



iSeries

# Generic Security Service APIs

*Version 5 Release 3*







@server

iSeries

Generic Security Service APIs

*Version 5 Release 3*

**Note**

Before using this information and the product it supports, be sure to read the information in "Notices," on page 77.

**Sixth Edition (August 2005)**

This edition applies to version 5, release 3, modification 0 of Operating System/400 (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 1998, 2005. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

## Generic Security Service APIs . . . . . 1

APIs . . . . .	3
<code>gss_accept_sec_context()</code> —Accept Security Context . . . . .	3
Parameters . . . . .	4
Return Value . . . . .	5
Authorities . . . . .	6
Error Messages . . . . .	6
Usage Notes . . . . .	6
<code>gss_acquire_cred()</code> —Acquire GSS Credential . . . . .	8
Parameters . . . . .	8
Return Value . . . . .	9
Authorities . . . . .	9
Error Messages . . . . .	10
Usage Notes . . . . .	10
<code>gss_add_cred()</code> —Add Credential Element to Existing GSS Credential . . . . .	10
Parameters . . . . .	10
Return Value . . . . .	11
Authorities . . . . .	12
Error Messages . . . . .	12
Usage Notes . . . . .	12
<code>gss_add_oid_set_member()</code> —Add OID to an OID Set . . . . .	13
Parameters . . . . .	13
Return Value . . . . .	13
Authorities . . . . .	13
Error Messages . . . . .	13
Usage Notes . . . . .	14
<code>gss_canonicalize_name()</code> —Reduce GSS Internal Name to Mechanism Name . . . . .	14
Parameters . . . . .	14
Return Value . . . . .	15
Authorities . . . . .	15
Error Messages . . . . .	15
<code>gss_compare_name()</code> —Compare Two Internal GSS Names . . . . .	15
Parameters . . . . .	16
Return Value . . . . .	16
Authorities . . . . .	16
Error Messages . . . . .	16
<code>gss_context_time()</code> —Get Number of Seconds Security Context Remains Valid . . . . .	17
Parameters . . . . .	17
Return Value . . . . .	17
Authorities . . . . .	18
Error Messages . . . . .	18
<code>gss_create_empty_oid_set()</code> —Create Empty OID Set . . . . .	18
Parameters . . . . .	18
Return Value . . . . .	18
Authorities . . . . .	19
Error Messages . . . . .	19
<code>gss_delete_sec_context()</code> —Delete Security Context . . . . .	19
Parameters . . . . .	19
Return Value . . . . .	20
Authorities . . . . .	20
Error Messages . . . . .	20

Usage Notes . . . . .	20
<code>gss_display_name()</code> —Get Textual Representation of Internal GSS Name . . . . .	21
Parameters . . . . .	21
Return Value . . . . .	21
Authorities . . . . .	22
Error Messages . . . . .	22
Usage Notes . . . . .	22
<code>gss_display_status()</code> —Get Textual Representation of GSS Status Code or Mechanism Code . . . . .	22
Parameters . . . . .	23
Return Value . . . . .	23
Authorities . . . . .	23
Error Messages . . . . .	24
Usage Notes . . . . .	24
<code>gss_duplicate_name()</code> —Create Duplicate GSS Internal Name . . . . .	24
Parameters . . . . .	24
Return Value . . . . .	24
Authorities . . . . .	25
Error Messages . . . . .	25
<code>gss_export_cred()</code> —Export GSS Credential . . . . .	25
Parameters . . . . .	26
Return Value . . . . .	26
Authorities . . . . .	26
Error Messages . . . . .	26
<code>gss_export_name()</code> —Create Opaque Token for a Mechanism Name . . . . .	27
Parameters . . . . .	27
Return Value . . . . .	27
Authorities . . . . .	27
Error Messages . . . . .	28
<code>gss_export_sec_context()</code> —Export Security Context . . . . .	28
Parameters . . . . .	28
Return Value . . . . .	29
Authorities . . . . .	29
Error Messages . . . . .	29
<code>gss_get_mic()</code> —Generate Cryptographic Signature for Message . . . . .	29
Parameters . . . . .	30
Return Value . . . . .	30
Authorities . . . . .	30
Error Messages . . . . .	31
<code>gss_import_cred()</code> —Import GSS Credential . . . . .	31
Parameters . . . . .	31
Return Value . . . . .	31
Authorities . . . . .	32
Error Messages . . . . .	32
<code>gss_import_name()</code> —Convert Printable Name to GSS Internal Format . . . . .	32
Parameters . . . . .	32
Return Value . . . . .	33
Authorities . . . . .	33
Error Messages . . . . .	34
<code>gss_import_sec_context()</code> —Import Security Context . . . . .	34
Parameters . . . . .	34

Return Value . . . . .	34	<code>gss_krb5_ccache_name()</code> —Set Default Kerberos Protocol Credentials Cache Name . . . . .	53
Authorities . . . . .	35	Parameters . . . . .	53
Error Messages . . . . .	35	Return Value . . . . .	53
<code>gss_indicate_mechs()</code> —Determine Available Security Mechanisms . . . . .	35	Authorities . . . . .	53
Parameters . . . . .	35	Error Messages . . . . .	53
Return Value . . . . .	35	<code>gss_krb5_copy_ccache()</code> —Copy Tickets From Associated GSS Credentials to Kerberos Protocol Credentials Cache . . . . .	54
Authorities . . . . .	36	Parameters . . . . .	54
Error Messages . . . . .	36	Return Value . . . . .	54
<code>gss_init_sec_context()</code> —Initiate Security Context . . . . .	36	Authorities . . . . .	55
Parameters . . . . .	37	Error Messages . . . . .	55
Return Value . . . . .	38	<code>gss_krb5_get_tkt_flags()</code> —Get Kerberos Protocol Ticket Flags . . . . .	55
Authorities . . . . .	39	Parameters . . . . .	55
Error Messages . . . . .	39	Return Value . . . . .	55
Usage Notes . . . . .	39	Authorities . . . . .	56
<code>gss_inquire_context()</code> —Get Information About Security Context . . . . .	41	Error Messages . . . . .	56
Parameters . . . . .	41	<code>gss_oid_to_str()</code> —Convert OID Object to String Representation of Object . . . . .	56
Return Value . . . . .	42	Parameters . . . . .	57
Authorities . . . . .	43	Return Value . . . . .	57
Error Messages . . . . .	43	Authorities . . . . .	57
<code>gss_inquire_cred()</code> —Get Information About GSS Credential . . . . .	43	Error Messages . . . . .	57
Parameters . . . . .	43	<code>gss_process_context_token()</code> —Process Received Context Token . . . . .	58
Return Value . . . . .	44	Parameters . . . . .	58
Authorities . . . . .	44	Return Value . . . . .	58
Error Messages . . . . .	45	Authorities . . . . .	58
<code>gss_inquire_cred_by_mech()</code> —Get Information About GSS Credential for Single Security Mechanism . . . . .	45	Error Messages . . . . .	59
Parameters . . . . .	45	Usage Notes . . . . .	59
Return Value . . . . .	46	<code>gss_release_buffer()</code> —Release Storage Associated with Buffer . . . . .	59
Authorities . . . . .	46	Parameters . . . . .	59
Error Messages . . . . .	46	Return Value . . . . .	60
<code>gss_inquire_mechs_for_name()</code> —Determine Mechanisms to Process Name . . . . .	47	Authorities . . . . .	60
Parameters . . . . .	47	Error Messages . . . . .	60
Return Value . . . . .	47	<code>gss_release_cred()</code> —Release Storage Associated with GSS Credential . . . . .	60
Authorities . . . . .	48	Parameters . . . . .	60
Error Messages . . . . .	48	Return Value . . . . .	61
<code>gss_inquire_names_for_mech()</code> —Get Name Types Supported by Security Mechanism. . . . .	48	Authorities . . . . .	61
Parameters . . . . .	48	Error Messages . . . . .	61
Return Value . . . . .	49	<code>gss_release_name()</code> —Release Storage Associated with GSS Internal Name . . . . .	62
Authorities . . . . .	49	Parameters . . . . .	62
Error Messages . . . . .	49	Return Value . . . . .	62
<code>gss_krb5_get_ccache()</code> —Get Kerberos Protocol Credentials Cache Associated with Specified GSS Credential . . . . .	49	Authorities . . . . .	62
Parameters . . . . .	50	Error Messages . . . . .	62
Return Value . . . . .	50	<code>gss_release_oid()</code> —Release Storage Associated with OID Object . . . . .	63
Authorities . . . . .	50	Parameters . . . . .	63
Error Messages . . . . .	50	Return Value . . . . .	63
<code>gss_krb5_acquire_cred_cache()</code> —Acquire GSS Credential from a Kerberos Protocol Credentials Cache . . . . .	51	Authorities . . . . .	63
Parameters . . . . .	51	Error Messages . . . . .	64
Return Value . . . . .	52	<code>gss_release_oid_set()</code> —Release Storage Associated with a Set of OID Objects. . . . .	64
Authorities . . . . .	52	Parameters . . . . .	64
Error Messages . . . . .	52	Return Value . . . . .	64
		Authorities . . . . .	64

Error Messages . . . . .	65	Return Value . . . . .	71
gss_str_to_oid()—Convert String Representation of an Object Identifier to an Internal OID Object . . .	65	Authorities . . . . .	71
Parameters . . . . .	65	Error Messages . . . . .	72
Return Value . . . . .	65	gss_wrap()—Cryptographically Sign and Optionally Encrypt Message . . . . .	72
Authorities . . . . .	66	Parameters . . . . .	72
Error Messages . . . . .	66	Return Value . . . . .	73
Usage Notes . . . . .	66	Authorities . . . . .	73
gss_test_oid_set_member()—Determine if Specified OID is Contained in a Specified OID Set. . . . .	67	Error Messages . . . . .	74
Parameters . . . . .	67	Usage Notes . . . . .	74
Return Value . . . . .	67	gss_wrap_size_limit()—Determine Largest Message that can be Wrapped . . . . .	74
Authorities . . . . .	67	Parameters . . . . .	74
Error Messages . . . . .	68	Return Value . . . . .	75
Usage Notes . . . . .	68	Authorities . . . . .	75
gss_unwrap()—Unwrap a Message . . . . .	68	Error Messages . . . . .	75
Parameters . . . . .	68	<b>Appendix. Notices . . . . .</b>	<b>77</b>
Return Value . . . . .	69	Trademarks . . . . .	78
Authorities . . . . .	70	Terms and conditions for downloading and printing publications . . . . .	79
Error Messages . . . . .	70	Code disclaimer information. . . . .	80
gss_verify_mic()—Verify that Cryptographic Signature is Correct. . . . .	70		
Parameters . . . . .	70		





---

## Generic Security Service APIs

The Generic Security Service APIs support job environments for most EBCDIC CCSIDs. CCSID 290 and 5026 are not supported because of the variance of lowercase letters a to z.

The GSS APIs provide security services to applications that use peer-to-peer communications. For more information on this topic, see Network Authentication Service.

The Generic Security Service APIs are:

- “`gss_accept_sec_context()`—Accept Security Context” on page 3 (Accept security context) accepts a security context created by the context initiator.
- “`gss_acquire_cred()`—Acquire GSS Credential” on page 8 (Acquire GSS credential) allows an application to acquire a GSS credential.
- “`gss_add_cred()`—Add Credential Element to Existing GSS Credential” on page 10 (Add credential element to existing GSS credential) adds a credential element to an existing GSS credential.
- “`gss_add_oid_set_member()`—Add OID to an OID Set” on page 13 (Add OID to an OID set) adds a new OID to an existing OID set.
- “`gss_canonicalize_name()`—Reduce GSS Internal Name to Mechanism Name” on page 14 (Reduce GSS internal name to mechanism name) takes a GSS internal name that contains multiple internal representations and returns a new GSS internal name with a single name representation that corresponds to the specified security mechanism.
- “`gss_compare_name()`—Compare Two Internal GSS Names” on page 15 (Compare two internal GSS names) allows an application to compare two internal names to determine whether they refer to the same object.
- “`gss_context_time()`—Get Number of Seconds Security Context Remains Valid” on page 17 (Get number of seconds security context remains valid) checks the specified security context and returns the number of seconds that the context remains valid.
- “`gss_create_empty_oid_set()`—Create Empty OID Set” on page 18 (Create empty OID set) creates a new, empty OID set. Members can be added to the OID set by calling the `gss_add_oid_set_member()` routine.
- “`gss_delete_sec_context()`—Delete Security Context” on page 19 (Delete security context) deletes one end of a security context.
- “`gss_display_name()`—Get Textual Representation of Internal GSS Name” on page 21 (Get textual representation of internal GSS name) returns the textual representation of an opaque internal name.
- “`gss_display_status()`—Get Textual Representation of GSS Status Code or Mechanism Code” on page 22 (Get textual representation of GSS status code or mechanism code) provides an application with a textual representation of a GSS or mechanism status code.
- “`gss_duplicate_name()`—Create Duplicate GSS Internal Name” on page 24 (Create duplicate GSS internal name) creates a duplicate of a GSS internal name.
- “`gss_export_cred()`—Export GSS Credential” on page 25 (Export GSS Credential) creates a credential token for a GSS-API credential.
- “`gss_export_name()`—Create Opaque Token for a Mechanism Name” on page 27 (Create Opaque Token for a Mechanism Name) creates an opaque token for a mechanism name.
- “`gss_export_sec_context()`—Export Security Context” on page 28 (Export Security Context) creates a context token for a GSS API security context.
- “`gss_get_mic()`—Generate Cryptographic Signature for Message” on page 29 (Generate cryptographic signature for message) generates a cryptographic signature for a message and returns this signature in a token that can be sent to a partner application.

- “gss\_import\_cred()—Import GSS Credential” on page 31 (Import GSS Credential) accepts a credential token created by the `gss_export_cred()` routine and creates a GSS API credential.
- “gss\_import\_name()—Convert Printable Name to GSS Internal Format” on page 32 (Convert printable name to GSS internal format) converts a printable name to the GSS internal format.
- “gss\_import\_sec\_context()—Import Security Context” on page 34 (Import Security Context) accepts a security context token created by the `gss_export_sec_context()` routine and creates a GSS API security context.
- “gss\_indicate\_mechs()—Determine Available Security Mechanisms” on page 35 (Determine available security mechanisms) allows an application to determine which security mechanisms are available on the local system.
- “gss\_init\_sec\_context()—Initiate Security Context” on page 36 (Initiate security context) initiates a security context for use by two communicating applications.
- “gss\_inquire\_context()—Get Information About Security Context” on page 41 (Get information about security context) returns information about a security context to the calling application.
- “gss\_inquire\_cred()—Get Information About GSS Credential” on page 43 (Get information about GSS credential) returns information about a GSS credential to the calling application.
- “gss\_inquire\_cred\_by\_mech()—Get Information About GSS Credential for Single Security Mechanism” on page 45 (Get information about GSS credential for single security mechanism) returns information about a GSS credential for a single security mechanism.
- “gss\_inquire\_mechs\_for\_name()—Determine Mechanisms to Process Name” on page 47 (Determine mechanisms to process name) returns the mechanisms with which a name may be processed.
- “gss\_inquire\_names\_for\_mech()—Get Name Types Supported by Security Mechanism” on page 48 (Get name types supported by security mechanism) returns the name types supported by a security mechanism.
- “gss\_krb5\_acquire\_cred\_cache()—Acquire GSS Credential from a Kerberos Protocol Credentials Cache” on page 51 (Acquire GSS Credential from a Kerberos Protocol Credentials Cache) acquires a GSS API credential using a Kerberos credentials cache.
- “gss\_krb5\_ccache\_name()—Set Default Kerberos Protocol Credentials Cache Name” on page 53 (Set Default Kerberos Protocol Credentials Cache Name) sets the default credentials cache name for use by the Kerberos mechanism.
- “gss\_krb5\_copy\_ccache()—Copy Tickets From Associated GSS Credentials to Kerberos Protocol Credentials Cache” on page 54 (Copy Tickets From Associated GSS Credentials to Kerberos Protocol Credentials Cache) copies the tickets from the Kerberos credentials cache associated with a GSS API credential to a credentials cache provided by the caller.
- “gss\_krb5\_get\_ccache()—Get Kerberos Protocol Credentials Cache Associated with Specified GSS Credential” on page 49 (Get Kerberos protocol credentials cache associated with specified GSS credential) returns the handle for the Kerberos credentials cache associated with a GSS credential.
- “gss\_krb5\_get\_tkt\_flags()—Get Kerberos Protocol Ticket Flags” on page 55 (Get Kerberos protocol ticket flags) returns the Kerberos ticket flags from the Kerberos ticket associated with the security context.
- “gss\_oid\_to\_str()—Convert OID Object to String Representation of Object” on page 56 (Convert OID object to string representation of object) converts a `gss_oid` object to a string representation of the object identifier.
- “gss\_process\_context\_token()—Process Received Context Token” on page 58 (Process received context token) processes a context token received from the partner application.
- “gss\_release\_buffer()—Release Storage Associated with Buffer” on page 59 (Release storage associated with buffer) releases storage associated with a `gss_buffer_t` buffer. The `gss_buffer_desc` structure itself is not released.
- “gss\_release\_cred()—Release Storage Associated with GSS Credential” on page 60 (Release storage associated with GSS credential) releases the local data structures associated with a GSS credential.

- “gss\_release\_name()—Release Storage Associated with GSS Internal Name” on page 62 (Release storage associated with GSS internal name) releases storage associated with a gss\_name\_t internal name.
- “gss\_release\_oid()—Release Storage Associated with OID Object” on page 63 (Release storage associated with OID object) releases storage associated with a gss\_oid object.
- “gss\_release\_oid\_set()—Release Storage Associated with a Set of OID Objects” on page 64 (Release storage associated with a set of OID objects) releases storage associated with a gss\_oid\_set object.
- “gss\_str\_to\_oid()—Convert String Representation of an Object Identifier to an Internal OID Object” on page 65 (Convert string representation of an object identifier to an internal OID object) converts the string representation of an object identifier to a gss\_OID object.
- “gss\_test\_oid\_set\_member()—Determine if Specified OID is Contained in a Specified OID Set” on page 67 (Determine if specified OID is contained in a specified OID set) checks an oid set to see if a specified oid is a member of the set.
- “gss\_unwrap()—Unwrap a Message” on page 68 (Unwrap a message) unwraps a message sealed by the gss\_wrap() routine and verifies the embedded signature.
- “gss\_verify\_mic()—Verify that Cryptographic Signature is Correct” on page 70 (Verify that cryptographic signature is correct) verifies that the cryptographic signature for a message is correct.
- “gss\_wrap()—Cryptographically Sign and Optionally Encrypt Message” on page 72 (Cryptographically sign and optionally encrypt message) cryptographically signs and optionally encrypts a message.
- “gss\_wrap\_size\_limit()—Determine Largest Message that can be Wrapped” on page 74 (Determine largest message that can be wrapped) determines the largest message that can be processed by the gss\_wrap() routine without exceeding the specified output token size.

Top | Security APIs | UNIX-Type APIs | APIs by category

---

## APIs

These are the APIs for this category.

---

### **gss\_accept\_sec\_context()—Accept Security Context**

Syntax

```
#include <gssapi.h>

OM_uint32 gss_accept_sec_context (
    OM_uint32 *   minor_status,
    gss_ctx_id_t * context_handle,
    gss_cred_id_t acceptor_cred_handle,
    gss_buffer_t  input_token,
    gss_channel_bindings_t input_chan_bindings,
    gss_name_t *  src_name,
    gss_OID *     mech_type,
    gss_buffer_t  output_token,
    gss_flags_t * ret_flags,
    OM_uint32 *  time_rec,
    gss_cred_id_t * delegated_cred_handle);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_accept\_sec\_context()** function accepts a security context created by the context initiator.

## Parameters

### **minor\_status (Output)**

A status code from the security mechanism.

### **context\_handle (Input/Output)**

A context handle for the context. The first time the context acceptor calls the `gss_accept_sec_context()` routine, the context handle value must be set to `GSS_C_NO_CONTEXT`. For subsequent calls to continue setting up the context, the context handle must be the value returned by the previous call to the `gss_accept_sec_context()` routine.

### **acceptor\_cred\_handle (Input)**

The GSS credential for the identity claimed by the context acceptor. The credential must have been created using either `GSS_C_ACCEPT` or `GSS_C_BOTH`.

### **input\_token (Input)**

The token received from the context initiator.

### **input\_chan\_bindings (Input)**

The bindings describing the communications channel used between the communicating applications. The channel bindings specified by the context acceptor must match the bindings that were specified by the context initiator when the input token was created. Specify `GSS_C_NO_CHANNEL_BINDINGS` if there are no channel bindings.

### **src\_name (Output)**

The authenticated name of the context initiator. If the authenticated name is not required, specify `NULL` for this parameter. The returned name is an anonymous internal name if the `GSS_C_ANON_FLAG` is set in the returned flags.

### **mech\_type (Output)**

The security mechanism with which the context was established. If the security mechanism type is not required, specify `NULL` for this parameter. The `gss_OID` value returned for this parameter points to a read-only structure and must not be released by the application. The returned security mechanism is one of the following:

`gss_mech_krb5_old` Beta Kerberos V5 mechanism

`gss_mech_krb5` Kerberos V5 mechanism

### **output\_token (Output)**

A token to be returned to the context initiator. If no token is to be passed to the context initiator, the `gss_accept_sec_context()` routine sets the `output_token_length` field to zero. Otherwise, the `output_token_length` and `value` fields are set to nonzero values. The application should release the output token when it is no longer needed by calling the `gss_release_buffer()` routine.

### **ret\_flags (Output)**

A bit mask containing independent flags representing services that have been requested by the initiating application. Specify `NULL` for this parameter if the flag values are not required. The following symbolic definitions are provided to test the individual flags and should be logically ANDed with the value of `ret_flags` to test whether the context supports the service option.

`GSS_C_ANON_FLAG`

Anonymous services are available if this flag is TRUE. The `src_name` parameter returns an anonymous internal name.

`GSS_C_CONF_FLAG`

Confidentiality services are available if this flag is TRUE.

`GSS_C_DELEG_FLAG`

Delegated credentials are available if this flag is TRUE.

`GSS_C_INTEG_FLAG`

Integrity services are available if this flag is TRUE.

`GSS_C_MUTUAL_FLAG`

Mutual authentication is required if this flag is TRUE.

<code>GSS_C_PROT_READY_FLAG</code>	Protection services, as specified by the <code>GSS_C_CONF_FLAG</code> and <code>GSS_C_INTEG_FLAG</code> , are available if the accompanying major status is <code>GSS_S_COMPLETE</code> or <code>GSS_S_CONTINUE_NEEDED</code> . Otherwise, protection services are available only if the accompanying major status is <code>GSS_S_COMPLETE</code> .
<code>GSS_C_REPLAY_FLAG</code>	Replayed signed or sealed messages are detected if this flag is TRUE.
<code>GSS_C_SEQUENCE_FLAG</code>	Out-of-sequence signed or sealed messages are detected if this flag is TRUE.

**time\_rec (Output)**

The number of seconds remaining before the context is no longer valid. If the mechanism does not support credential expiration, the return value is `GSS_C_INDEFINITE`. Specify `NULL` for this parameter if the remaining time is not required.

**delegated\_cred\_handle (Output)**

The credential handle for delegated credentials received from the context initiator. Specify `NULL` for this parameter if the delegated credentials are not required. A credential handle is returned only if the `GSS_C_DELEG_FLAG` flag is set in the return flags. The returned credential can then be used to initiate a new security context by calling the `gss_init_sec_context()` routine. The returned credential should be released when it is no longer needed by calling the `gss_release_cred()` routine.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_BAD\_BINDINGS**

The `input_token` parameter contains different channel bindings from those specified with the `input_chan_bindings` parameter.

**GSS\_S\_BAD\_MECH**

The security mechanism used by the context initiator is not available on the acceptor system.

**GSS\_S\_BAD\_SIG**

The received input token contains an incorrect signature.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CONTINUE\_NEEDED**

Control information in the returned output token must be sent to the initiator and a response must be received and passed as the `input_token` argument to a continuation call to the `gss_accept_sec_context()` routine.

**GSS\_S\_CREDENTIALS\_EXPIRED**

Credentials are no longer valid.

**GSS\_S\_DEFECTIVE\_CREDENTIAL**

Consistency checks performed on the credential structure referenced by the `verifier_cred_handle` parameter failed.

**GSS\_S\_DEFECTIVE\_TOKEN**

Consistency checks performed on the input token failed.

**GSS\_S\_DUPLICATE\_TOKEN**

The token is a duplicate of a token that already has been processed. This is a fatal error during context establishment.

## GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## GSS\_S\_NO\_CONTEXT

The context identifier provided by the caller does not refer to a valid security context.

## GSS\_S\_NO\_CRED

No credentials are available or the credentials are valid for context initiation use only.

## GSS\_S\_OLD\_TOKEN

The token is too old to be checked for duplication against previous tokens. This is a fatal error during context establishment.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R
Each directory in the path name preceding the keytab file	*X
Keytab file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. The **gss\_accept\_sec\_context()** routine is the second step in establishing a security context between the context initiator and the context acceptor. In the first step, the context initiator calls the **gss\_init\_sec\_context()** routine, which returns a token for the security context. The context initiator then passes this security token to the context acceptor. In the second step, the context acceptor takes the token supplied by the context initiator and calls the **gss\_accept\_sec\_context()** routine to accept the context.

If the length value in the *output\_token* is not zero, the context acceptor must pass the returned token to the context initiator. The context initiator must then call **gss\_init\_sec\_context()** and specify the context identifier returned by the original call to **gss\_init\_sec\_context()**, as well as the output token that was returned by the context acceptor.

To complete the context establishment, one or more reply tokens may be required from the peer application. If so, **gss\_accept\_sec\_context()** returns a status flag of **GSS\_S\_CONTINUE\_NEEDED**, in which case it should be called again when the reply token is received from the peer application, passing the token to **gss\_accept\_sec\_context()** through the *input\_token* parameter.

2. The availability of confidentiality services is dependent on the underlying security mechanism and the features that have been installed on the system. The **GSS\_C\_CONF\_FLAG** is returned only if confidentiality services are available on both the local and remote systems. If confidentiality services are available on the remote system but not on the local system, an error is returned by the **gss\_unwrap()** routine if an encrypted message is received (that is, confidentiality was requested on the call to the **gss\_wrap()** routine on the remote system).
3. Whenever the **GSS\_S\_CONTINUE\_NEEDED** status flag is set, the context is not fully established and the following restrictions apply to the output parameters:

- The value returned by the *time\_rec* parameter is undefined.
- Unless the accompanying *ret\_flags* parameter contains the bit **GSS\_C\_PROT\_READY\_FLAG**, indicating that per-message services may be applied in advance of a successful completion status, the value returned by the *mech\_type* parameter may be undefined until the routine returns a major status of **GSS\_S\_COMPLETE**.
- The values of the **GSS\_C\_DELEG\_FLAG**, **GSS\_C\_MUTUAL\_FLAG**, **GSS\_C\_REPLAY\_FLAG**, **GSS\_C\_SEQUENCE\_FLAG**, **GSS\_C\_CONF\_FLAG**, **GSS\_C\_INTEG\_FLAG**, and **GSS\_C\_ANON\_FLAG** bits returned by the *ret\_flags* parameter contain the values that the implementation expects would be valid if context establishment were to succeed.
- The value of the **GSS\_C\_PROT\_READY\_FLAG** bit returned by the *ret\_flags* parameter indicates the actual state at the time **gss\_accept\_sec\_context()** returns, whether or not the context is fully established.

#### 4. Kerberos mechanism

- The **gss\_accept\_sec\_context()** routine needs a key to decrypt the token provided by the context initiator. The token contains the clear text principal name of the context acceptor. This name identifies the key that the context initiator used to encrypt the token. The default key table is used to obtain the key for the indicated principal. The **KRB5\_KTNAME** environment variable can be set to use a different key table.
- The context expiration time is obtained from the service ticket that was obtained by the context initiator as part of the **gss\_init\_sec\_context()** processing.
- When delegation is used, the forwarded Kerberos credentials are stored in a new Kerberos credentials cache that will be associated with the GSS credential returned for the *delegated\_cred\_handle* parameter. This GSS credential can then be used to initiate new security contexts on behalf of the original context initiator.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_acquire\_cred()—Acquire GSS Credential

```
Syntax
#include <gssapi.h>

OM_uint32 gss_acquire_cred(
    OM_uint32 *   minor_status,
    gss_name_t    desired_name,
    OM_uint32     time_req,
    gss_OID_set   desired_mechs,
    gss_cred_usage_t cred_usage,
    gss_cred_id_t * output_cred_handle,
    gss_OID_set * actual_mechs,
    OM_uint32 *   time_rec);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_acquire_cred()` function allows an application to acquire a GSS credential. The application can then use the credential with the `gss_init_sec_context()` and `gss_accept_sec_context()` routines.

### Parameters

#### **minor\_status (Output)**

A status code from the security mechanism.

#### **desired\_name (Input)**

The principal name to be used for the credential. Specify `GSS_C_NO_NAME` for this parameter to use the name obtained from the default login context.

#### **time\_req (Input)**

The number of seconds that the credential remains valid. Specify `GSS_C_INDEFINITE` to request the maximum credential lifetime. Specify zero for the default lifetime of 2 hours. The actual credential lifetime is limited by the lifetime of the underlying ticket-granting ticket for `GSS_C_INITIATE` and `GSS_C_BOTH` credentials.

#### **desired\_mechs (Input)**

The desired security mechanisms for use with the credential. Mechanisms that are not available on the local system are ignored. The actual mechanisms that can be used with the credential are returned in the *actual\_mechs* parameter. Specify `GSS_C_NO_OID_SET` for this parameter to use the default mechanism of `gss_mech_krb5`.

The following security mechanisms are supported:

`gss_mech_krb5_old` Beta Kerberos V5 mechanism  
`gss_mech_krb5` Kerberos V5 mechanism

#### **cred\_usage (Input)**

The desired credential usage as follows:

`GSS_C_ACCEPT` The credential can be used only to accept security contexts.



**GSS\_C\_BOTH** The credential can be used to both initiate and accept security contexts.  
**GSS\_C\_INITIATE** The credential can be used only to initiate security contexts.

**output\_cred\_handle (Output)**

The handle for the GSS credential.

**actual\_mechs (Output)**

The set of mechanism identifiers for which the credential is valid. If the actual mechanisms are not required, specify **NULL** for this parameter. The `gss_OID_set` returned for this parameter should be released by calling the `gss_release_oid_set()` routine when it is no longer needed.

**time\_rec (Output)**

The number of seconds for which the credential will remain valid. If the time remaining is not required, specify **NULL** for this parameter.

**Return Value**

The return value is one of the following status codes:

**GSS\_S\_BAD\_MECH**

None of the requested mechanisms are supported by the local system.

**GSS\_S\_BAD\_NAME**

The name specified for the *desired\_name* parameter is not valid.

**GSS\_S\_BAD\_NAME\_TYPE**

The name specified for the *desired\_name* parameter is not supported by the applicable underlying GSS mechanisms.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CRED**

No credentials are available or the credentials are valid for context initiation use only.

**Authorities**

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R
Each directory preceding the credential cache file if <b>GSS_C_INITIATE</b> or <b>GSS_C_BOTH</b> is specified for credential usage	*X
Credential cache file	*RW
Each directory preceding the keytab file if <b>GSS_C_ACCEPT</b> or <b>GSS_C_BOTH</b> is specified for credential usage	*X
Keytab file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. If `GSS_C_INITIATE` or `GSS_C_BOTH` is specified for the credential usage, the application must have a valid ticket-granting ticket in the default credentials cache and the ticket must not expire for at least 10 minutes. The `gss_acquire_cred()` routine uses this ticket-granting ticket to create the GSS credential. The principal specified by the `desired_name` parameter must match the principal obtained from the credentials cache or must be specified as `GSS_C_NO_NAME`. The `KRB5CCNAME` environment variable is used to identify the credentials cache used by the Kerberos security mechanism.
2. If `GSS_C_ACCEPT` or `GSS_C_BOTH` is specified for the credential usage, the principal specified by the `desired_name` parameter must be defined in a key table. The `KRB5_KTNAME` environment variable can be used to set the key table used by the Kerberos security mechanism.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_add_cred()`—Add Credential Element to Existing GSS Credential

Syntax

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

```
OM_uint32 gss_add_cred(  
    OM_uint32 *   minor_status,  
    gss_cred_id_t input_cred_handle,  
    gss_name_t    desired_name,  
    gss_OID      mech_type,  
    gss_cred_usage_t cred_usage,  
    OM_uint32    init_time_req,  
    OM_uint32    accept_time_req,  
    gss_cred_id_t * output_cred_handle,  
    gss_OID_set *  actual_mechs,  
    OM_uint32 *   init_time_rec,  
    OM_uint32 *   accept_time_rec);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_add_cred()` function adds a credential element to an existing GSS credential. The credential must not already contain an element for the mechanism. A GSS credential must contain an element for each mechanism that will be used for contexts that are initiated or accepted using the credential.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

**input\_cred\_handle (Input)**

The GSS credential that is to be modified. Specify **GSS\_C\_NO\_CREDENTIAL** to modify the default GSS credential.

**desired\_name (Input)**

The principal name to be used for the credential.

**mech\_type (Input)**

The mechanism element to be added to the credential. The credential must not already contain an element for this mechanism.

The following security mechanisms are supported:

*gss\_mech\_krb5\_old* Beta Kerberos V5 mechanism

*gss\_mech\_krb5* Kerberos V5 mechanism

**cred\_usage (Input)**

The desired credential usage as follows:

*GSS\_C\_ACCEPT* The credential can be used only to accept security contexts.

*GSS\_C\_BOTH* The credential can be used to both initiate and accept security contexts.

*GSS\_C\_INITIATE* The credential can be used only to initiate security contexts.

**init\_time\_req (Input)**

The number of seconds the credential remains valid for initiating contexts. The OS/400 implementation of GSS does not support separate initiate and accept expiration times. The actual expiration time will be the smaller of the initiate and accept times. Specify zero to request the default lifetime of 2 hours. Specify **GSS\_C\_INDEFINITE** to request the maximum lifetime.

**accept\_time\_req (Input)**

The number of seconds the credential remains valid for accepting contexts. The OS/400 implementation of GSS does not support separate initiate and accept expiration times. The actual expiration time will be the smaller of the initiate and accept times. Specify zero to request the default lifetime of 2 hours. Specify **GSS\_C\_INDEFINITE** to request the maximum lifetime.

**output\_cred\_handle (Output)**

The credential handle for the updated credential. If **NULL** is specified for this parameter, the new credential element is added to the input credential. Otherwise, a new credential is created from the input credential and contains all of the credential elements of the input credential plus the new credential element. **NULL** may not be specified for this parameter if **GSS\_C\_NO\_CREDENTIAL** is specified for the input credential.

**actual\_mechs (Output)**

The total set of mechanisms supported by the GSS credential. Specify **NULL** for this parameter if the actual mechanisms are not required. The *gss\_OID\_set* returned for this parameter should be released by calling the **gss\_release\_oid\_set()** routine when it is no longer needed.

**init\_time\_rec (Output)**

The initiate expiration time in seconds. Specify **NULL** for this parameter if the initiate time is not required.

**accept\_time\_rec (Output)**

The accept expiration time in seconds. Specify **NULL** for this parameter if the accept time is not required.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_BAD\_MECH**

The specified mechanism is not supported.

**GSS\_S\_BAD\_NAME**

The name specified for the *desired\_name* parameter is not valid.

**GSS\_S\_BAD\_NAME\_TYPE**

The name specified for the *desired\_name* parameter is not supported by the applicable underlying GSS mechanisms.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_DUPLICATE\_ELEMENT**

The credential already contains an element for the specified mechanism.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CRED**

The referenced credential does not exist.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. The `gss_add_cred()` routine performs the same function as the `gss_acquire_cred()` routine for a single mechanism.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

## **gss\_add\_oid\_set\_member()**—Add OID to an OID Set

```
Syntax
#include <gssapi.h>

OM_uint32 gss_add_oid_set_member(
    OM_uint32 *   minor_status,
    gss_OID      input_oid,
    gss_OID_set * oid_set);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_add_oid_set_member()` function adds a new OID to an existing OID set.

### **Parameters**

**minor\_status (Output)**

A status code from the security mechanism.

**input\_oid (Input)**

The OID to add to the OID set.

**oid\_set (Input/Output)**

The OID set. The `gss_OID` array referenced by the `elements` field of the `gss_OID_set` will be reallocated to hold the new OID. The application should call the `gss_release_oid_set()` routine to release the OID set when it is no longer needed.

### **Return Value**

The return value is one of the following status codes:

<code>GSS_S_COMPLETE</code>	The routine completed successfully.
<code>GSS_S_FAILURE</code>	The routine failed for reasons that are not defined at the GSS level. The <code>minor_status</code> return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **Authorities**

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

### **Error Messages**

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. You can create an empty OID set by calling the `gss_create_empty_oid_set()` routine. The `gss_add_oid_set_member()` routine makes a copy of the input OID, so any future changes to the input OID will have no effect on the copy in the OID set.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_canonicalize_name()`—Reduce GSS Internal Name to Mechanism Name

Syntax

```
#include <gssapi.h>

OM_uint32 gss_canonicalize_name(
    OM_uint32 *   minor_status,
    gss_name_t    input_name,
    gss_OID       mech_type,
    gss_name_t *  output_name);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_canonicalize_name()` routine takes a GSS internal name that contains multiple internal representations and returns a new GSS internal name with a single name representation that corresponds to the specified security mechanism. A name that represents a single security mechanism is called a **mechanism name**.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `input_name` (Input)

The name to be processed. An error is returned if `GSS_C_NO_NAME` is specified for this parameter.

### `mech_type` (Input)

The security mechanism to be used.

The following security mechanisms are supported:

`gss_mech_krb5_old` Beta Kerberos V5 mechanism  
`gss_mech_krb5` Kerberos V5 mechanism

### `output_name` (Output)

The mechanism name. The `gss_name_t` returned by this parameter should be released by calling the `gss_release_name()` function when it is no longer needed.

## Return Value

The return value is one of the following status codes:

### GSS\_S\_BAD\_MECH

The specified mechanism is not supported.

### GSS\_S\_BAD\_NAME

The input name is not valid.

### GSS\_S\_BAD\_NAME\_TYPE

The input name does not contain an element for the mechanism.

### GSS\_S\_COMPLETE

The routine completed successfully.

### GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_compare\_name()—Compare Two Internal GSS Names

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_compare_name(     OM_uint32 *   minor_status,     gss_name_t    name1,     gss_name_t    name2,     int *         name_equal);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The `gss_compare_name()` function allows an application to compare two internal names to determine whether they refer to the same object. The two names must have an internal representation format in common to be comparable. The names are considered not equal if either name denotes an anonymous principal.

## Parameters

**minor\_status (Output)**

A status code from the security mechanism.

**name1 (Input)**

The first internal name.

**name2 (Input)**

The second internal name.

**name\_equal (Output)**

Returns 1 if the names refer to the same object and 0 otherwise.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_BAD\_NAME**

One of the input names is not valid.

**GSS\_S\_BAD\_NAME\_TYPE**

The two name types are not comparable. The names must have an internal representation in common to be comparable.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)



---

## **gss\_context\_time()**—Get Number of Seconds Security Context Remains Valid

Syntax

```
#include <gssapi.h>

OM_uint32 gss_context_time(
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    OM_uint32 *   time_rec);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_context\_time()** function checks the specified security context and returns the number of seconds that the context remains valid. The returned value is **GSS\_C\_INDEFINITE** if the context does not have an expiration time. The Kerberos security mechanism does support context expiration and returns the time remaining before the underlying service ticket expires.

### **Parameters**

**minor\_status (Output)**

A status code from the security mechanism.

**context\_handle (Input)**

The context to be checked.

**time\_rec (Output)**

The number of seconds that the context remains valid.

### **Return Value**

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CONTEXT\_EXPIRED**

The referenced context has expired.

**GSS\_S\_CREDENTIALS\_EXPIRED**

The credentials associated with the referenced context have expired.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CONTEXT**

The referenced context does not exist.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_create\_empty\_oid\_set()—Create Empty OID Set

```
Syntax
#include <gssapi.h>

OM_uint32 gss_create_empty_oid_set(
    OM_uint32 *   minor_status,
    gss_OID_set *   oid_set);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_create_empty_oid_set()` function creates a new, empty OID set. Members can be added to the OID set by calling the `gss_add_oid_set_member()` routine. The OID set should be released when it is no longer needed by calling the `gss_release_oid_set()` routine.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `oid_set` (Output)

The OID set created by this routine. The application should call the `gss_release_oid_set()` routine to release the OID set when it is no longer needed.

## Return Value

The return value is one of the following status codes:

### `GSS_S_COMPLETE`

The routine completed successfully.

## GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_delete\_sec\_context()—Delete Security Context

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_delete_sec_context (     OM_uint32 *   minor_status,     gss_ctx_id_t * context_handle,     gss_buffer_t  output_token);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The `gss_delete_sec_context()` function deletes one end of a security context. It also deletes the local data structures associated with the security context. When it deletes the context, the routine can generate a token. The application must then pass this token to the partner application. The partner application calls the `gss_process_context_token()` routine to process the token and complete the process of deleting the security context.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### context\_handle (Input/Output)

The context to be deleted. Upon successful completion, the *context\_handle* value is set to **GSS\_C\_NO\_CONTEXT**.

### output\_token (Output)

A token to be sent to the partner application. The partner application then passes this token to the **gss\_process\_context\_token()** routine to delete the other end of the security context. The **gss\_delete\_sec\_context()** routine sets the *output\_token\_length* field to zero if no token needs to be sent to the partner application.

**GSS\_C\_NO\_BUFFER** may be specified for the *output\_token* parameter. In this case, no token is returned by the **gss\_delete\_sec\_context()** routine. Both of the communicating applications must call **gss\_delete\_sec\_context()** to delete both ends of the security context.

## Return Value

The return value is one of the following status codes:

### GSS\_S\_COMPLETE

The routine completed successfully.

### GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### GSS\_S\_NO\_CONTEXT

The context identifier provided by the caller does not refer to a valid security context.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. This call can be made by either peer in a security context to flush context-specific information. Both communicating applications must call the **gss\_delete\_sec\_context()** routine if **GSS\_C\_NO\_BUFFER** is specified for the *output\_token* parameter.
2. The *context\_handle* may not be used for additional security services once the **gss\_delete\_sec\_context()** routine has completed successfully.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_display\_name()—Get Textual Representation of Internal GSS Name**

```
Syntax
#include <gssapi.h>

OM_uint32 gss_display_name(
    OM_uint32 *   minor_status,
    gss_name_t    input_name,
    gss_buffer_t  output_name_buffer,
    gss_OID *     output_name_type);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_display_name()` function returns the textual representation of an opaque internal name. The syntax of the text representation is determined by the mechanism that was used to convert the name.

### **Parameters**

#### **minor\_status (Output)**

A status code from the security mechanism.

#### **input\_name (Input)**

The internal name to be converted to a text string.

#### **output\_name\_buffer (Output)**

Return buffer for the character string.

#### **output\_name\_type (Output)**

The name type corresponding to the returned character string. The `gss_OID` value returned for this parameter points to read-only storage and must not be released by the application.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_BAD\_NAME**

The provided name is not valid.

#### **GSS\_S\_BAD\_NAME\_TYPE**

The internal name provided does not have an internal representation for any of the supported mechanisms.

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. Kerberos names are formatted as **principal-name@realm-name**.  
Not every coded character set identifier (CCSID) contains the '@' character; however, alternative CCSID values often are available. For example, instead of using Greece 423, run the job with a default CCSID of 875.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_display\_status()**—Get Textual Representation of GSS Status Code or Mechanism Code

```
Syntax
#include <gssapi.h>

OM_uint32 gss_display_status(
    OM_uint32 * minor_status,
    OM_uint32 status_value,
    int status_type,
    gss_OID mech_type,
    gss_msg_ctx_t * message_context,
    gss_buffer_t status_string);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_display\_status()** function provides an application with a textual representation of a GSS or mechanism status code. The returned message can then be displayed to the user or written to a log file.

## Parameters

### **minor\_status (Output)**

A status code from the security mechanism.

### **status\_value (Input)**

The status value to be converted. A status value of zero is not valid and causes the `gss_display_status()` routine to return a major status of `GSS_S_BAD_STATUS` to the application.

### **status\_type (Input)**

The status value type. The status value type must be one of the following:

`GSS_C_GSS_CODE`                    GSS major status code  
`GSS_C_MECH_CODE`                Mechanism minor status code

### **mech\_type (Input)**

The security mechanism associated with a minor status code. This parameter is used only when converting a minor status code.

### **message\_context (Input/Output)**

Whether the status code has multiples messages to be processed. The first time an application calls `gss_display_status()`, the `message_context` parameter must be initialized to zero. The `gss_display_status()` routine returns the first message and sets the `message_context` parameter to a nonzero value if more messages are available. The application then continues to call the `gss_display_status()` routine to obtain the additional messages until the `message_context` value is zero upon return from the `gss_display_status()` routine.

### **status\_string (Output)**

The text message for the status value.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_BAD\_MECH**

The mechanism specified by the `mech_type` parameter is not supported.

### **GSS\_S\_BAD\_STATUS**

The value of the `status_type` parameter is not `GSS_C_GSS_CODE` or `GSS_C_MECH_CODE` or the value of the `status_value` parameter is not a valid status code.

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. The *message\_context* parameter indicates which error message should be returned when a status code has multiple messages. The first time an application calls the `gss_display_status()` routine, it must initialize the *message\_context* value to zero. The `gss_display_status()` routine then returns the first message for the status code and sets *message\_context* to a nonzero value if there are additional messages available. The application can then continue to call `gss_display_status()` until the *message\_context* value is zero upon return.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_duplicate_name()`—Create Duplicate GSS Internal Name

```
Syntax
#include <gssapi.h>

OM_uint32 gss_duplicate_name(
    OM_uint32 *   minor_status,
    gss_name_t   input_name,
    gss_name_t *  output_name);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_duplicate_name()` function creates a duplicate of a GSS internal name.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `input_name` (Input)

The name to be duplicated. An error is returned if `GSS_C_NO_NAME` is specified for this parameter.

### `output_name` (Output)

The new GSS internal name. The `gss_name_t` returned for this parameter should be released by calling the `gss_release_name()` function when it is no longer needed.

## Return Value

The return value is one of the following status codes:



### GSS\_S\_BAD\_NAME

The input name is not valid.

### GSS\_S\_BAD\_NAME\_TYPE

The input name type is not supported.

### GSS\_S\_COMPLETE

The routine completed successfully.

### GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

## gss\_export\_cred()—Export GSS Credential

<p>Syntax</p> <pre>#include &lt;krb5.h&gt;  krb5_error_code gss_export_cred (     OM_uint32 *     gss_cred_id_t     gss_buffer_t     minor_status,     cred_handle,     cred_token)</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default Public Authority: *USE</p> <p>Threadsafe: Yes</p>
--

The `gss_export_cred()` routine creates a credential token for a GSS-API credential. This credential token can then be given to another process on the same system or on a different system. This second process calls `gss_import_cred()` to create a GSS-API credential from the credential token. In order to use the

credential on a different system, the security mechanism must allow the credential to be used from any system. In the case of the Kerberos security mechanism, this means the Kerberos ticket must not contain a client address list.

A credential can be exported only if it is an initiate credential (GSS\_C\_INITIATE was specified when the credential was created). The major status will be set to GSS\_S\_NO\_CRED if the credential is not an initiate credential. The credential remains available upon completion of the export operation and can be used in subsequent GSS-API operations. The credential token created by one implementation of GSS-API cannot be used with a different implementation of GSS-API.

## Parameters

### **minor\_status (Output)**

Status code returned from the security mechanism.

### **cred\_handle (Input/Output)**

The credential handle of the GSS-API credential to be used to create the credential token. The credential must be an initiate credential.

### **cred\_token (Output)**

The credential token returned. The storage for the token should be released when it is no longer needed by calling the **gss\_release\_buffer()** routine.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_FAILURE**

The routine failed for reasons which are not defined at the GSS level. The **minor\_status** return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **GSS\_S\_NO\_CRED**

The supplied credential handle does not refer to a valid credential.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_export\_name()—Create Opaque Token for a Mechanism Name**

```
Syntax
#include <krb5.h>

krb5_error_code gss_export_name (
    OM_uint32 *          minor_status,
    gss_name_t          input_name,
    gss_buffer_t        exported_name)
```

Service Program Name: QSYS/QKRBGSS

Default Public Authority: \*USE

Threadsafe: Yes

The `gss_export_name()` routine creates an opaque token for a mechanism name.

### **Parameters**

#### **minor\_status (Output)**

Status code returned from the security mechanism.

#### **input\_name (Input)**

The GSS-API name to be exported. This must represent a mechanism name.

#### **exported\_name (Output)**

The token returned that represents the GSS-API name. The `gss_release_buffer()` routine should be called to release the token when it is no longer needed.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

#### **GSS\_S\_NAME\_NOT\_MN**

The supplied name is not a mechanism name. Use the `gss_canonicalize_name()` routine to convert an internal name to a mechanism name.

#### **GSS\_S\_BAD\_NAME\_TYPE**

The input name is not supported by the current GSS-API Implementation.

#### **GSS\_S\_BAD\_NAME**

The input name is not valid.

### **Authorities**

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

The `gss_canonicalize_name()` routine will convert a GSS-API internal name with multiple mechanism representations to a mechanism name. The `gss_canonicalize_name()` and `gss_export_name()` calls enable callers to acquire and process exported name objects, canonicalized and translated in accordance with the procedures of a particular GSS-API mechanism. Exported name objects can, in turn, be input to `gss_import_name()`, yielding equivalent mechanism names. These facilities are designed specifically to enable efficient storage and comparison of names (for example, for use in access control lists).

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_export_sec_context()`—Export Security Context

```
Syntax
#include <krb5.h>

krb5_error_code gss_export_sec_context (
    OM_uint32 *                minor_status,
    gss_ctx_id_t *             context_handle,
    gss_buffer_t               context_token)
```

Service Program Name: QSYS/QKRBGSS

Default Public Authority: \*USE

Threadsafe: Yes

The `gss_export_sec_context()` routine creates a context token for a GSS-API security context. This context token can then be given to another process on the same system. This second process calls `gss_import_sec_context()` to create a GSS-API security context from the context token. Upon successful completion of `gss_export_sec_context()`, the security context is no longer available for use by the current process. The security context token created by one implementation of GSS-API cannot be used with a different implementation of GSS-API.

## Parameters

### `minor_status` (Output)

Status code returned from the security mechanism.

### `context_handle` (Input/Output)

The context handle of the GSS-API security context to be used to create the security context token. The context handle will be set to `GSS_C_NO_CONTEXT` upon successful completion.

### `context_token` (Output)

The security context token returned. The storage for the token should be released when it is no longer needed by calling the `gss_release_buffer()` routine.

## Return Value

The return value is one of the following status codes:

### GSS\_S\_COMPLETE

The routine completed successfully.

### GSS\_S\_FAILURE

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

### GSS\_S\_NO\_CONTEXT

The supplied context handle does not refer to a valid context.

### GSS\_S\_CONTEXT\_EXPIRED

The supplied context is no longer valid.

### GSS\_S\_UNAVAILABLE

Security context cannot be exported.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_get\_mic()**—Generate Cryptographic Signature for Message

```
Syntax
#include <gssapi.h>

OM_uint32 gss_get_mic(
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    gss_qop_t     qop_req,
    gss_buffer_t  input_message
    gss_buffer_t  output_token);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_get_mic()` function generates a cryptographic signature for a message and returns this signature in a token that can be sent to a partner application. The partner application then calls the `gss_verify_mic()` routine to validate the signature.

## Parameters

### **minor\_status (Output)**

A status code from the security mechanism.

### **context\_handle (Input)**

The context to be associated with the message when it is sent to the partner application.

### **qop\_req (Input)**

The requested quality of protection for the message. Specify **GSS\_C\_QOP\_DEFAULT** to use the default quality of protection as defined by the selected security mechanism.

The Kerberos security mechanism supports three quality of protection levels as follows (in decreasing order or speed):

<i>GSS_KRB5_INTEG_C_QOP_MD5</i>	Truncated MD5
<i>GSS_KRB5_INTEG_C_QOP_DES_MD5</i>	DES_MAC of an MD5 hash (default)
<i>GSS_KRB5_INTEG_C_QOP_DES_MAC</i>	Normal DES_MAC algorithm

### **input\_message (Input)**

The message for which a signature is to be generated.

### **output\_token (Output)**

A token containing the message signature. The message and this token are then sent to the partner application, which calls the **gss\_verify\_mic()** function to verify the authenticity of the message.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_BAD\_QOP**

The requested quality of protection value is not valid.

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_CONTEXT\_EXPIRED**

The referenced context has expired.

### **GSS\_S\_CREDENTIALS\_EXPIRED**

The credentials associated with the referenced context have expired.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **GSS\_S\_NO\_CONTEXT**

The context identifier provided by the caller does not refer to a valid security context.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_import\_cred()—Import GSS Credential

Syntax

```
#include <krb5.h>

krb5_error_code gss_import_cred (
    OM_uint32 *          minor_status,
    gss_buffer_t         cred_token,
    gss_ctx_id_t *      cred_handle)

Service Program Name: QSYS/QKRBGSS

Default Public Authority: *USE

Threadsafe: Yes
```

The `gss_import_cred()` routine accepts a credential token created by the `gss_export_cred()` routine and creates a GSS-API credential.

The `gss_release_cred()` routine should be called to release the GSS-API credential when it is no longer needed. The credential token created by one implementation of GSS-API cannot be used with a different implementation of GSS-API.

## Parameters

### `minor_status` (Output)

Status code returned from the security mechanism.

### `cred_token` (Input)

The credential token created by the `gss_export_cred()` routine.

### `cred_handle` (Output)

The credential handle returned for the GSS-API credential created from the credential token. The `gss_release_cred()` routine should be called to release the credential when it is no longer needed.

## Return Value

The return value is one of the following status codes:

### `GSS_S_COMPLETE`

The routine completed successfully.

### `GSS_S_FAILURE`

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## GSS\_S\_DEFECTIVE\_TOKEN

The supplied credential token is not valid.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_import\_name()—Convert Printable Name to GSS Internal Format

```
Syntax
#include <gssapi.h>

OM_uint32 gss_import_name(
    OM_uint32 *   minor_status,
    gss_buffer_t  input_name_buffer,
    gss_OID      input_name_type,
    gss_name_t *  output_name);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_import_name()` function converts a printable name to the GSS internal format. The `gss_name_t` object created by this routine can then be used as input to other GSS routines. The `gss_name_t` object created by the `gss_import_name()` routine contains an internal representation for each of the supported security mechanisms.

Not every coded character set identifier (CCSID) contains the '@' character; however, alternative CCSID values often are available. For example, instead of using Greece 423, run the job with a default CCSID of 875.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `input_name_buffer` (Input)

The buffer containing the name to convert.



### input\_name\_type (Input)

The object identifier for the type of printable name.

The following name types are supported:

*GSS\_C\_NO\_OID*

The default name type. For the OS/400 implementation of GSS, the default is **GSS\_C\_NT\_USER\_NAME**.

*GSS\_C\_NT\_USER\_NAME*

For the Kerberos mechanism, this is assumed to be the name of a Kerberos principal in the format **principal@realm**.

*GSS\_C\_NT\_HOSTBASED\_SERVICE*

A service that is related to a particular host. For the Kerberos mechanism, the service name is specified as **service@host**. The service name is mapped to the principal **service/primary-host@realm** using the **krb5\_sname\_to\_principal()** function. The primary host name must be associated with a Kerberos realm to map the service name to the proper principal.

*GSS\_C\_NT\_HOSTBASED\_SERVICE\_X*

A service that is related to a particular host. This is the same as **GSS\_C\_NT\_HOSTBASED\_SERVICE** and should not be used by new applications.

*gss\_nt\_krb5\_name*

A Kerberos name in the format **principal@realm**. This name type is valid only for the Kerberos mechanism.

*gss\_nt\_krb5\_principal*

A **krb5\_principal** created by the **krb5\_parse\_name()** routine. This name type is valid only for the Kerberos mechanism.

### output\_name (Output)

The name in the GSS internal format. The internal format contains an internal representation for each of the supported security mechanisms.

## Return Value

The return value is one of the following status codes:

#### **GSS\_S\_BAD\_NAME**

The input name is not formatted properly or is not valid.

#### **GSS\_S\_BAD\_NAMETYPE**

The name type specified by the *input\_name\_type* parameter is not valid.

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_import\_sec\_context()**—Import Security Context

```
Syntax
#include <krb5.h>

krb5_error_code gss_import_sec_context (
    OM_uint32 *                minor_status,
    gss_buffer_t               context_token,
    gss_ctx_id_t *             context_handle)

Service Program Name: QSYS/QKRBGSS

Default Public Authority: *USE

Threadsafe: Yes
```

The **gss\_import\_sec\_context()** routine accepts a security context token created by the **gss\_export\_sec\_context()** routine and creates a GSS-API security context. Since the security context contains message sequencing information, it is usually not feasible to create multiple security contexts from a single context token.

The **gss\_delete\_sec\_context()** routine should be called to delete the GSS-API security context when it is no longer needed. The security context token created by one implementation of GSS-API cannot be used with a different implementation of GSS-API.

## Parameters

### **minor\_status** (Output)

Status code returned from the security mechanism.

### **context\_token** (Input)

The security context token created by the **gss\_export\_sec\_context()** routine.

### **context\_handle** (Output)

The context handle returned for the security context created from the context token. The **gss\_delete\_sec\_context()** routine should be called to delete the security context when it is no longer needed.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_COMPLETE**

The routine completed successfully.

## GSS\_S\_FAILURE

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## GSS\_S\_DEFECTIVE\_TOKEN

The supplied credential token is not valid.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_indicate_mechs()`—Determine Available Security Mechanisms

```
Syntax
#include <gssapi.h>

OM_uint32 gss_indicate_mechs(
    OM_uint32 *   minor_status,
    gss_OID_set * mech_set);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_indicate_mechs()` function allows an application to determine which security mechanisms are available on the local system.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `mech_set` (Output)

The set of supported security mechanisms. The application should release the `gss_OID_set` returned for this parameter by calling the `gss_release_oid_set()` routine.

## Return Value

The return value is one of the following status codes:

## GSS\_S\_COMPLETE

The routine completed successfully.

## GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_init\_sec\_context()—Initiate Security Context

```
Syntax
#include <gssapi.h>

OM_uint32 gss_init_sec_context (
    OM_uint32 *   minor_status,
    gss_cred_id_t cred_handle,
    gss_ctx_id_t * context_handle,
    gss_name_t    target_name,
    gss_OID       mech_type,
    gss_flags_t   req_flags,
    OM_uint32     time_req,
    gss_channel_bindings_t input_chan_bindings,
    gss_buffer_t   input_token,
    gss_OID *      actual_mech_type,
    gss_buffer_t   output_token,
    gss_flags_t *  ret_flags,
    OM_uint32 *    time_rec);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_init_sec_context()` function initiates a security context for use by two communicating applications.

## Parameters

### **minor\_status (Output)**

A status code from the security mechanism.

### **cred\_handle (Input)**

The credential handle of the GSS credential to be used to initiate the security context. The specified credential must have been created using either **GSS\_C\_INITIATE** or **GSS\_C\_BOTH**. Specify **GSS\_C\_NO\_CREDENTIAL** to use the default credential obtained from the current login context.

### **context\_handle (Input/Output)**

The context handle for the context. The first time the context initiator calls the **gss\_init\_sec\_context()** routine, the context handle must be set to **GSS\_C\_NO\_CONTEXT**. For subsequent calls to continue setting up the context, the context handle must be the value returned by the previous call to the **gss\_init\_sec\_context()** routine.

### **target\_name (Input)**

The name of the context acceptor. This must be a Kerberos service name if delegation is requested for the Kerberos security mechanism. Otherwise, it can be any principal defined in the security registry, subject to registry policy rules.

### **mech\_type (Input)**

The desired security mechanism as follows:

*gss\_mech\_krb5\_old* Beta Kerberos V5 mechanism

*gss\_mech\_krb5* Kerberos V5 mechanism

*GSS\_C\_NO\_OID* Default mechanism. For the OS/400 implementation of GSS, this is the Kerberos V5 mechanism.

### **req\_flags (Input)**

A bit mask containing independent flags representing requested GSS services. GSS does not guarantee that a requested service will be available on all systems. The application should check the *ret\_flags* parameter to determine which of the requested services are actually provided for the context. The following symbolic definitions are provided to correspond to each flag. The symbolic names should be logically ORed to form the bit mask value.

<i>GSS_C_ANON_FLAG</i>	Request initiator anonymity. This flag is ignored in the current GSS implementation since Kerberos mechanism does not support initiator anonymity.
<i>GSS_C_DELEG_FLAG</i>	Request delegated credentials for use by the context acceptor.
<i>GSS_C_MUTUAL_FLAG</i>	Request mutual authentication to validate the identity of the context acceptor.
<i>GSS_C_REPLAY_FLAG</i>	Request message replay detection for signed or sealed messages.
<i>GSS_C_SEQUENCE_FLAG</i>	Request message sequence checking for signed or sealed messages.

### **time\_req (Input)**

The desired number of seconds the security context remains valid. Specify zero for the default lifetime of 2 hours. Specify **GSS\_C\_INDEFINITE** to request the maximum lifetime.

### **input\_chan\_bindings (Input)**

The bindings describing the communications channel that is used between the communicating applications. The channel bindings information is placed in the output token that is generated by the **gss\_init\_sec\_context()** routine and is validated by the **gss\_accept\_sec\_context()** routine. Specify **GSS\_C\_NO\_CHANNEL\_BINDINGS** if there are no channel bindings.

### **input\_token (Input)**

The token received from the context acceptor. **GSS\_C\_NO\_BUFFER** should be specified if this is the first call to the **gss\_init\_sec\_context()** routine.

**actual\_mech\_type (Output)**

The security mechanism that is used with the context. The `gss_OID` value returned for this parameter points to read-only storage and must not be released by the application.

**output\_token (Output)**

A token to be sent to the context acceptor. If no token is to be sent to the context acceptor, the `gss_init_sec_context()` routine sets the `output_token_length` field to zero. Otherwise, the `output_token_length` and `value` fields are set. The application should release the output token when it is no longer needed by calling the `gss_release_buffer()` routine.

**ret\_flags (Output)**

A bit mask containing independent flags indicating which GSS services are available for the context. The following symbolic definitions are provided to test the individual flags and should be logically ANDed with the value of `ret_flags` to test whether the context supports the service options:

<code>GSS_C_ANON_FLAG</code>	The initiator identity will not be provided to the context acceptor.
<code>GSS_C_CONF_FLAG</code>	Message confidentiality services are available.
<code>GSS_C_DELEG_FLAG</code>	Delegated credentials will be available to the context acceptor.
<code>GSS_C_INTEG_FLAG</code>	Message integrity services are available.
<code>GSS_C_MUTUAL_FLAG</code>	Mutual authentication will be performed. The <code>gss_accept_sec_context()</code> routine will generate an output token which the context acceptor must return to the context initiator to complete the security context setup.
<code>GSS_C_PROT_READY_FLAG</code>	Protection services, as specified by the states of the <code>GSS_C_CONF_FLAG</code> and <code>GSS_C_INTEG_FLAG</code> , are available for use if the accompanying major status return value is <code>GSS_S_COMPLETE</code> or <code>GSS_S_CONTINUE_NEEDED</code> . Otherwise, protection services are available for use only if the accompanying major status return value is <code>GSS_S_COMPLETE</code> .
<code>GSS_C_REPLAY_FLAG</code>	Message replay detection will be performed.
<code>GSS_C_SEQUENCE_FLAG</code>	Message sequence checking will be performed.

**time\_rec (Output)**

The number of seconds for which the context will remain valid. If the mechanism does not support context expiration, the return value will be `GSS_C_INDEFINITE`. Specify `NULL` for this parameter if the context expiration time is not required.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_BAD\_BINDINGS**

The channel bindings are not valid.

**GSS\_S\_BAD\_MECH**

The request security mechanism is not supported.

**GSS\_S\_BAD\_NAME**

The `target_name` parameter is not valid.

**GSS\_S\_BAD\_SIG**

The input token contains an incorrect integrity check value.

### GSS\_S\_CONTINUE\_NEEDED

To complete the context, the `gss_init_sec_context()` routine must be called again with a token created by the `gss_accept_sec_context()` routine.

### GSS\_S\_CREDENTIALS\_EXPIRED

The supplied credentials are no longer valid.

### GSS\_S\_DEFECTIVE\_CREDENTIAL

Consistency checks performed on the credential failed.

### GSS\_S\_DEFECTIVE\_TOKEN

Consistency checks performed on the input token failed.

### GSS\_S\_DUPLICATE\_TOKEN

The token is a duplicate of a token that has already been processed.

### GSS\_S\_NO\_CONTEXT

The context handle provided by the caller does not refer to a valid security context.

### GSS\_S\_NO\_CRED

The supplied credential handle does not refer to a valid credential, the supplied credential is not valid for context initiation, or there are no default credentials available.

### GSS\_S\_OLD\_TOKEN

The token is too old to be checked for duplication against previous tokens which have already been processed.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R
Each directory in the path name preceding the credential cache file	*X
Credential cache file	*RW

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. The `gss_init_sec_context()` routine is the first step in the establishment of a security context between the context initiator and the context acceptor. To ensure the portability of the application, use the default credential by specifying `GSS_C_NO_CREDENTIAL` for the `cred_handle` parameter.

The first time the application calls the `gss_init_sec_context()` routine, the `input_token` parameter should either be specified as `GSS_C_NO_BUFFER` or the buffer length field should be set to zero. If no token needs to be sent to the context acceptor, the `gss_init_sec_context()` routine sets the `output_token length` field to zero.

To finish establishing the context, the calling application can require one or more tokens from the context acceptor. If the application requires reply tokens, the `gss_init_sec_context()` routine returns `GSS_S_CONTINUE_NEEDED` in the supplementary information portion of the major status value. The application must call the `gss_init_sec_context()` routine again when it receives the reply token from the context acceptor and pass the token using the `input_token` parameter. When calling the `gss_init_sec_context()` routine to continue processing a context, the same request values must be used as for the initial call.

2. The availability of confidentiality services is dependent on the underlying security mechanism and the features that have been installed on the system. The `GSS_C_CONF_FLAG` is returned only if confidentiality services are available on the local system. This does not guarantee, however, that confidentiality services are also available on the remote system. If confidentiality services are available on the local system but not on the remote system, an error is returned by the `gss_unwrap()` routine on the remote system if an encrypted message is received (that is, confidentiality was requested on the call to the `gss_wrap()` routine on the local system).
3. Whenever the routine returns a major status that includes the value `GSS_S_CONTINUE_NEEDED`, the context is not fully established and the following restrictions apply to the output parameters:
  - The value returned by the `time_rec` parameter is undefined.
  - Unless the accompanying `ret_flags` parameter contains the bit `GSS_C_PROT_READY_FLAG`, indicating that per-message services may be applied in advance of a successful completion status, the value returned by the `actual_mech_type` parameter is undefined until the routine returns a major status value of `GSS_S_COMPLETE`.
  - The values of the `GSS_C_DELEG_FLAG`, `GSS_C_MUTUAL_FLAG`, `GSS_C_REPLAY_FLAG`, `GSS_C_SEQUENCE_FLAG`, `GSS_C_CONF_FLAG`, `GSS_C_INTEG_FLAG`, and `GSS_C_ANON_FLAG` bits returned by the `ret_flags` parameter contain the values that would be returned if the context establishment were to succeed. In particular, if the application has requested a service such as delegation or anonymous authentication through the `req_flags` parameter and such a service is unavailable from the underlying mechanism, `gss_init_sec_context()` generates a token that does not provide the service and indicates through the `ret_flags` parameter that the service is not supported. The application may choose to abort the context establishment by calling `gss_delete_sec_context()` or it may choose to transmit the token and continue context establishment.
  - The value of the `GSS_C_PROT_READY_FLAG` bit returned by the `ret_flags` parameter indicates the actual state at the time `gss_accept_init_context()` returns, whether or not the context is fully established.
4. Kerberos mechanism
  - To use delegation, the target principal name must be a service name. A service name is created by calling the `gss_import_name()` routine with the name type specified as `gss_nt_service_name` (object identifier {1 2 840 113554 1 2 1 4}). The service name is specified as "name@host" and results in a Kerberos principal of "name/host@host-realm". The local host name is used if no host is specified. If a host name alias is specified, the primary host name returned by the domain name service is used when constructing the principal name. The target principal name is not required to be a service name if the ticket-granting ticket does not contain a client address list. You can obtain a ticket-granting ticket without a client address list by specifying the `-a` option on the `kinit` command. Otherwise, the service name must correctly identify the host on which the target service is running.
  - The requested context lifetime is used to specify the end time when obtaining a Kerberos service ticket to the target application. The actual context lifetime is then set to the lifetime of the ticket, which may be less than the requested lifetime as determined by the registry policy.



- If delegation is requested, the ticket-granting-ticket contained in the login context must allow forwardable tickets. If the ticket-granting ticket is not forwardable, the `gss_init_sec_context()` request will be successful but the `GSS_C_DELEG_FLAG` will not be set in the returned flags. In addition, the service ticket obtained for the target principal must allow delegation. If the target server is not enabled for delegation, the `gss_init_sec_context()` request will be successful but the `GSS_C_DELEG_FLAG` will not be set in the returned flags. You can use the `klist` command with the `-f` option to display the ticket flags. The ticket-granting ticket must have the `F` flag set and the service ticket must have the `o` flag set.

API introduced: V5R1

Top | Security APIs  
UNIX-Type APIs | APIs by category

---

## `gss_inquire_context()`—Get Information About Security Context

```
Syntax
#include <gssapi.h>

OM_uint32 gss_inquire_context (
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    gss_name_t *  source_name,
    gss_name_t *  target_name,
    OM_uint32 *  lifetime,
    gss_OID *     mech_type,
    gss_flags_t * ret_flags,
    int *         local,
    int *         open);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_inquire_context()` function returns information about a security context to the calling application.

### Parameters

**minor\_status (Output)**

A status code from the security mechanism.

**context\_handle (Input)**

The handle for the security context.

**source\_name (Output)**

The principal name associated with the context initiator. Specify `NULL` for this parameter if the principal name is not required.

**target\_name (Output)**

The principal name associated with the context acceptor. Specify `NULL` for this parameter if the principal name is not required.

### lifetime (Output)

The mechanism used to create the security context. The `gss_OID` value returned for this parameter points to read-only storage and must not be released by the application. Specify **NULL** for this parameter if the mechanism type is not required.

### mech\_type (Output)

A bit mask of seconds for which the context remains valid. Specify **NULL** for this parameter if the context lifetime is not required. The returned value is **GSS\_C\_INDEFINITE** if the security mechanism does not support context expiration.

### ret\_flags (Output)

The mechanism used to create the security context. The `gss_OID` value returned for this parameter points to read-only storage and must not be released by the application. Specify **NULL** for this parameter if the mechanism type is not required.

**GSS\_C\_ANON\_FLAG**

The initiator identity will not be provided to the context acceptor.

**GSS\_C\_CONF\_FLAG**

Message confidentiality services are available.

**GSS\_C\_DELEG\_FLAG**

Delegated credentials will be available to the context acceptor.

**GSS\_C\_INTEG\_FLAG**

Message integrity services are available.

**GSS\_C\_MUTUAL\_FLAG**

Mutual authentication will be performed. The `gss_accept_sec_context()` routine will generate an output token which the context acceptor must return to the context initiator to complete the security context setup.

**GSS\_C\_PROT\_READY\_FLAG**

Protection services, as specified by the states of the **GSS\_C\_CONF\_FLAG** and **GSS\_C\_INTEG\_FLAG**, are available for use even if the context is not fully established. Otherwise, protection services are available for use only if value returned by the `open` parameter is **TRUE**.

**GSS\_C\_REPLAY\_FLAG**

Message replay detection will be performed.

**GSS\_C\_SEQUENCE\_FLAG**

Message sequence checking will be performed.

### local (Output)

**TRUE** if the context was initiated locally and **FALSE** otherwise. Specify **NULL** for this parameter if the local indication is not required.

### open (Output)

**TRUE** if context establishment has been completed and **FALSE** otherwise. Specify **NULL** for this parameter if the open indication is not required.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CONTEXT\_EXPIRED**

The referenced context has expired.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CONTEXT**

The context handle provided by the caller does not refer to a valid security context.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_inquire\_cred()—Get Information About GSS Credential

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_inquire_cred (     OM_uint32 *   minor_status,     gss_cred_id_t cred_handle,     gss_name_t *  name,     OM_uint32 *  lifetime,     gss_cred_usage_t * cred_usage,     gss_OID_set * mechanisms);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The `gss_inquire_cred()` function returns information about a GSS credential to the calling application. If `GSS_C_NO_CREDENTIAL` is specified for the `cred_handle` parameter, the default security mechanism is used to process the request.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `cred_handle` (Input)

The handle for the GSS credential. Specify `GSS_C_NO_CREDENTIAL` to get information about the default credential for the default security mechanism.

**name (Output)**

The principal name associated with the credential. Specify **NULL** for this parameter if the principal name is not required.

**lifetime (Output)**

The number of seconds for which the credential remains valid. The returned value is zero if the credential has expired. Specify **NULL** for this parameter if the credential lifetime is not required.

**cred\_usage (Output)**

One of the following values describing how the application can use the credential. Specify **NULL** for this parameter if the credential usage is not required.

*GSS\_C\_INITIATE* The application may initiate a security context.

*GSS\_C\_ACCEPT* The application may accept a security context.

*GSS\_C\_BOTH* The application may both initiate and accept security contexts.

**mechanisms (Output)**

The set of security mechanisms supported by the credential. Specify **NULL** for this parameter if the mechanism set is not required. The *gss\_OID\_set* returned for this parameter should be released when it is no longer needed by calling the **gss\_release\_oid\_set()** routine.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CREDENTIALS\_EXPIRED**

The credentials have expired. Credential information is still returned for an expired credential, but the *lifetime* value is returned as zero.

**GSS\_S\_DEFECTIVE\_CREDENTIAL**

The credentials are not valid.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CRED**

The *cred\_handle* parameter does not refer to a valid credential or there are no default credentials available.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R
Each directory in the path name preceding the credential cache file	*X
Credential cache file	*RW

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_inquire\_cred\_by\_mech()**—Get Information About GSS Credential for Single Security Mechanism

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_inquire_cred_by_mech (     OM_uint32 *    minor_status,     gss_cred_id_t  cred_handle,     gss_OID        mech_type,     gss_name_t *   name,     OM_uint32 *    init_lifetime,     OM_uint32 *    accept_lifetime,     gss_cred_usage_t * cred_usage);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The **gss\_inquire\_cred\_by\_mech()** function returns information about a GSS credential for a single security mechanism. The information is obtained using the specified security mechanism.

### Parameters

#### **minor\_status** (Output)

A status code from the security mechanism.

#### **cred\_handle** (Input)

The handle for the GSS credential. Specify **GSS\_C\_NO\_CREDENTIAL** to get information about the default credential for the default security mechanism.

#### **mech\_type** (Input)

The mechanism to be used to obtain the returned information as follows:

*gss\_mech\_krb5\_old* Beta Kerberos V5 mechanism  
*gss\_mech\_krb5* Kerberos V5 mechanism

#### **name** (Output)

The principal name associated with the credential. Specify **NULL** for this parameter if the principal name is not required.

**init\_lifetime (Output)**

The number of seconds for which the credential remains valid for initiating contexts. Specify **NULL** for this parameter if the credential lifetime is not required.

**accept\_lifetime (Output)**

The number of seconds for which the credential remains valid for accepting contexts. Specify **NULL** for this parameter if the credential lifetime is not required.

**cred\_usage (Output)**

One of the following values describing how the application can use the credential. Specify **NULL** for this parameter if the credential usage is not required.

*GSS\_C\_ACCEPT* The application may accept a security context.

*GSS\_C\_BOTH* The application may both initiate and accept security contexts.

*GSS\_C\_INITIATE* The application may initiate a security context.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_BAD\_MECH**

The requested mechanism is not supported.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CREDENTIALS\_EXPIRED**

The credentials have expired. Credential information will still be returned for an expired credential, but the *lifetime* value will be returned as zero.

**GSS\_S\_DEFECTIVE\_CREDENTIAL**

The credentials are not valid.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CRED**

The *cred\_handle* parameter does not refer to a valid credential or there are no default credentials available.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

---

## **gss\_inquire\_mechs\_for\_name()**—Determine Mechanisms to Process Name

```
Syntax
#include <gssapi.h>

OM_uint32 gss_inquire_mechs_for_name (
    OM_uint32 *   minor_status,
    gss_name_t    input_name,
    gss_OID_set * mech_types);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_inquire_mechs_for_name()` function returns the mechanisms with which a name may be processed.

### **Parameters**

#### **minor\_status (Output)**

A status code from the security mechanism.

#### **input\_name (Input)**

The name to be queried.

#### **mech\_types (Output)**

The mechanisms that can be used with the specified name. The `gss_OID_set` returned for this parameter should be released by calling the `gss_release_oid_set()` routine when it is no longer needed.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_BAD\_NAME**

The supplied name is not valid.

#### **GSS\_S\_BAD\_NAME\_TYPE**

The name type is not supported.

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_inquire\_names\_for\_mech()—Get Name Types Supported by Security Mechanism

```
Syntax
#include <gssapi.h>

OM_uint32 gss_inquire_names_for_mech (
    OM_uint32 *   minor_status,
    gss_OID      mech_type,
    gss_OID_set * mech_names);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_inquire_names_for_mech()` function returns the name types supported by a security mechanism.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `mech_type` (Input)

The mechanism to be queried as follows:

`gss_mech_krb5_old` Beta Kerberos V5 mechanism  
`gss_mech_krb5` Kerberos V5 mechanism



### **mech\_names (Output)**

The name types supported by the specified mechanism. The `gss_OID_set` returned for this parameter should be released by calling the `gss_release_oid_set()` routine when it is no longer needed.

## **Return Value**

The return value is one of the following status codes:

### **GSS\_S\_BAD\_MECH**

The requested mechanism is not supported.

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

## **Authorities**

<b>Object Referred to</b>	<b>Data Authority Required</b>
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## **Error Messages**

<b>Message ID</b>	<b>Error Message Text</b>
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_krb5\_get\_ccache()—Get Kerberos Protocol Credentials Cache Associated with Specified GSS Credential**

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_krb5_get_ccache (     OM_uint32 *   minor_status,     gss_cred_id_t cred_handle,     krb5_ccache * ccache);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
--

The `gss_krb5_get_ccache()` function returns the handle for the Kerberos credentials cache associated with a GSS credential. The application must not close or destroy this credentials cache. The returned handle is no longer valid once the GSS credential has been released.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `cred_handle` (Input)

The handle for the GSS credential.

### `ccache` (Output)

The handle for the credentials cache. A NULL value is returned if there is no credentials cache associated with the GSS credential.

## Return Value

The return value is one of the following status codes:

### `GSS_S_COMPLETE`

The routine completed successfully.

### `GSS_S_FAILURE`

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

### `GSS_S_NO_CRED`

The credential handle does not refer to a valid GSS credential.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_krb5\_acquire\_cred\_cache()**—Acquire GSS Credential from a Kerberos Protocol Credentials Cache

```
Syntax
#include <krb5.h>

krb5_error_code gss_krb5_acquire_cred_cache (
    OM_uint32 *                minor_status,
    krb5_ccache                ccache,
    OM_uint32                  time_req,
    gss_cred_usage_t          cred_usage,
    gss_cred_id_t *           output_cred_handle,
    OM_uint32 *                time_rec)

Service Program Name: QSYS/QKRBGSS

Default Public Authority: *USE

Threadsafe: Yes
```

The **gss\_krb5\_acquire\_cred\_ccache()** routine acquires a GSS-API credential using a Kerberos credentials cache. This function allows an application to obtain a GSS-API credential for use with the Kerberos mechanism. The application can then use the credential with the **gss\_init\_sec\_context()** and **gss\_accept\_sec\_context()** routines. The Kerberos credentials cache must not be closed until the GSS-API credential is no longer needed and has been deleted.

If GSS\_C\_INITIATE or GSS\_C\_BOTH is specified for the credential usage, the application must have a valid ticket in the credentials cache and the ticket must not expire for at least 10 minutes. The **gss\_krb5\_acquire\_cred\_ccache()** routine will use the first valid ticket-granting ticket (or the first valid service ticket if there is no TGT) to create the GSS-API credential.

If GSS\_C\_ACCEPT or GSS\_C\_BOTH is specified for the credential usage, the principal associated with the GSS-API credential must be defined in a key table. The KRB5\_KTNAME environment variable is used to identify the key table used by the Kerberos security mechanism.

### **Parameters**

#### **minor\_status (Output)**

Status code returned from the security mechanism.

#### **ccache (Input)**

The Kerberos credentials cache to be used for the credential. The principal name for the GSS-API credential is obtained from the credentials cache. The credentials cache must contain a valid ticket-granting ticket for this principal if a GSS\_C\_INITIATE or GSS\_C\_BOTH credential is Requested.

#### **time\_req (Input)**

The number of seconds that the credential remains valid. Specify GSS\_C\_INDEFINITE to request the maximum credential lifetime. Specify zero for the default lifetime of 2 hours. The actual credential lifetime will be limited by the lifetime of the underlying ticket-granting ticket for GSS\_C\_INITIATE and GSS\_C\_BOTH credentials.

#### **cred\_usage (Input)**

The desired credential usage as follows:

- GSS\_C\_INITIATE if the credential can be used only to initiate security contexts.
- GSS\_C\_ACCEPT if the credential can be used only to accept security contexts.
- GSS\_C\_BOTH if the credential can be used to both initiate and accept security contexts.

**output\_cred\_handle (Output)**

The handle returned for the GSS-API credential.

**time\_rec (Output)**

The number of seconds returned for which the credential will remain valid. If the time remaining is not required, specify NULL for this parameter.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_BAD\_MECH**

None of the requested mechanisms are supported by the local system.

**GSS\_S\_NO\_CRED**

The Kerberos credentials cache does not contain a valid ticket-granting ticket.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_krb5\_ccache\_name()—Set Default Kerberos Protocol Credentials Cache Name**

```
Syntax
#include <krb5.h>

krb5_error_code gss_krb5_ccache_name (
    OM_uint32 *                minor_status,
    char *                    new_name,
    char **                   old_name)
```

Service Program Name: QSYS/QKRBGSS

Default Public Authority: \*USE

Threadsafe: Yes

The `gss_krb5_ccache_name()` routine sets the default credentials cache name for use by the Kerberos mechanism. The default credentials cache is used by `gss_acquire_cred()` to create a GSS-API credential. It is also used by `gss_init_sec_context()` when `GSS_C_NO_CREDENTIAL` is specified for the GSS-API credential used to establish the security context.

### **Parameters**

#### **minor\_status (Output)**

Status code returned from the security mechanism.

#### **new\_name (Input)**

The new name for the default GSS-API Kerberos credentials cache.

#### **old\_name (Output)**

The name returned of the current default credentials cache or NULL if the default credentials cache has not been set. Specify NULL for this parameter if you do not need the current credentials cache name. The returned name should be released by calling `krb5_free_string()` when it is no longer needed.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons which are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **Authorities**

None.

### **Error Messages**

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

Message ID	Error Message Text
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_krb5\_copy\_ccache()—Copy Tickets From Associated GSS Credentials to Kerberos Protocol Credentials Cache**

```

Syntax
#include <krb5.h>

krb5_error_code gss_krb5_copy_ccache (
    OM_uint32 *          minor_status,
    gss_cred_id_t        cred_handle,
    krb5_ccache          ccache)

```

Service Program Name: QSYS/QKRBGSS

Default Public Authority: \*USE

Threadsafe: Yes

The **gss\_krb5\_copy\_ccache()** routine will copy the tickets from the Kerberos credentials cache associated with a GSS-API credential to a credentials cache provided by the caller. The supplied Kerberos credentials cache must have been initialized by **krb5\_cc\_initialize()** before calling **gss\_krb5\_copy\_ccache()**. The GSS-API credential must have been created by specifying **GSS\_C\_INITIATE** or **GSS\_C\_BOTH**.

### **Parameters**

**minor\_status (Output)**

Status code returned from the security mechanism.

**cred\_handle (Input)**

The GSS-API credential handle. This must be a **GSS\_C\_INITIATE** or **GSS\_C\_BOTH** credential.

**ccache (Input)**

The Kerberos credentials cache.

### **Return Value**

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons which are not defined at the GSS level. The **minor\_status** return parameter contains a mechanism-dependent error code describing the reason for the failure.

## GSS\_S\_NO\_CRED

The credential handle does not refer to a valid GSS-API credential.

## Authorities

None.

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.
CPFA081 E	Unable to set return value or error code.

API introduced: V5R2

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_krb5\_get\_tkt\_flags()—Get Kerberos Protocol Ticket Flags

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_krb5_get_tkt_flags (     OM_uint32 *   minor_status,     gss_ctx_id_t  context_handle,     krb5_flags *  tkt_flags);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The `gss_krb5_get_tkt_flags()` function returns the Kerberos ticket flags from the Kerberos ticket associated with the security context. Refer to the Kerberos protocol-specific API documentation for a description of the various flags.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `context_handle` (Input)

The handle for the GSS security context.

### `tkt_flags` (Output)

The ticket flags from the Kerberos ticket associated with the security context.

## Return Value

The return value is one of the following status codes:

## GSS\_S\_COMPLETE

The routine completed successfully.

## GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## GSS\_S\_NO\_CONTEXT

The context handle does not refer to a valid security context.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_oid\_to\_str()—Convert OID Object to String Representation of Object

```
Syntax
#include <gssapi.h>

OM_uint32 gss_oid_to_str(
    OM_uint32 *   minor_status,
    gss_OID      input_oid,
    gss_buffer_t  output_string);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The **gss\_oid\_to\_str()** function converts a `gss_oid` object to a string representation of the object identifier. The string representation consists of a series of blank-separated numbers enclosed in braces. The **gss\_str\_to\_oid()** routine can be used to convert the string representation back to a `gss_oid` object.



Not every coded character set identifier (CCSID) contains the left and right brace characters; however, alternative CCSID values often are available. For example, instead of using Greece 423, run the job with a default CCSID of 875.

## Parameters

### **minor\_status (Output)**

A status code from the security mechanism.

### **input\_oid (Input)**

The gss\_OID to be converted.

### **output\_string (Output)**

The string representation of the object identifier. The gss\_buffer\_t returned for this parameter should be released by calling the **gss\_release\_buffer()** routine when it is no longer needed.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_process\_context\_token()**—Process Received Context Token

```
Syntax
#include <gssapi.h>

OM_uint32 gss_process_context_token(
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    gss_buffer_t  input_token);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_process\_context\_token()** function processes a context token received from the partner application.

### **Parameters**

#### **minor\_status (Output)**

A status code from the security mechanism.

#### **context\_handle (Input)**

The context that should be used when processing the token.

#### **input\_token (Input)**

The token received from the partner application.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_BAD\_SIG**

The token signature was not correct.

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_DEFECTIVE\_TOKEN**

Consistency checks performed on the input token failed.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

#### **GSS\_S\_NO\_CONTEXT**

The context handle does not refer to a valid security context.

### **Authorities**

<b>Object Referred to</b>	<b>Data Authority Required</b>
Each directory in the path name preceding the configuration file	*X

Object Referred to	Data Authority Required
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. Tokens are usually associated with either the context establishment or with message security services. If the tokens are associated with the context establishment, they are processed by the `gss_init_sec_context()` and `gss_accept_sec_context()` routines. If the tokens are associated with message security services, they are processed by the `gss_verify_mic()` and `gss_unwrap()` routines. Tokens generated by the `gss_delete_sec_context()` routine, however, are processed by the `gss_process_context_token()` routine.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_release_buffer()`—Release Storage Associated with Buffer

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_release_buffer(     OM_uint32 * minor_status,     gss_buffer_t buffer);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
--

The `gss_release_buffer()` function releases storage associated with a `gss_buffer_t` buffer. The `gss_buffer_desc` structure itself is not released.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `buffer` (Input/Output)

The buffer to be released. Upon successful completion, the *length* and *value* fields are set to zero.

## Return Value

The return value is one of the following status codes:

### GSS\_S\_COMPLETE

The routine completed successfully.

### GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_release\_cred()—Release Storage Associated with GSS Credential

Syntax
<pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_release_cred(     OM_uint32 *   minor_status,     gss_cred_id_t * cred_handle);</pre>
Service Program Name: QSYS/QKRBGSS
Default public authority: *USE
Threadsafe: Yes

The `gss_release_cred()` function releases the local data structures associated with a GSS credential. If `gss_c_no_credential` is specified for the `cred_handle` parameter, no credential is released and `gss_s_complete` is returned for the major status return value.

## Parameters

### minor\_status (Output)

A status code from the security mechanism.

### cred\_handle (Input/Output)

The credential to be released. Upon successful completion, the *cred\_handle* value is set to **GSS\_C\_NO\_CREDENTIAL**. If the *cred\_handle* value is **GSS\_C\_NO\_CREDENTIAL**, the major status return value is **GSS\_S\_COMPLETE** and nothing is released.

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_DEFECTIVE\_CREDENTIAL**

Consistency checks performed on the credential structure failed.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **GSS\_S\_NO\_CRED**

The *cred\_handle* parameter does not refer to a valid credential.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_release\_name()—Release Storage Associated with GSS Internal Name

```
Syntax
#include <gssapi.h>

OM_uint32 gss_release_name(
    OM_uint32 *   minor_status,
    gss_name_t *  name);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_release_name()` function releases storage associated with a `gss_name_t` internal name.

### Parameters

#### **minor\_status** (Output)

A status code from the security mechanism.

#### **name** (Input/Output)

The name to be released. Upon successful completion, the *name* value is set to `GSS_C_NO_NAME`.

### Return Value

The return value is one of the following status codes:

#### **GSS\_S\_BAD\_NAME**

The specified name is not valid.

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

### Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

Top | Security APIs  
UNIX-Type APIs | APIs by category

---

## **gss\_release\_oid()—Release Storage Associated with OID Object**

Syntax
<pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_release_oid(     OM_uint32 *  minor_status,     gss_OID *    oid);</pre>
Service Program Name: QSYS/QKRBGSS
Default public authority: *USE
Threadsafe: Yes

The **gss\_release\_oid()** function releases storage associated with a **gss\_oid** object. The **gss\_release\_oid()** routine must not be called to release a read-only oid that was returned by one of the GSS routines.

### **Parameters**

**minor\_status (Output)**

A status code from the security mechanism.

**oid (Input/Output)**

The **gss\_OID** to be released. Upon successful completion, the *oid* value is set to **GSS\_C\_NO\_OID**.

### **Return Value**

The return value is one of the following status codes:

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **Authorities**

<b>Object Referred to</b>	<b>Data Authority Required</b>
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

**Message ID**      **Error Message Text**  
CPE3418 E      Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_release\_oid\_set()—Release Storage Associated with a Set of OID Objects

```
Syntax
#include <gssapi.h>

OM_uint32 gss_release_oid_set(
    OM_uint32 *   minor_status,
    gss_OID_set *   oid_set);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_release_oid_set()` function releases storage associated with a `gss_oid_set` object.

### Parameters

#### **minor\_status** (Output)

A status code from the security mechanism.

#### **oid** (Input/Output)

The `gss_OID_set` to be released. Upon successful completion, the `oid_set` value is set to `GSS_C_NO_OID_SET`.

### Return Value

The return value is one of the following status codes:

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

### Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X



Object Referred to	Data Authority Required
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

## **gss\_str\_to\_oid()**—Convert String Representation of an Object Identifier to an Internal OID Object

<p>Syntax</p> <pre>#include &lt;gssapi.h&gt;  OM_uint32 gss_str_to_oid(     OM_uint32 *   minor_status,     gss_buffer_t  input_string,     gss_OID *     output_oid);</pre> <p>Service Program Name: QSYS/QKRBGSS</p> <p>Default public authority: *USE</p> <p>Threadsafe: Yes</p>
---

The `gss_str_to_oid()` function converts the string representation of an object identifier to a `gss_OID` object.

### Parameters

#### **minor\_status** (Output)

A status code from the security mechanism.

#### **input\_string** (Input)

The string to be converted.

#### **output\_oid** (Output)

The object identifier. The `gss_OID` returned for this parameter should be released by calling the `gss_release_oid()` routine when it is no longer needed.

### Return Value

The return value is one of the following status codes:

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

## GSS\_S\_FAILURE

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. A string representation is a series of blank-separated or period-separated numbers enclosed in braces. For example, the Kerberos V5 security mechanism object identifier is represented as {1 2 840 113554 1 2 2}.  
Not every coded character set identifier (CCSID) contains the left and right brace characters; however, alternative CCSID values often are available. For example, instead of using Greece 423, run the job with a default CCSID of 875.
2. While the blank-separated form should be used for portability, the `gss_str_to_oid()` routine also accepts the period-separated form for compatibility with other applications. The `gss_oid_to_str()` routine, however, always generates the blank-separated form.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

## **gss\_test\_oid\_set\_member()—Determine if Specified OID is Contained in a Specified OID Set**

```
Syntax
#include <gssapi.h>

OM_uint32 gss_test_oid_set_member(
    OM_uint32 *   minor_status,
    gss_OID      member_oid,
    gss_OID_set   oid_set,
    int *        is_present);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_test_oid_set_member()` function checks an oid set to see if a specified oid is a member of the set.

### **Parameters**

#### **minor\_status (Output)**

A status code from the security mechanism.

#### **member\_oid (Input)**

The OID to search for in the OID set.

#### **oid\_set (Input)**

The OID set to check.

#### **is\_present (Output)**

1 if the OID is a member of the OID set. Otherwise, it is set to zero.

### **Return Value**

The return value is one of the following status codes:

#### **GSS\_S\_COMPLETE**

The routine completed successfully.

#### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The `minor_status` return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **Authorities**

<b>Object Referred to</b>	<b>Data Authority Required</b>
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. The `gss_create_empty_oid_set()` routine can be used to create an empty oid set. The `gss_add_oid_set_member()` routine can be used to add an oid to an existing oid set.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## `gss_unwrap()`—Unwrap a Message

```
Syntax
#include <gssapi.h>

OM_uint32 gss_unwrap (
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    gss_buffer_t  input_message,
    gss_buffer_t  output_message,
    int *         conf_state,
    gss_qop_t *   qop_state);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The `gss_unwrap()` function unwraps a message sealed by the `gss_wrap()` routine and verifies the embedded signature. The `conf_state` return parameter indicates whether or not the message has been encrypted.

## Parameters

### `minor_status` (Output)

A status code from the security mechanism.

### `context_handle` (Input)

The context in which the message arrived.

### `input_message` (Input)

The sealed message token generated by the `gss_wrap()` routine.

### `output_message` (Output)

The unsealed message.

### `conf_state` (Output)

The level of confidentiality that was applied to the message. Specify **NULL** for this parameter if the confidentiality state is not needed. The return value is set as follows:

*TRUE* Both confidentiality and integrity services were applied.  
*FALSE* Only integrity services were applied.

### **gop\_state (Output)**

The quality of protection that was applied to the message. Specify **NULL** for this parameter if the quality of protection is not needed.

The Kerberos security mechanism supports three quality of protection levels as follows (in decreasing order of speed):

<i>GSS_KRB5_INTEG_C_QOP_MD5</i>	Truncated MD5
<i>GSS_KRB5_INTEG_C_QOP_DES_MD5</i>	DES_MAC of an MD5 hash
<i>GSS_KRB5_INTEG_C_QOP_DES_MAC</i>	Normal DES_MAC algorithm

## **Return Value**

The return value is one of the following status codes:

### **GSS\_S\_BAD\_SIG**

The input token contains an incorrect signature.

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_CONTEXT\_EXPIRED**

The context identifier provided by the caller has expired.

### **GSS\_S\_CREDENTIALS\_EXPIRED**

Credentials are no longer valid.

### **GSS\_S\_DEFECTIVE\_TOKEN**

Consistency checks performed on the input token failed.

### **GSS\_S\_DUPLICATE\_TOKEN**

The token is a duplicate of a token that has already been processed.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **GSS\_S\_GAP\_TOKEN**

One or more predecessor tokens have not been processed.

### **GSS\_S\_NO\_CONTEXT**

The context identifier provided by the caller does not refer to a valid security context.

### **GSS\_S\_OLD\_TOKEN**

The token is too old to be checked for duplication against previous tokens. This is a fatal error during context establishment.

### **GSS\_S\_UNSEQ\_TOKEN**

A later token has already been processed.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

**Message ID**      **Error Message Text**  
CPE3418 E      Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_verify\_mic()—Verify that Cryptographic Signature is Correct

```
Syntax
#include <gssapi.h>

OM_uint32 gss_verify_mic (
    OM_uint32 * minor_status,
    gss_ctx_id_t context_handle,
    gss_buffer_t input_message,
    gss_buffer_t input_token,
    gss_qop_t * qop_state);

Service Program Name: QSYS/QKRBGSS

Default public authority: *USE

Threadsafe: Yes
```

The `gss_verify_mic()` function verifies that the cryptographic signature for a message is correct. This ensures that the message has not been modified since the signature was generated.

## Parameters

### **minor\_status** (Output)

A status code from the security mechanism.

### **context\_handle** (Input)

The context in which the message arrived.

### **input\_message** (Input)

The message to be verified.

### **input\_token** (Input)

The signature token generated by the `gss_get_mic()` routine.

### gop\_state (Output)

The quality of protection that was applied to the message. Specify **NULL** for this parameter if the quality of protection is not needed.

The Kerberos security mechanism supports three quality of protection levels as follows:

<i>GSS_KRB5_INTEG_C_QOP_MD5</i>	Truncated MD5
<i>GSS_KRB5_INTEG_C_QOP_DES_MD5</i>	DES_MAC of an MD5 hash
<i>GSS_KRB5_INTEG_C_QOP_DES_MAC</i>	Normal DES_MAC algorithm

## Return Value

The return value is one of the following status codes:

### **GSS\_S\_BAD\_SIG**

The input token contains an incorrect signature.

### **GSS\_S\_COMPLETE**

The routine completed successfully.

### **GSS\_S\_CONTEXT\_EXPIRED**

The context identifier provided by the caller has expired.

### **GSS\_S\_CREDENTIALS\_EXPIRED**

The credentials associated with the referenced context have expired.

### **GSS\_S\_DEFECTIVE\_CREDENTIAL**

The credential is defective.

### **GSS\_S\_DEFECTIVE\_TOKEN**

Consistency checks performed on the input token failed.

### **GSS\_S\_DUPLICATE\_TOKEN**

The token is a duplicate of a token that has already been processed.

### **GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

### **GSS\_S\_GAP\_TOKEN**

One or more predecessor tokens have not been processed.

### **GSS\_S\_NO\_CONTEXT**

The context identifier provided by the caller does not refer to a valid security context.

### **GSS\_S\_OLD\_TOKEN**

The token is too old to be checked for duplication against previous tokens. This is a fatal error during context establishment.

### **GSS\_S\_UNSEQ\_TOKEN**

A later token has already been processed.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## gss\_wrap()—Cryptographically Sign and Optionally Encrypt Message

```
Syntax
#include <gssapi.h>

OM_uint32 gss_wrap (
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    int           conf_req,
    gss_qop_t     qop_req,
    gss_buffer_t  input_message,
    int *         conf_state,
    gss_buffer_t  output_message);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_wrap()** function cryptographically signs and optionally encrypts a message. The token returned in the *output\_message* parameter contains both the signature and the message. This token is then sent to the partner application that calls the **gss\_unwrap()** routine to extract the original message and verify its authenticity.

### Parameters

#### **minor\_status** (Output)

A status code from the security mechanism.

#### **context\_handle** (Input)

The context handle to be associated with the message when it is sent to the partner application.

#### **conf\_req** (Input)

The requested level of confidentiality and integrity services as follows:

*TRUE*

Both confidentiality and integrity services are requested.

*FALSE*

Only integrity services are requested.

#### **qop\_req** (Input)

The requested quality of protection for the message. Specify **GSS\_C\_QOP\_DEFAULT** to use the default quality of protection as defined by the selected security mechanism.

The Kerberos security mechanism supports three quality of protection levels as follows (in decreasing order or speed). Specify **GSS\_KRB5\_INTEG\_C\_QOP\_DES\_MD5** (or



**GSS\_C\_QOP\_DEFAULT**) for interoperability with other implementations of the Kerberos security mechanism.

<i>GSS_KRB5_INTEG_C_QOP_MD5</i>	Truncated MD5
<i>GSS_KRB5_INTEG_C_QOP_DES_MD5</i>	DES_MAC of an MD5 hash (default)
<i>GSS_KRB5_INTEG_C_QOP_DES_MAC</i>	Normal DES_MAC algorithm

**input\_message (Input)**  
The message to be wrapped.

**conf\_state (Output)**  
The level of confidentiality that was applied to the message. Specify **NULL** for this parameter if the confidentiality state is not needed. The return value is set as follows:

<i>TRUE</i>	Both confidentiality and integrity services were applied.
<i>FALSE</i>	Only integrity services were applied.

**output\_message (Output)**  
The wrapped message. The buffer should be released when it is no longer needed by calling the **gss\_release\_buffer()** routine.

## Return Value

The return value is one of the following status codes:

**GSS\_S\_BAD\_QOP**  
The quality of protection value is not valid.

**GSS\_S\_COMPLETE**  
The routine completed successfully.

**GSS\_S\_CONTEXT\_EXPIRED**  
The context identifier provided by the caller has expired.

**GSS\_S\_CREDENTIALS\_EXPIRED**  
Credentials are no longer valid.

**GSS\_S\_FAILURE**  
The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CONTEXT**  
The context identifier provided by the caller does not refer to a valid security context.

## Authorities

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

## Error Messages

Message ID	Error Message Text
CPE3418 E	Possible APAR condition or hardware failure.

## Usage Notes

1. If confidentiality is requested (the *conf\_req* is **true**) but confidentiality services are not available for the security context, no error is returned and only integrity services are performed. The *conf\_state* return parameter indicates whether or not the requested confidentiality services were performed.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## **gss\_wrap\_size\_limit()**—Determine Largest Message that can be Wrapped

```
Syntax
#include <gssapi.h>

OM_uint32 gss_wrap_size_limit (
    OM_uint32 *   minor_status,
    gss_ctx_id_t  context_handle,
    int           conf_req,
    gss_qop_t     qop_req,
    OM_uint32     size_req,
    OM_uint32 *   max_size);
```

Service Program Name: QSYS/QKRBGSS

Default public authority: \*USE

Threadsafe: Yes

The **gss\_wrap\_size\_limit()** function determines the largest message that can be processed by the **gss\_wrap()** routine without exceeding the specified output token size.

## Parameters

### **minor\_status** (Output)

A status code from the security mechanism.

### **context\_handle** (Input)

The security context that will be associated with the messages.

### **conf\_req** (Input)

Whether confidentiality services will be requested for the messages as follows:

*TRUE*

Both confidentiality and integrity and authentication services will be requested.

FALSE

Only integrity and authentication services will be requested.

**qop\_req (Input)**

The quality of protection that will be used with the messages. Specify **GSS\_C\_QOP\_DEFAULT** to use the default quality of protection as defined by the selected security mechanism.

The Kerberos security mechanism supports three quality of protection levels as follows (in decreasing order or speed):

<i>GSS_KRB5_INTEG_C_QOP_MD5</i>	Truncated MD5
<i>GSS_KRB5_INTEG_C_QOP_DES_MD5</i>	DES_MAC of an MD5 hash (default)
<i>GSS_KRB5_INTEG_C_QOP_DES_MAC</i>	Normal DES_MAC algorithm

**size\_req (Input)**

The maximum output token size.

**max\_size (Output)**

The maximum message size that can be processed without exceeding the specified maximum token size.

**Return Value**

The return value is one of the following status codes:

**GSS\_S\_BAD\_QOP**

The quality of protection requested is not valid.

**GSS\_S\_COMPLETE**

The routine completed successfully.

**GSS\_S\_CONTEXT\_EXPIRED**

The context identifier provided by the caller has expired.

**GSS\_S\_FAILURE**

The routine failed for reasons that are not defined at the GSS level. The *minor\_status* return parameter contains a mechanism-dependent error code describing the reason for the failure.

**GSS\_S\_NO\_CONTEXT**

The context identifier provided by the caller does not refer to a valid security context.

**Authorities**

Object Referred to	Data Authority Required
Each directory in the path name preceding the configuration file	*X
Configuration file	*R

**Error Messages**

<b>Message ID</b>	<b>Error Message Text</b>
CPE3418 E	Possible APAR condition or hardware failure.

API introduced: V5R1

[Top](#) | [Security APIs](#)  
[UNIX-Type APIs](#) | [APIs by category](#)

---

## Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Advanced 36  
Advanced Function Printing  
Advanced Peer-to-Peer Networking  
AFP  
AIX  
AS/400  
COBOL/400  
CUA  
DB2  
DB2 Universal Database  
Distributed Relational Database Architecture  
Domino  
DPI

DRDA  
eServer  
GDDM  
IBM  
Integrated Language Environment  
Intelligent Printer Data Stream  
IPDS  
iSeries  
Lotus Notes  
MVS  
Netfinity  
Net.Data  
NetView  
Notes  
OfficeVision  
Operating System/2  
Operating System/400  
OS/2  
OS/400  
PartnerWorld  
PowerPC  
PrintManager  
Print Services Facility  
RISC System/6000  
RPG/400  
RS/6000  
SAA  
SecureWay  
System/36  
System/370  
System/38  
System/390  
VisualAge  
WebSphere  
xSeries

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

---

## Terms and conditions for downloading and printing publications

Permissions for the use of the information you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

**Personal Use:** You may reproduce this information for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of this information, or any portion thereof, without the express consent of IBM<sup>(R)</sup>.

**Commercial Use:** You may reproduce, distribute and display this information solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of this information, or reproduce, distribute or display this information or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the information or any data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the information is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THIS INFORMATION. THE INFORMATION IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

All material copyrighted by IBM Corporation.

By downloading or printing information from this site, you have indicated your agreement with these terms and conditions.

---

## **Code disclaimer information**

This document contains programming examples.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM<sup>(R)</sup>, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.







Printed in USA