

**A PRF for the Kerberos V GSS-API Mechanism
draft-ietf-kitten-krb5-gssapi-prf-00.txt**

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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 December 30, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document defines the Pseudo-Random Function (PRF) for the Kerberos V GSS-API mechanism, based on the PRF defined for the Kerberos V cryptographic framework, for keying application protocols given an established Kerberos V GSS-API security context.

Table of Contents

1.	Conventions used in this document	3
2.	Introduction	4
3.	Security Considerations	5
4.	Normative	5
	Author's Address	5
	Intellectual Property and Copyright Statements	6

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. Introduction

The GSS-API PRF [[GSS-PRF](#)] function for the Kerberos V mechanism shall be the output of a PRF+ function based on the enctype's PRF function keyed with the negotiated session key of the security context (e.g., the acceptor's subkey) and key usage X (TBD).

The PRF+ function is a simple counter-based extension of the enctype's prf using an 16-bit network byte order unsigned binary counter: $\text{PRF+}(k, \text{input}) = \text{random-to-key}(\text{k-truncate}(\text{prf}(k, 0 \parallel \text{input}) \parallel \text{prf}(k, 1 \parallel \text{input}), \dots, \text{prf}(k, n \parallel \text{input})))$. The maximum output length for this PRF+ then is 65536 times the output length of the Kerberos V cryptographic framework PRF for the enctype of the input key.

If the `desired_output_len` input parameter exceeds the maximum output of this function then the maximum will be output instead.

Williams

Expires December 30, 2004

[Page 4]

3. Security Considerations

Kerberos V enctypees' PRF functions use a key derived from contexts' session keys and should preserve the forward security properties of the mechanisms' key exchanges.

See also [[GSS-PRF](#)] for generic security considerations of GSS_Pseudo_random().

4 Normative

[GSS-PRF] Williams, N., "A PRF API extension for the GSS-API".

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

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", [RFC 2743](#), January 2000.

[RFC2744] Wray, J., "Generic Security Service API Version 2 : C-bindings", [RFC 2744](#), January 2000.

Author's Address

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

EMail: Nicolas.Williams@sun.com

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2004). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Williams

Expires December 30, 2004

[Page 6]