

GSS-APIv2 Extension for Storing Delegated Credentials
<[draft-williams-gssapi-cred-store-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [[RFC2026](#)].

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>.

Copyright Notice

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

Abstract

The details of Generic Security Service (GSS) credential store management vary by platform and even by GSS mechanism. Credential store management is an interesting concept that requires exploration.

This document defines a small extension to the GSS-API for GSS-API credential store management. While exploration of the credential store management problem is the goal of this document, implementation of these interfaces is not discounted nor discouraged.

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](#)].

Table of Contents

1.	Introduction	pg. 3
2.	GSS_Make_cred_store()	pg. 3
3.	GSS_Get_current_cred_store()	pg. 3
4.	GSS_Set_current_cred_store()	pg. 4
5.	GSS_Inquire_cred_store()	pg. 5
6.	GSS_Display_cred_store()	pg. 5
7.	C-Bindings	pg. 5
8.	Examples	pg. 5
9.	Security Considerations	pg. 5
10.	Acknowledgements	pg. 5
11.	References	pg. 5
11.1.	Informative References	pg. 5
11.2.	Normative References	pg. 5
12.	Author's Address	pg. 6

1. Introduction

[Text needed on what is a "credential store" and what is a "current credential store,:" and their relation to the callers' current execution context.]

[Also add text about how this stuff imports concepts such as "process," which does not augur well for interface genericity.]

[See [[gss_store_cred](#)].]

2. GSS_Make_cred_store()

Inputs:

```
o inheritance SET OF ENUMERATED, -- Specifies the desired
-- inheritance rule for this store. Possible values include:
--
-- o none (this process only)
-- o default
-- o spawn
-- o fork
-- o exec

o sharing ENUMERATED, -- Specifies the desired degree of sharing
-- of this store with other processes or threads. Possible values
-- include:
--
-- o none
-- o default
-- o allThreadsInSameProcess
-- o allProcessesInSameSession
-- o allProcessesForSameUser
-- o allProcesses
```

Outputs:

```
o major_status INTEGER,

o minor_status INTEGER,

o cred_store_handle CREDENTIAL STORE HANDLE
```

Return status codes:

...

3. GSS_Get_current_cred_store()

Inputs:

N. Williams

[Page 3]

o <none>

Outputs:

o major_status INTEGER,

o minor_status INTEGER,

o cred_store_handle CREDENTIAL STORE HANDLE

Return status codes:

o GSS_S_COMPLETE indicates that there is a credential store or that one can be created, when GSS_Store_cred() is called, for the current execution context of the caller.

o GSS_S_UNAVAILABLE indicates that no credential store exists for the current execution context of the caller.

o GSS_S_FAILURE indicates that an unspecified failure has occurred.

This function returns a credential store handle that refers to the credential store from which credentials would be acquired given the current execution context of the caller.

Credential store handles may not remain accessible when the caller switches the user of the execution context.

4. GSS_Set_current_cred_store()

Inputs:

o cred_store_handle CREDENTIAL STORE HANDLE,

Outputs:

o major_status INTEGER,

o minor_status INTEGER

Return status codes:

o GSS_S_COMPLETE indicates that the given credential store will be used by subsequent GSS-API credential acquisition or storage made in the same execution context as that of the caller to GSS_Set_current_cred_store(). If the given store handle is GSS_C_NO_STORE then either a default or new (which is a platform-specific matter) credential store will be created and set as the current credential store.

o GSS_S_BAD_STORE indicates that the given credential store handle is not recognized or refers to a credential store that no longer exists or is otherwise corrupt.

o GSS_S_UNAVAILABLE indicates that the current credential store for the current execution context could not be set, possibly due to lack of resources.

o GSS_S_FAILURE indicates that a generic failure has occurred.

This function changes the credential store for the current execution context.

Calls to this function MAY have platform-specific side effects (e.g., setting environment variables, setting a process' "pag," etc...), but an implementation of it MUST NOT change the user context of the application, a restriction applicable only on multi-user platforms.

The current credential store may change or become unavailable when the caller switches the user of the execution context.

5. GSS_Inquire_cred_store()

[Inquire a cred store for inheritance and sharing levels, supported mechanisms.]

6. GSS_Display_cred_store()

[Display a credential store. A generic equivalent of MIT's klist(1).]

7. C-Bindings

[...]

8. Examples

[...]

9. Security Considerations

10. Acknowledgements

[...]

11. References

11.1. Informative References

[gss_store_cred]

N. Williams, [draft-williams-gssapi-store-deleg-creds-00](#):
"GSS-APIv2 Extension for Storing Delegated Credentials," September 2003, Status: Internet-Draft.

11.2. Normative References

N. Williams

[Page 5]

[RFC2026]

S. Bradner, [RFC2026](#): "The Internet Standard Process - Revision 3," October 1996, Obsoletes - [RFC 1602](#), Status: Best Current Practice.

[RFC2119]

S. Bradner, [RFC2119](#) ([BCP14](#)): "Key words for use in RFCs to Indicate Requirement Levels," March 1997, Status: Best Current Practice.

[RFC2743]

J. Linn, [RFC2743](#): "Generic Security Service Application Program Interface Version 2, Update 1," January 2000, Status: Proposed Standard.

[RFC2744]

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

[12.](#) Author's Address

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
Email: Nicolas.Williams@sun.com

Full Copyright Statement

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

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING

TASK FORCE DISCLAIMS 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

DRAFT

GSS Credential Store API

Expires November 2004

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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

