NETWORK WORKING GROUP
Internet-Draft
Expires: May 11, 2008

N. Williams
Sun

November 8, 2007

Channel Binding Identifiers for Secure Shell Channel
draft-williams-sshv2-channel-bindings-00.txt

Status of this Memo

Copyright Notice

Abstract

This document defines the channel bindings for SSHv2 connections.

Table of Contents

1. Conventions used in this document

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. Bindings to SSHv2 channels

SSHv2 [RFC4251] provides both, a secure channel and material (the SSHv2 "session ID") that is suitable for use as channel binding identifiers [I-D.williams-on-channel-bindings].

Thus it is RECOMMENDED that the SSHv2 "session ID" be used as the channel bindings for SSHv2.

3. IANA Considerations

There are no IANA considerations in this document.

4. Security Considerations

See [I-D.williams-on-channel-bindings].

5. Normative References

[I-D.williams-on-channel-bindings]
Williams, N., "On Channel Binding", draft-williams-on-channel-bindings-00 (work in progress), July 2006.

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

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

Author's Address

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US

Email: Nicolas.Williams@sun.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).