

NETWORK WORKING GROUP  
Internet-Draft  
Expires: December 30, 2004

N. Williams  
Sun  
July 2004

**A PRF API extension for the GSS-API  
draft-ietf-kitten-gssapi-prf-01.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 a Pseudo-Random Function (PRF) extension to the Generic Security Service Application Programming Interface (GSS-API) for keying application protocols given an established GSS-API security context. The primary intended use of this function is to key secure session layers that don't or cannot use GSS-API per-message MIC (message integrity check) and wrap tokens for session protection.

Williams

Expires December 30, 2004

[Page 1]

## Table of Contents

<a href="#">1.</a>	Conventions used in this document . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">4</a>
<a href="#">3.</a>	GSS_Pseudo_random() . . . . .	<a href="#">5</a>
<a href="#">3.1</a>	C-Bindings . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">5.</a>	References . . . . .	<a href="#">8</a>
<a href="#">5.1</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">5.2</a>	Informative References . . . . .	<a href="#">8</a>
	Author's Address . . . . .	<a href="#">8</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">9</a>



## **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**

A need has arisen for users of the GSS-API to key applications' cryptographic protocols using established GSS-API security contexts. Such applications can use the GSS-API for authentication, but not for transport security (for whatever reasons), and since the GSS-API does not provide a method for obtaining keying material from established security contexts such applications cannot make effective use of the GSS-API.

To address this need we define a pseudo-random function (PRF) extension to the GSS-API.



### **3. GSS\_Pseudo\_random()**

Inputs:

- o context CONTEXT handle,
- o prf\_in OCTET STRING,
- o desired\_output\_len INTEGER

Outputs:

- o major\_status INTEGER,
- o minor\_status INTEGER,
- o prf\_out OCTET STRING

Return major\_status codes:

- o GSS\_S\_COMPLETE indicates no error.
- o GSS\_S\_NO\_CONTEXT indicates that a null context has been provided as input.
- o GSS\_S\_CONTEXT\_EXPIRED indicates that an expired context has been provided as input.
- o GSS\_S\_UNAVAILABLE indicates that the mechanism lacks support for this function.
- o GSS\_S\_FAILURE indicates failure or lack of support; the minor status code may provide additional information.

This function applies the established context's mechanism's keyed PRF function to the input data (prf\_in), keyed with key material associated with the given security context and outputs the resulting octet string (prf\_out) of desired\_output\_len length.

The output string of this function MUST be a pseudo-random function [GGM1][GGM2] of the input keyed with key material from the established security context -- the chances of getting the same output given different input parameters should be exponentially small.

This function, applied to the same inputs by an initiator and acceptor using the same established context, MUST produce the \*same results\* for both, the initiator and acceptor, even if called multiple times for the same context.

Mechanisms MAY limit the output of the PRF according, possibly in ways related to the types of cryptographic keys available for the PRF function, thus the prf\_out output of GSS\_Pseudo\_random() MAY be smaller than requested.

#### **3.1 C-Bindings**



Williams

Expires December 30, 2004

[Page 5]

```
OM_uint32 gss_pseudo_random(  
    OM_uint32          *minor_status,  
    gss_ctx_id_t       context,  
    const gss_buffer_t  prf_in,  
    ssize_t            desired_output_len,  
    gss_buffer_t        prf_out  
);
```

#### **4. Security Considerations**

Care should be taken in properly designing a mechanism's PRF function.

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

## **5. References**

### **5.1 Normative References**

- [GGM1] Goldreich, O., Goldwasser, S. and S. Micali, "How to Construct Random Functions", October 1986.
- [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.

### **5.2 Informative References**

- [GGM2] Goldreich, O., Goldwasser, S. and S. Micali, "On the Cryptographic Applications of Random Functions", 1985.
- [RFC1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", [RFC 1750](#), December 1994.

#### 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)



## 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](mailto: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 9]