Network Working Group	J. Salowey	
Internet-Draft	Cisco Systems	
Intended status: Standards Track	S. Suehring	
Expires: May 14, 2011	November 10, 2010	

TOC

Uniform Resource Identifier (URI) Scheme for Secure Shell (SSH)
draft-salowey-secsh-uri-00.txt

Abstract

This document describes the Uniform Resource Identifiers used to locate resources for the Secure Shell (SSH) protocol. The document describes the generic syntax involved in URI definitions as well as specific definitions for the protocol. These specific definitions include user credentials such as username and other parameters such as host key fingerprint.

Status of this Memo

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on May 14, 2011.

Table of Contents

1. Introduction

TOC

This document describes the Uniform Resource Identifiers (URIs) to be used with the Secure Shell (SSH) [RFC4251] (Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Protocol Architecture,” January 2006.) protocos.
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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

2. General Syntax

TOC

A hierarchical URI shall consist of the scheme and the scheme specific portion separated by a colon ":" followed by the hierarchical part, as discussed in [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.).

This specification uses the definitions "port", "host", "scheme", "userinfo", "path-empty", "path-abempty" and "authority" from [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.). This document follows the ABNF notation defined in [RFC5234] (Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.).

---

3. Secure Shell (SSH) URI

TOC

This section describes the SSH URI and contains the information necessary to register the URI according to the template in [RFC4395] (Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes," February 2006.).

3.1. Scheme Name

TOC

The Secure Shell scheme name is "ssh".

3.2. Status

TOC

The requested status of the SSH URI is "permanent".

3.3. URI Scheme Syntax

TOC

The Secure Shell (SSH) scheme shall consist of the scheme name "ssh" followed by a colon ":" followed by hier-part defined in [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," January 2005.). The SSH URI ABNF definition follows.

```
sshURI        =  "ssh:" hier-part
hier-part     =  "//" authority path-abempty
authority     =  [ [ ssh-info ] "@" ] host [ ":" port ]
host          =  <as specified in [RFC3986]>
port          =  <as specified in [RFC3986]>
path-abempty  =  <as specified in [RFC3986]>
ssh-info      =  [ userinfo ] [";" c-param *("," c-param)]
userinfo      =  <as specified in [RFC3986]>
c-param       =  paramname "=" paramvalue
paramname     =  *( ALPHA / DIGIT / "-" )
paramvalue    =  *( ALPHA / DIGIT / "-" )
```

The following reserved characters from [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.) are used as delimiters within the SSH URI: ";", ",", ":", and "=" . They must not be escaped when used as delimiters and must be escaped when the appear in other uses.

3.4. URI Semantics

TOC

The intended usage of the SSH URI is to establish an interactive SSH terminal session with the host defined in the authority portion of the URI. The only operation defined for the URI is to establish an SSH terminal session with a remote host.

If the userinfo or connection parameters are present the at-sign "@" shall precede the authority section of the URI. Optionally, the authority section MAY also include the port preceded by a colon ":". The host SHOULD be a non-empty string. If the port is not included, the default port is assumed.

The ssh-info portion of the URI MAY include credentials consisting of a username followed by optional parameters. The convention of including the password separated from the username by a ":" in the URI is NOT RECOMMENDED and is deprecated in accordance with [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.).

One or more optional connection parameters (c-param) may be specified within the userinfo section of the URI. These conn-parameters are separated from the userinfo by a semi-colon ";". The only connection parameter defined in this document is for the host-key fingerprint described in Section 4.1 (SSH connection parameters). It is possible that additional parameters be defined in the future. If a connection parameter is not understood it SHOULD be ignored.

The SSH URI does not define a usage for a non-empty path element. If a non-empty path element is included in an SSH URI then it SHOULD be ignored.

3.5. Encoding Considerations

TOC

The encoding of the "host" portion of the URI is as defined in [RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.). The encoding of the connection parameters is described in Section 4.1 (SSH connection parameters)

3.6. Protocols using this URI scheme

TOC

This URI scheme is used by the SSH protocol version 2 defined in [RFC4251] (Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Protocol Architecture,” January 2006.).

3.7. Security Considerations

TOC

See Section 7 (Security Considerations).

3.8. Contact

TOC

This document is discussed on the IETF SSH list: ietf-ssh@netbsd.org

4. Parameters

TOC

4.1. SSH connection parameters

TOC

The following parameters are associated with an SSH connection and are applicable to SSH and SFTP. All parameters are optional and MUST NOT overwrite configured defaults. Individual parameters are separated by a comma (",").

fingerprint
: The fingerprint parameter contains the fingerprint of the host key for the host specified in the URL. The fingerprint

> is encoded as host-key-alg-fingerprint. Host-key-alg is host public key algorithm defined in [RFC4253] (Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," January 2006.) and the fingerprint format is [RFC4716] (Galbraith, J. and R. Thayer, "The Secure Shell (SSH) Public Key File Format," November 2006.). For use in a URI, the fingerprint shall use a single dash "-" as a separator instead of the colon ":" as described in [RFC4716] (Galbraith, J. and R. Thayer, "The Secure Shell (SSH) Public Key File Format," November 2006.). This parameter MUST NOT overwrite a key that is already configured for the host. The fingerprint MAY be used to validate the authenticity of the host key if the URL was obtained from an authenticated source with its integrity protected. If this parameter is not included then the host key is validated using another method. See Security Considerations section for additional considerations. There MUST be only one fingerprint parameter present in a given URL.

---

5. Examples

TOC

The following section shows basic examples of URLs for each protocol. This section should not be considered to include all possible combinations of URLs for each protocol.
An SSH connection to the host host.example.com on the standard port using username user.

```
ssh://user@host.example.com
```

An SSH connection to the host host.example.com on port 2222 using username user.

```
ssh://user@host.example.com:2222
```

An SSH connection to the host having the specified host-key fingerprint at host.example.com on the standard port using username user.

```
ssh://user;fingerprint=ssh-dss-c1-b1-30-29-d7-b8-de-6c-97-
     77-10-d7-46-41-63-87@host.example.com
```

TOC

6. IANA Considerations

Section 3 (Secure Shell (SSH) URI) provides the information required in the URL registration template in accordance with [RFC4395] (Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes," February 2006.).

---

7. Security Considerations

TOC

Passwords SHOULD NOT be included within the URI as doing so poses a security risk. URIs are usually sent in the clear with no encryption or other security, any password or other credentials included in the userinfo could be seen by a potential attacker.
Although the host-key fingerprint is not confidential information, care must be taken in handling fingerprints associated with URIs because URIs transmitted or stored without protection may be modified by an attacker. In general an implementation cannot determine the source of a URI so a fingerprint received in a URI should have no more trust associated with it than a raw public key received in the SSH protocol itself. If a locally configured key exists for the server already it MUST NOT be automatically overwritten with information from the URI. If the host is unknown then the implementation should treat the fingerprint received with the same caution that it does with any unknown public key. The client MAY offer the fingerprint and URI for external validation before allowing a connection based on this information. If the client chooses to make a connection based on the URI information and it finds that the fingerprint in the URI and the public key offered by the server do not match then it SHOULD provide a warning and provide a means to abort the connection. Sections 4.1 and 9.2.4 of [RFC4251] (Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," January 2006.) provide a good discussion of handling public keys received in the SSH protocol.

---

8. Acknowledgements

TOC

Ben Harris, Tom Petch and the members of the SSH working group have provided much useful feedback in the preparation of this document.

---

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4251]	Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," RFC 4251, January 2006 (TXT).
[RFC4253]	Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," RFC 4253, January 2006 (TXT).
[RFC4716]	Galbraith, J. and R. Thayer, "The Secure Shell (SSH) Public Key File Format," RFC 4716, November 2006 (TXT).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).

9.2. Informative References

TOC

[RFC4395]	Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes," BCP 35, RFC 4395, February 2006 (TXT).

Authors' Addresses

TOC

	Joseph Salowey
	Cisco Systems
	2901 3rd Ave
	Seattle, WA 98121
	US
Email:	jsalowey@cisco.com
	Steve Suehring
	PO BOX 1033
	Stevens Point, WI 54481
	US
Email:	suehring@braingia.com