NAME

gss_wrap, gss_seal - Attach a cryptographic MIC and optionally encrypt a message

SYNOPSIS

#include <gssapi/gssapi.h>

OM_uint32
gss_wrap(*OM_uint32 *minor_status*, *const gss_ctx_id_t context_handle*, *int conf_req_flag*,
   gss_qop_t qop_req, *const gss_buffer_t input_message_buffer*, *int *conf_state*,
   gss_buffer_t output_message_buffer);

OM_uint32
gss_seal(*OM_uint32 *minor_status*, *gss_ctx_id_t context_handle*, *int conf_req_flag*, *gss_qop_t qop_req*,
   gss_buffer_t input_message_buffer, *int *conf_state*, *gss_buffer_t output_message_buffer*);

DESCRIPTION

Attaches a cryptographic MIC and optionally encrypts the specified input_message. The
output_message contains both the MIC and the message. The qop_req parameter allows a choice
between several cryptographic algorithms, if supported by the chosen mechanism.

Since some application-level protocols may wish to use tokens emitted by **gss_wrap**() to provide "secure
framing", implementations must support the wrapping of zero-length messages.

The **gss_seal**() routine is an obsolete variant of **gss_wrap**(). It is provided for backwards compatibility
with applications using the GSS-API V1 interface. A distinct entrypoint (as opposed to #define) is
provided, both to allow GSS-API V1 applications to link and to retain the slight parameter type
differences between the obsolete versions of this routine and its current form.

PARAMETERS

minor_status   Mechanism specific status code.

context_handle   Identifies the context on which the message will be sent.

conf_req_flag

                    Non-zero Both confidentiality and integrity services are requested.
                    Zero   Only integrity service is requested.

qop_req   Specifies required quality of protection. A mechanism-specific default may be
                    requested by setting qop_req to GSS_C_QOP_DEFAULT. If an unsupported
                    protection strength is requested, **gss_wrap**() will return a major_status of

GSS_S_BAD_QOP.

input_message_buffer   Message to be protected.

conf_state

        Non-zero   Confidentiality, data origin authentication and integrity services have
                     been applied.
        Zero   Integrity and data origin services only has been applied.

output_message_buffer   Buffer to receive protected message. Storage associated with this buffer must
                     be freed by the application after use with a call to gss_release_buffer(3).

RETURN VALUES

GSS_S_COMPLETE   Successful completion.

GSS_S_CONTEXT_EXPIRED The context has already expired

GSS_S_NO_CONTEXT   The context_handle parameter did not identify a valid context.

GSS_S_BAD_QOP   The specified QOP is not supported by the mechanism.

SEE ALSO

gss_release_buffer(3), gss_unwrap(3)

STANDARDS

RFC 2743 Generic Security Service Application Program Interface Version 2, Update 1

RFC 2744 Generic Security Service API Version 2 : C-bindings

HISTORY

The **gss_wrap** function first appeared in FreeBSD 7.0.

AUTHORS

John Wray, Iris Associates

COPYRIGHT

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 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.