

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

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/ietf/1id-abstracts.txt>.

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

This Internet-Draft will expire on May 11, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document defines the channel bindings for SSHv2 connections.

Table of Contents

- [1. Conventions used in this document . . . . .](#) [3](#)
- [2. Bindings to SSHv2 channels . . . . .](#) [4](#)
- [3. IANA Considerations . . . . .](#) [5](#)
- [4. Security Considerations . . . . .](#) [6](#)
- [5. Normative References . . . . .](#) [7](#)
- [Author's Address . . . . .](#) [8](#)
- [Intellectual Property and Copyright Statements . . . . .](#) [9](#)



## **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](mailto:Nicolas.Williams@sun.com)

## Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

## Acknowledgment

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

