..............7
      5.3.2. ECDSA Public Key with SHA-256 Fingerprint .........7
6. IANA Considerations ..................................................7
   6.1. SSHFP RR Types for Public Key Algorithms .................7
   6.2. SSHFP RR Types for Fingerprint Types ......................7
7. Security Considerations ...............................................8
8. References ....................................................................8
   8.1. Normative References ........................................8
   8.2. Informative References .......................................9
1. Introduction

The Domain Name System (DNS) is the global, hierarchical distributed database for Internet naming. The Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. RFC 4253 [RFC4253] defines Public Key Algorithms for the Secure Shell server public keys.

The DNS has been extended to store fingerprints in a DNS Resource Record named SSHFP [RFC4255], which provides out-of-band verification by looking up a fingerprint of the server public key in the DNS [RFC1034][RFC1035] and using Domain Name System Security Extensions (DNSSEC) [RFC4033][RFC4034][RFC4035] to verify the lookup.

RFC 4255 [RFC4255] describes how to store the cryptographic fingerprint of SSH public keys in SSHFP Resource Records. SSHFP Resource Records contain the fingerprint and two index numbers identifying the cryptographic algorithms used:

1. to link the fingerprinted public key with the corresponding private key, and
2. to derive the message digest stored as the fingerprint in the record.

RFC 4255 [RFC4255] then specifies lists of cryptographic algorithms and the corresponding index numbers used to identify them in SSHFP Resource Records.

This document updates the IANA registry "SSHFP RR Types for public key algorithms" and "SSHFP RR types for fingerprint types" [SSHFPVALS] by adding a new option in each list:

- the Elliptic Curve Digital Signature Algorithm (ECDSA) [RFC6090], which has been added to the Secure Shell Public Key list by RFC 5656 [RFC5656] in the public key algorithms list, and
- the SHA-256 algorithm [FIPS.180-3.2008] in the SSHFP fingerprint type list.

Familiarity with DNSSEC, SSH Protocol [RFC4251][RFC4253][RFC4250], SSHFP [RFC4255], and the SHA-2 [FIPS.180-3.2008] family of algorithms is assumed in this document.
2. Requirements Language

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 RFC 2119 [RFC2119].

3. SSHFP Resource Records

The format of the SSHFP RR can be found in RFC 4255 [RFC4255].

3.1. SSHFP Fingerprint Type Specification

The fingerprint type octet identifies the message digest algorithm used to calculate the fingerprint of the public key.

3.1.1. SHA-256 SSHFP Fingerprint Type Specification

SHA-256 fingerprints of the public keys are stored in SSHFP Resource Records with the fingerprint type 2.

3.2. SSHFP Algorithm Number Specification

The SSHFP Resource Record algorithm number octet describes the algorithm of the public key.

3.2.1. ECDSA SSHFP Algorithm Number Specification

ECDSA public keys are stored in SSHFP Resource Records with the algorithm number 3.

4. Implementation Considerations

4.1. Support for SHA-256 Fingerprints

SSHFP-aware Secure Shell implementations SHOULD support the SHA-256 fingerprints for verification of the public key. Secure Shell implementations that support SHA-256 fingerprints MUST prefer a SHA-256 fingerprint over SHA-1 if both are available for a server. If the SHA-256 fingerprint is tested and does not match the SSH public key received from the SSH server, then the key MUST be rejected rather than testing the alternative SHA-1 fingerprint.

4.2. Support for ECDSA

SSHFP-aware Secure Shell implementations that also implement the ECDSA for the public key SHOULD support SSHFP fingerprints for ECDSA public keys.
5. Examples

The following examples provide reference for both the newly defined value for ECDSA and the use of the SHA-256 fingerprint combined with both the new and the existing algorithm numbers.

5.1. RSA Public Key

A public key with the following value in OpenSSH format [RFC4716] would appear as follows:

```
----- BEGIN SSH2 PUBLIC KEY -----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDCUR4JOhxTinzq7Q03bQXW4jmPCCu1Fsnh8Yi7MKwpMnd96+T7uV7nEwy+6+GWYu98lxJByIjFXX/a6BXDp3878wezH1DZ2tND/tu/eudz6ErpTFYmnVLyEDARYSzVBNqsIK1U5qVVtBBkffJcny78FpWk27uGkqEkam7GaurPRAgwXehDB/gMwRtXVR2+13zYwkAmAY+5OAWmdXuQVm5kJlvCNzto2H3m3nqJtD4J9L1lKpuSVVqW4jr4/6hibXjKqEVeVnPvUvdOAUw3rKrPwNaN932fXk3ke4rsDjQ/W8GyleMtK3TxBtE4z1uwovXtYe6Ba8q3LAPs/m2S4pUscx
----- END SSH2 PUBLIC KEY -----
```

5.1.1. RSA Public Key with SHA1 Fingerprint

The SSHFP Resource Record for this key would be:

```
server.example.net IN SSHFP 1 1 ( dd465c09cfa51fb45020cc83316fff21b9ec7ac )
```

5.1.2. RSA Public Key with SHA-256 Fingerprint

The SSHFP Resource Record for this key would be:

```
server.example.net IN SSHFP 1 2 ( b049f950d1397b8fee6a61e4d14a9acdc4721e084eff5460bbed80cfaa2ce2cb )
```
5.2. DSA Public Key

A public key with the following value in OpenSSH format would appear as follows:

```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBAPVFrcc0U36gWaywbfJzjc8ef13rAX4EJ18Na6xqvXh1
t+aCJEdS7soRjtvyK4KsNhhk78DjtdnfhEhyFKHHNz3i6/c/s91P0UjV7mRAo6nA7A
3Gs6iQE1b609Fqm6iVSC6bYW11TS0tYencEEJUaUua8YQF/uxRzPrReXxGqHnj
AAAAAQDC9M/pUi8VIVmEGO00wc1TeUTN4wAAAAEAgA2Fkbkbe0o/u/qw8mQFOFWZ
pTaqNo7d7joy3majbh5LqEVD7yT3MS1GSGhjgvyhhus/eHTqzYbJcOszUM9JnwT
7xq15P2ZDK8IIVxr31jMtsUUEmBqB4DUIjTurtaWmJ9LNaP1/k4bMoO/hotnOc
OVnIPsTLBFVvdNRRxUAAAACA02dcK0/NTMlqIYzBqCfwrwQ+9pmsuSI6nUzf
S4NysXkdbW5u5VxeLcwWjP5GbRfoS2P3vwYamakqgq502wigam18u9nAczUY1+
2kOeoiIItRrtSmlfP7tLQAo8k1E5jIlkn35jKmTC0mFRXbFmkKRTK80EnWQ8AVg
6w8=
---- END SSH2 PUBLIC KEY ----
```

5.2.1. DSA Public Key with SHA1 Fingerprint

The SSHFP Resource Record for this key would be:

```
server.example.net IN SSHFP 2 1 (3b6ba6110f5ffcd29469fc1ec2ee25
d61718badd)
```

5.2.2. DSA Public Key with SHA-256 Fingerprint

The SSHFP Resource Record for this key would be:

```
server.example.net IN SSHFP 2 2 (f9b8a6a460639306f1b38910456a6a
e1018a253c47ecec12db77d7a0878b
4d83)
```

5.3. ECDSA Public Key

A public key with the following value in OpenSSH format would appear as follows:

```
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAACBAPVFrcc0U36gWaywbfJzjc8ef13rAX4EJ18Na6xqvXh1
t+aCJEdS7soRjtvyK4KsNhhk78DjtdnfhEhyFKHHNz3i6/c/s91P0UjV7mRAo6nA7A
3Gs6iQE1b609Fqm6iVSC6bYW11TS0tYencEEJUaUua8YQF/uxRzPrReXxGqHnj
AAAAAQDC9M/pUi8VIVmEGO00wc1TeUTN4wAAAAEAgA2Fkbkbe0o/u/qw8mQFOFWZ
pTaqNo7d7joy3majbh5LqEVD7yT3MS1GSGhjgvyhhus/eHTqzYbJcOszUM9JnwT
7xq15P2ZDK8IIVxr31jMtsUUEmBqB4DUIjTurtaWmJ9LNaP1/k4bMoO/hotnOc
OVnIPsTLBFVvdNRRxUAAAACA02dcK0/NTMlqIYzBqCfwrwQ+9pmsuSI6nUzf
S4NysXkdbW5u5VxeLcwWjP5GbRfoS2P3vwYamakqgq502wigam18u9nAczUY1+
2kOeoiIItRrtSmlfP7tLQAo8k1E5jIlkn35jKmTC0mFRXbFmkKRTK80EnWQ8AVg
6w8=
---- END SSH2 PUBLIC KEY ----
```
5.3.1. ECDSA Public Key with SHA1 Fingerprint

The SSHFP Resource Record for this key would be:

server.example.net IN SSHFP 3 1 (c64607a28c5300fec1180b6e417b92 2943cfffcd)

5.3.2. ECDSA Public Key with SHA-256 Fingerprint

The SSHFP Resource Record for this key would be:

server.example.net IN SSHFP 3 2 (821eb6c1c98d9cc827ab7f456304c0 f14785b7008d9846a8519de80849 afc7)

6. IANA Considerations

This document updates the IANA registry "SSHFP RR Types for public key algorithms" and "SSHFP RR types for fingerprint types" [SSHFPVALS].

6.1. SSHFP RR Types for Public Key Algorithms

The following entries have been added to the "SSHFP RR Types for public key algorithms" registry:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>ECDSA</td>
<td>[This doc]</td>
</tr>
</tbody>
</table>

6.2. SSHFP RR Types for Fingerprint Types

The following entries have been added to the "SSHFP RR types for fingerprint types" registry:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>SHA-256</td>
<td>[This doc]</td>
</tr>
</tbody>
</table>

[This doc]
7. Security Considerations

Please see the security considerations in [RFC4255] for SSHFP Resource Records and [RFC5656] for the ECDSA.

Users of SSHFP are encouraged to deploy SHA-256 as soon as implementations allow for it. The SHA-2 family of algorithms is widely believed to be more resilient to attack than SHA-1, and confidence in SHA-1’s strength is being eroded by recently announced attacks [IACR2007/474]. Regardless of whether or not the attacks on SHA-1 will affect SSHFP, it is believed (at the time of this writing) that SHA-256 is the better choice for use in SSHFP records.

SHA-256 is considered sufficiently strong for the immediate future, but predictions about future development in cryptography and cryptanalysis are beyond the scope of this document.

8. References

8.1. Normative References


8.2. Informative References


Author’s Address

Ondrej Sury
CZ.NIC
Americka 23
120 00 Praha 2
Czech Republic

Phone: +420 222 745 110
EMail: ondrej.sury@nic.cz