

NAME

gss_verify_mic, **gss_verify** - Check a MIC against a message; verify integrity of a received message

SYNOPSIS

```
#include <gssapi/gssapi.h>
```

OM_uint32

```
gss_verify_mic(OM_uint32 *minor_status, const gss_ctx_id_t context_handle,  
               const gss_buffer_t message_buffer, const gss_buffer_t token_buffer, gss_qop_t *qop_state);
```

OM_uint32

```
gss_verify(OM_uint32 *minor_status, gss_ctx_id_t context_handle, gss_buffer_t message_buffer,  
           gss_buffer_t token_buffer, gss_qop_t *qop_state);
```

DESCRIPTION

Verifies that a cryptographic MIC, contained in the token parameter, fits the supplied message. The *qop_state* parameter allows a message recipient to determine the strength of protection that was applied to the message.

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

The **gss_verify()** routine is an obsolete variant of **gss_verify_mic()**. 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 arrived.

message_buffer
 Message to be verified.

token_buffer Token associated with message.

qop_state Quality of protection gained from MIC. Specify NULL if not required.

RETURN VALUES

GSS_S_COMPLETE	Successful completion
GSS_S_DEFECTIVE_TOKEN	The token failed consistency checks
GSS_S_BAD_SIG	The MIC was incorrect
GSS_S_DUPLICATE_TOKEN	The token was valid, and contained a correct MIC for the message, but it had already been processed
GSS_S_OLD_TOKEN	The token was valid, and contained a correct MIC for the message, but it is too old to check for duplication
GSS_S_UNSEQ_TOKEN	The token was valid, and contained a correct MIC for the message, but has been verified out of sequence; a later token has already been received.
GSS_S_GAP_TOKEN	The token was valid, and contained a correct MIC for the message, but has been verified out of sequence; an earlier expected token has not yet been received
GSS_S_CONTEXT_EXPIRED	The context has already expired
GSS_S_NO_CONTEXT	The context_handle parameter did not identify a valid context

SEE ALSO

gss_wrap(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_verify_mic** function first appeared in FreeBSD 7.0.

AUTHORS

John Wray, Iris Associates

COPYRIGHT

Copyright (C) The Internet Society (2000). 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 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.