

# **GNU SASL API Reference Manual**

---

**COLLABORATORS**

	<i>TITLE :</i> GNU SASL API Reference Manual		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY		April 3, 2012	

**REVISION HISTORY**

NUMBER	DATE	DESCRIPTION	NAME

# Contents

<b>1</b>	<b>GNU SASL API Reference Manual</b>	<b>1</b>
1.1	gsasl . . . . .	3
1.2	gsasl-mech . . . . .	23
1.3	gsasl-compatible . . . . .	26
<b>2</b>	<b>Index</b>	<b>64</b>

---

# List of Figures

1.1	Illustration of separation between application and individual mechanism . . . . .	2
1.2	High-level control flow of SASL application . . . . .	2
1.3	Low-level control flow of SASL application . . . . .	3

## Chapter 1

# GNU SASL API Reference Manual

GNU SASL is an implementation of the Simple Authentication and Security Layer framework and a few common SASL mechanisms. SASL is used by network servers (e.g., IMAP, SMTP) to request authentication from clients, and in clients to authenticate against servers.

GNU SASL consists of a library (`libgsasl`), a command line utility (`gsasl`) to access the library from the shell, and a manual. The library includes support for the framework (with authentication functions and application data privacy and integrity functions) and at least partial support for the ANONYMOUS, CRAM-MD5, DIGEST-MD5, EXTERNAL, GS2-KRB5, GSSAPI, LOGIN, NTLM, PLAIN, SCRAM-SHA-1, SCRAM-SHA-1-PLUS, SAML20, OPENID20, and SECURID mechanisms.

The library is easily ported because it does not do network communication by itself, but rather leaves it up to the calling application. The library is flexible with regards to the authorization infrastructure used, as it utilizes a callback into the application to decide whether a user is authorized or not.

GNU SASL is developed for the GNU/Linux system, but runs on over 20 platforms including most major Unix platforms and Windows, and many kind of devices including iPAQ handhelds and S/390 mainframes.

GNU SASL is written in pure ANSI C89 to be portable to embedded and otherwise limited platforms. The entire library, with full support for ANONYMOUS, EXTERNAL, PLAIN, LOGIN and CRAM-MD5, and the front-end that support client and server mode, and the IMAP and SMTP protocols, fits in under 60kb on an Intel x86 platform, without any modifications to the code. (This figure was accurate as of version 0.0.13.)

The library is licensed under the GNU Lesser General Public License version 2.1 or later. The command-line application (`src/`), examples (`examples/`), self-test suite (`tests/`) are licensed under the GNU General Public License license version 3.0 or later. The documentation (`doc/`) is licensed under the GNU Free Documentation License version 1.3 or later.

A conceptual view of how your application, the library, and each mechanism interact is shown in Figure 1.1.

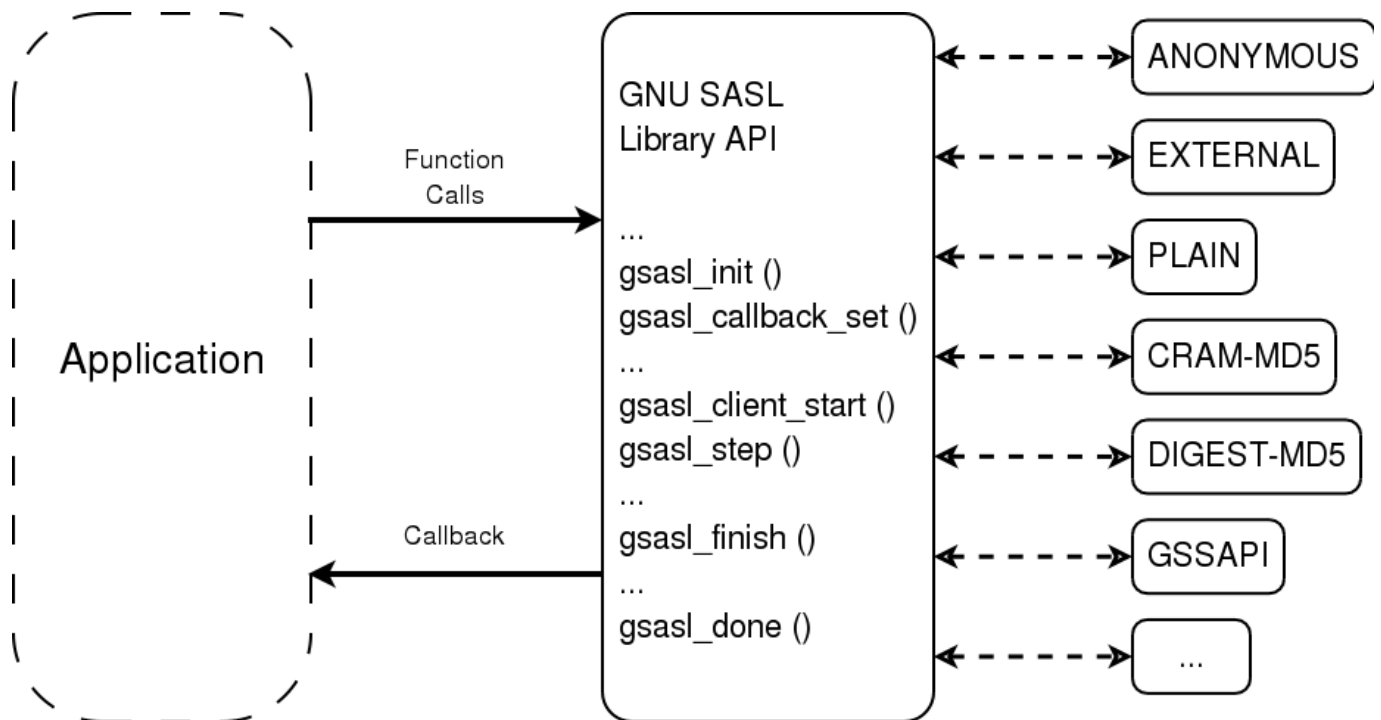


Figure 1.1: Illustration of separation between application and individual mechanism

The operation of an application using the library can best be understood in terms of a flow chart diagram, as shown in Figure 1.2. The details on how the actual negotiation are carried out are illustrated in Figure 1.3.

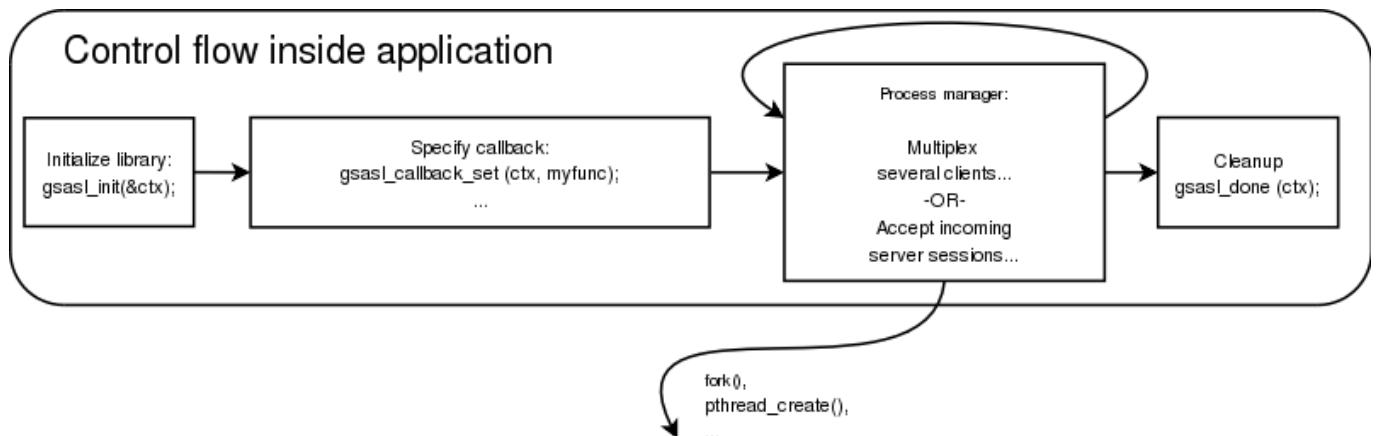


Figure 1.2: High-level control flow of SASL application

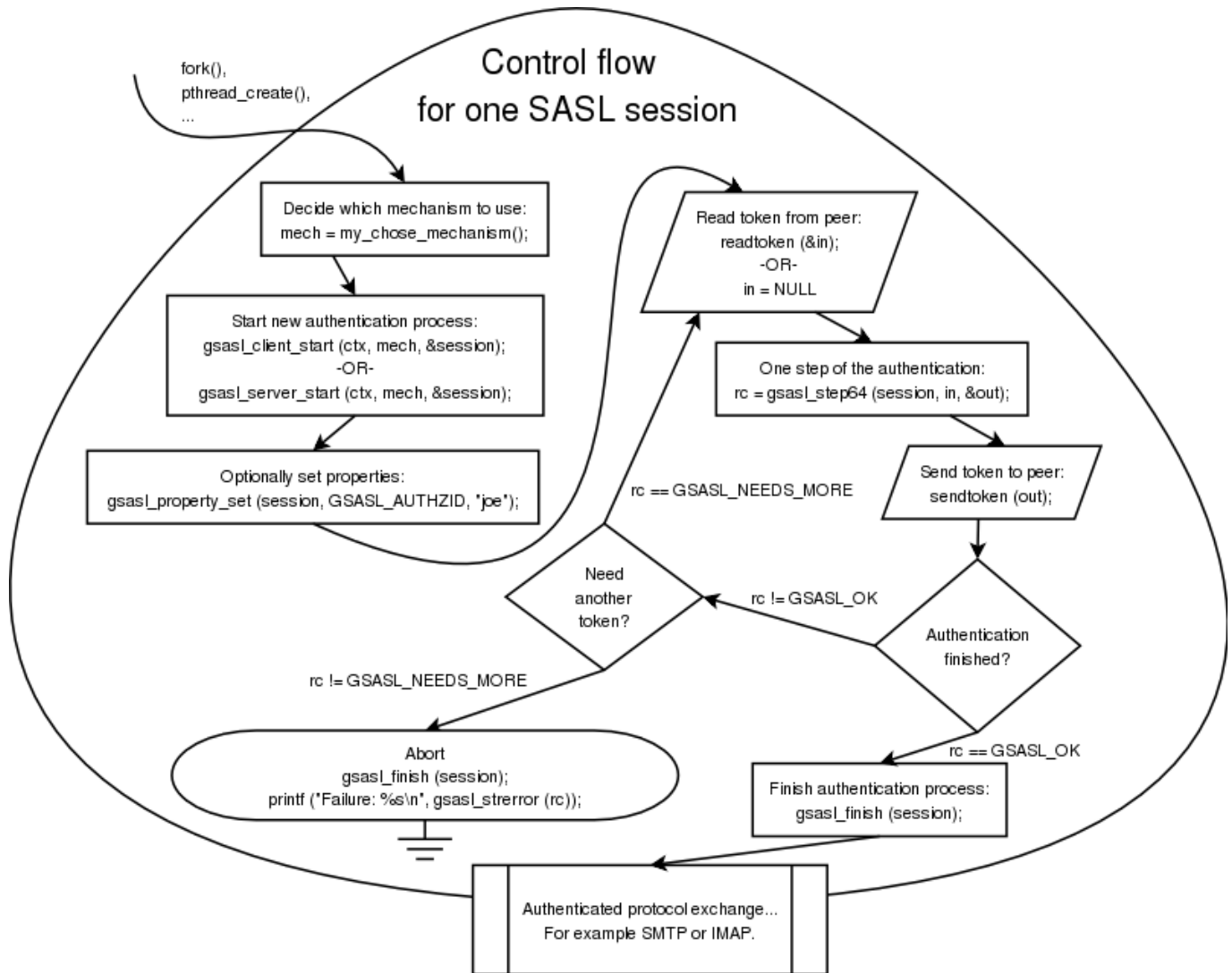


Figure 1.3: Low-level control flow of SASL application

## 1.1 gsasl

gsasl —

### Synopsis

```

#define GSASL_API
#define GSASL_VERSION
#define GSASL_VERSION_MAJOR
#define GSASL_VERSION_MINOR
#define GSASL_VERSION_PATCH
#define GSASL_VERSION_NUMBER
enum Gsasl_rc;
enum Gsasl_qop;
enum Gsasl_cipher;
enum Gsasl_saslprep_flags;

```

---

```

typedef          Gsasl;
typedef          Gsasl_session;
enum            Gsasl_property;
int             (*Gsasl_callback_function)

                (Gsasl *ctx,
                 Gsasl_session *sctx,
                 Gsasl_property prop);

int             gsasl_init
void            gsasl_done
const char *    gsasl_check_version
void            gsasl_callback_set
                (Gsasl *ctx,
                 Gsasl_callback_function cb);

int             gsasl_callback
                (Gsasl *ctx,
                 Gsasl_session *sctx,
                 Gsasl_property prop);

void            gsasl_callback_hook_set
                (Gsasl *ctx,
                 void *hook);

void *          gsasl_callback_hook_get
void            gsasl_session_hook_set
                (Gsasl_session *sctx,
                 void *hook);

void *          gsasl_session_hook_get
void            gsasl_property_set
                (Gsasl_session *sctx,
                 Gsasl_property prop,
                 const char *data);

void            gsasl_property_set_raw
                (Gsasl_session *sctx,
                 Gsasl_property prop,
                 const char *data,
                 size_t len);

const char *    gsasl_property_get
                (Gsasl_session *sctx,
                 Gsasl_property prop);

const char *    gsasl_property_fast
                (Gsasl_session *sctx,
                 Gsasl_property prop);

int             gsasl_client_mechlist
                (Gsasl *ctx,
                 char **out);

int             gsasl_client_support_p
                (Gsasl *ctx,
                 const char *name);

const char *    gsasl_client_suggest_mechanism
                (Gsasl *ctx,
                 const char *mechlist);

int             gsasl_server_mechlist
                (Gsasl *ctx,
                 char **out);

int             gsasl_server_support_p
                (Gsasl *ctx,
                 const char *name);

int             gsasl_client_start
                (Gsasl *ctx,
                 const char *mech,
                 Gsasl_session **sctx);

int             gsasl_server_start
                (Gsasl *ctx,
                 const char *mech,
                 Gsasl_session **sctx);

int             gsasl_step
                (Gsasl_session *sctx,
                 const char *input,
                 size_t input_len,
                 char **output,
                 size_t *output_len);

int             gsasl_step64
                (Gsasl_session *sctx,
                 const char *b64input,
                 char **b64output);

void            gsasl_finish
int             gsasl_encode
                (Gsasl_session *sctx,

```

---



int	gsasl_decode	const char *input, size_t input_len, char **output, size_t *output_len); (Gsasl_session *sctx, const char *input, size_t input_len, char **output, size_t *output_len);
const char *	gsasl_mechanism_name	(Gsasl_session *sctx);
const char *	gsasl_strerror	(int err);
const char *	gsasl_strerror_name	(int err);
int	gsasl_saslprep	(const char *in, Gsasl_saslprep_flags flags, char **out, int *stringpreprc);
int	gsasl_simple_getpass	(const char *filename, const char *username, char **key);
int	gsasl_base64_to	(const char *in, size_t inlen, char **out, size_t *outlen);
int	gsasl_base64_from	(const char *in, size_t inlen, char **out, size_t *outlen);
int	gsasl_nonce	(char *data, size_t datalen);
int	gsasl_random	(char *data, size_t datalen);
int	gsasl_md5	(const char *in, size_t inlen, char *out[16]);
int	gsasl_hmac_md5	(const char *key, size_t keylen, const char *in, size_t inlen, char *outhash[16]);
int	gsasl_shal	(const char *in, size_t inlen, char *out[20]);
int	gsasl_hmac_shal	(const char *key, size_t keylen, const char *in, size_t inlen, char *outhash[20]);
void	gsasl_free	(void *ptr);

## Description

## Details

### GSASL\_API

```
#define GSASL_API
```

## GSASL\_VERSION

```
#define GSASL_VERSION "1.7.3"
```

Pre-processor symbol with a string that describe the header file version number. Used together with `gsasl_check_version()` to verify header file and run-time library consistency.

## GSASL\_VERSION\_MAJOR

```
#define GSASL_VERSION_MAJOR 1
```

Pre-processor symbol with a decimal value that describe the major level of the header file version number. For example, when the header version is 1.2.3 this symbol will be 1.

Since 1.1

## GSASL\_VERSION\_MINOR

```
#define GSASL_VERSION_MINOR 7
```

Pre-processor symbol with a decimal value that describe the minor level of the header file version number. For example, when the header version is 1.2.3 this symbol will be 2.

Since 1.1

## GSASL\_VERSION\_PATCH

```
#define GSASL_VERSION_PATCH 3
```

Pre-processor symbol with a decimal value that describe the patch level of the header file version number. For example, when the header version is 1.2.3 this symbol will be 3.

Since 1.1

## GSASL\_VERSION\_NUMBER

```
#define GSASL_VERSION_NUMBER 0x010703
```

Pre-processor symbol with a hexadecimal value describing the header file version number. For example, when the header version is 1.2.3 this symbol will have the value 0x010203.

Since 1.1

## enum Gsasl\_rc

```
typedef enum
{
    GSASL_OK = 0,
    GSASL_NEEDS_MORE = 1,
    GSASL_UNKNOWN_MECHANISM = 2,
    GSASL_MECHANISM_CALLED_TOO_MANY_TIMES = 3,
    GSASL_MALLOC_ERROR = 7,
    GSASL_BASE64_ERROR = 8,
    GSASL_CRYPTO_ERROR = 9,
    GSASL_SASLPREP_ERROR = 29,
```

```
GSASL_MECHANISM_PARSE_ERROR = 30,
GSASL_AUTHENTICATION_ERROR = 31,
GSASL_INTEGRITY_ERROR = 33,
GSASL_NO_CLIENT_CODE = 35,
GSASL_NO_SERVER_CODE = 36,
GSASL_NO_CALLBACK = 51,
GSASL_NO_ANONYMOUS_TOKEN = 52,
GSASL_NO_AUTHID = 53,
GSASL_NO_AUTHZID = 54,
GSASL_NO_PASSWORD = 55,
GSASL_NO_PASSCODE = 56,
GSASL_NO_PIN = 57,
GSASL_NO_SERVICE = 58,
GSASL_NO_HOSTNAME = 59,
GSASL_NO_CB_TLS_UNIQUE = 65,
GSASL_NO_SAML20_IDP_IDENTIFIER = 66,
GSASL_NO_REDIRECT_URL = 67,
/* Mechanism specific errors. */
GSASL_GSSAPI_RELEASE_BUFFER_ERROR = 37,
GSASL_GSSAPI_IMPORT_NAME_ERROR = 38,
GSASL_GSSAPI_INIT_SEC_CONTEXT_ERROR = 39,
GSASL_GSSAPI_ACCEPT_SEC_CONTEXT_ERROR = 40,
GSASL_GSSAPI_UNWRAP_ERROR = 41,
GSASL_GSSAPI_WRAP_ERROR = 42,
GSASL_GSSAPI_ACQUIRE_CRED_ERROR = 43,
GSASL_GSSAPI_DISPLAY_NAME_ERROR = 44,
GSASL_GSSAPI_UNSUPPORTED_PROTECTION_ERROR = 45,
GSASL_KERBEROS_V5_INIT_ERROR = 46,
GSASL_KERBEROS_V5_INTERNAL_ERROR = 47,
GSASL_SHISHI_ERROR = GSASL_KERBEROS_V5_INTERNAL_ERROR,
GSASL_SECURID_SERVER_NEED_ADDITIONAL_PASSCODE = 48,
GSASL_SECURID_SERVER_NEED_NEW_PIN = 49,
GSASL_GSSAPI_ENCAPSULATE_TOKEN_ERROR = 60,
GSASL_GSSAPI_DECAPSULATE_TOKEN_ERROR = 61,
GSASL_GSSAPI_INQUIRE_MECH_FOR_SASLNAME_ERROR = 62,
GSASL_GSSAPI_TEST_OID_SET_MEMBER_ERROR = 63,
GSASL_GSSAPI_RELEASE_OID_SET_ERROR = 64
/* When adding new values, note that integers are not necessarily
   assigned monotonously increasingly. */
} Gsasl_rc;
```

Error codes for library functions.

**GSASL\_OK** Successful return code, guaranteed to be always 0.

**GSASL\_NEEDS\_MORE** Mechanism expects another round-trip.

**GSASL\_UNKNOWN\_MECHANISM** Application requested an unknown mechanism.

**GSASL\_MECHANISM\_CALLED\_TOO\_MANY\_TIMES** Application requested too many round trips from mechanism.

**GSASL\_MALLOC\_ERROR** Memory allocation failed.

**GSASL\_BASE64\_ERROR** Base64 encoding/decoding failed.

**GSASL\_CRYPTO\_ERROR** Cryptographic error.

**GSASL\_SASLPREP\_ERROR** Failed to prepare internationalized string.

**GSASL\_MECHANISM\_PARSE\_ERROR** Mechanism could not parse input.

**GSASL\_AUTHENTICATION\_ERROR** Authentication has failed.

**GSASL\_INTEGRITY\_ERROR** Application data integrity check failed.

**GSASL\_NO\_CLIENT\_CODE** Library was built with client functionality.

**GSASL\_NO\_SERVER\_CODE** Library was built with server functionality.

**GSASL\_NO\_CALLBACK** Application did not provide a callback.

**GSASL\_NO\_ANONYMOUS\_TOKEN** Could not get required anonymous token.

**GSASL\_NO\_AUTHID** Could not get required authentication identity (username).

**GSASL\_NO\_AUTHZID** Could not get required authorization identity.

**GSASL\_NO\_PASSWORD** Could not get required password.

**GSASL\_NO\_PASSCODE** Could not get required SecurID PIN.

**GSASL\_NO\_PIN** Could not get required SecurID PIN.

**GSASL\_NO\_SERVICE** Could not get required service name.

**GSASL\_NO\_HOSTNAME** Could not get required hostname.

**GSASL\_NO\_CB\_TLS\_UNIQUE** Could not get required tls-unique CB.

**GSASL\_NO\_SAML20\_IDP\_IDENTIFIER** Could not get required SAML IdP.

**GSASL\_NO\_REDIRECT\_URL** Could not get required redirect URL.

**GSASL\_GSSAPI\_RELEASE\_BUFFER\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_IMPORT\_NAME\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_INIT\_SEC\_CONTEXT\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_ACCEPT\_SEC\_CONTEXT\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_UNWRAP\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_WRAP\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_ACQUIRE\_CRED\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_DISPLAY\_NAME\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_UNSUPPORTED\_PROTECTION\_ERROR** An unsupported quality-of-protection layer was requested.

**GSASL\_KERBEROS\_V5\_INIT\_ERROR** Init error in KERBEROS\_V5.

**GSASL\_KERBEROS\_V5\_INTERNAL\_ERROR** General error in KERBEROS\_V5.

**GSASL\_SHISHI\_ERROR** Same as **GSASL\_KERBEROS\_V5\_INTERNAL\_ERROR**.

**GSASL\_SECURID\_SERVER\_NEED\_ADDITIONAL\_PASSCODE** SecurID mechanism needs an additional passcode.

**GSASL\_SECURID\_SERVER\_NEED\_NEW\_PIN** SecurID mechanism needs a new PIN.

**GSASL\_GSSAPI\_ENCAPSULATE\_TOKEN\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_DECAPSULATE\_TOKEN\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_INQUIRE\_MECH\_FOR\_SASLNAME\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_TEST\_OID\_SET\_MEMBER\_ERROR** GSS-API library call error.

**GSASL\_GSSAPI\_RELEASE\_OID\_SET\_ERROR** GSS-API library call error.

---

**enum Gsasl\_qop**

```
typedef enum
{
    GSASL_QOP_AUTH = 1,
    GSASL_QOP_AUTH_INT = 2,
    GSASL_QOP_AUTH_CONF = 4
} Gsasl_qop;
```

Quality of Protection types (DIGEST-MD5 and GSSAPI). The integrity and confidentiality values is about application data wrapping. We recommend that you use *GSASL\_QOP\_AUTH* with TLS as that combination is generally more secure and have better chance of working than the integrity/confidentiality layers of SASL.

**GSASL\_QOP\_AUTH** Authentication only.

**GSASL\_QOP\_AUTH\_INT** Authentication and integrity.

**GSASL\_QOP\_AUTH\_CONF** Authentication, integrity and confidentiality.

**enum Gsasl\_cipher**

```
typedef enum
{
    GSASL_CIPHER_DES = 1,
    GSASL_CIPHER_3DES = 2,
    GSASL_CIPHER_RC4 = 4,
    GSASL_CIPHER_RC4_40 = 8,
    GSASL_CIPHER_RC4_56 = 16,
    GSASL_CIPHER_AES = 32
} Gsasl_cipher;
```

Encryption types (DIGEST-MD5) for confidentiality services of application data. We recommend that you use TLS instead as it is generally more secure and have better chance of working.

**GSASL\_CIPHER\_DES** Cipher DES.

**GSASL\_CIPHER\_3DES** Cipher 3DES.

**GSASL\_CIPHER\_RC4** Cipher RC4.

**GSASL\_CIPHER\_RC4\_40** Cipher RC4 with 40-bit keys.

**GSASL\_CIPHER\_RC4\_56** Cipher RC4 with 56-bit keys.

**GSASL\_CIPHER\_AES** Cipher AES.

**enum Gsasl\_saslprep\_flags**

```
typedef enum
{
    GSASL_ALLOW_UNASSIGNED = 1
} Gsasl_saslprep_flags;
```

Flags for the SASLprep function, see [gsasl\\_saslprep\(\)](#). For background, see the GNU Libidn documentation.

**GSASL\_ALLOW\_UNASSIGNED** Allow unassigned code points.

## Gsasl

```
typedef struct Gsasl Gsasl;
```

Handle to global library context.

## Gsasl\_session

```
typedef struct Gsasl_session Gsasl_session;
```

Handle to SASL session context.

## enum Gsasl\_property

```
typedef enum
{
    /* Information properties, e.g., username. */
    GSASL_AUTHID = 1,
    GSASL_AUTHZID = 2,
    GSASL_PASSWORD = 3,
    GSASL_ANONYMOUS_TOKEN = 4,
    GSASL_SERVICE = 5,
    GSASL_HOSTNAME = 6,
    GSASL_GSSAPI_DISPLAY_NAME = 7,
    GSASL_PASSCODE = 8,
    GSASL_SUGGESTED_PIN = 9,
    GSASL_PIN = 10,
    GSASL_REALM = 11,
    GSASL_DIGEST_MD5_HASHED_PASSWORD = 12,
    GSASL_QOPS = 13,
    GSASL_QOP = 14,
    GSASL_SCRAM_ITER = 15,
    GSASL_SCRAM_SALT = 16,
    GSASL_SCRAM_SALTED_PASSWORD = 17,
    GSASL_CB_TLS_UNIQUE = 18,
    GSASL_SAML20_IDP_IDENTIFIER = 19,
    GSASL_REDIRECT_URL = 20,
    GSASL_OPENID20_OUTCOME_DATA = 22,
    /* Client callbacks. */
    GSASL_AUTHENTICATE_IN_BROWSER = 250,
    /* Server validation callback properties. */
    GSASL_VALIDATE_SIMPLE = 500,
    GSASL_VALIDATE_EXTERNAL = 501,
    GSASL_VALIDATE_ANONYMOUS = 502,
    GSASL_VALIDATE_GSSAPI = 503,
    GSASL_VALIDATE_SECURID = 504,
    GSASL_VALIDATE_SAML20 = 505,
    GSASL_VALIDATE_OPENID20 = 506
} Gsasl_property;
```

Callback/property types.

**GSASL\_AUTHID** Authentication identity (username).

**GSASL\_AUTHZID** Authorization identity.

**GSASL\_PASSWORD** Password.

**GSASL\_ANONYMOUS\_TOKEN** Anonymous identifier.

**GSASL\_SERVICE** Service name

**GSASL\_HOSTNAME** Host name.

**GSASL\_GSSAPI\_DISPLAY\_NAME** GSS-API credential principal name.

**GSASL\_PASSCODE** SecurID passcode.

**GSASL\_SUGGESTED\_PIN** SecurID suggested PIN.

**GSASL\_PIN** SecurID PIN.

**GSASL\_REALM** User realm.

**GSASL\_DIGEST\_MD5\_HASHED\_PASSWORD** Pre-computed hashed DIGEST-MD5 password, to avoid storing passwords in the clear.

**GSASL\_QOPS** Set of quality-of-protection values.

**GSASL\_QOP** Quality-of-protection value.

**GSASL\_SCRAM\_ITER** Number of iterations in password-to-key hashing.

**GSASL\_SCRAM\_SALT** Salt for password-to-key hashing.

**GSASL\_SCRAM\_SALTED\_PASSWORD** Pre-computed salted SCRAM key, to avoid re-computation and storing passwords in the clear.

**GSASL\_CB\_TLS\_UNIQUE** Base64 encoded tls-unique channel binding.

**GSASL\_SAML20\_IDP\_IDENTIFIER** SAML20 user IdP URL.

**GSASL\_REDIRECT\_URL** URL to access in GSASL\_AUTHENTICATE\_IN\_BROWSER.

**GSASL\_OPENID20\_OUTCOME\_DATA** OpenID 2.0 authentication outcome data.

**GSASL\_AUTHENTICATE\_IN\_BROWSER** Request to authenticate in browser.

**GSASL\_VALIDATE\_SIMPLE** Request for simple validation.

**GSASL\_VALIDATE\_EXTERNAL** Request for validation of EXTERNAL.

**GSASL\_VALIDATE\_ANONYMOUS** Request for validation of ANONYMOUS.

**GSASL\_VALIDATE\_GSSAPI** Request for validation of GSSAPI/GS2.

**GSASL\_VALIDATE\_SECURID** Request for validation of SecurID.

**GSASL\_VALIDATE\_SAML20** Request for validation of SAML20.

**GSASL\_VALIDATE\_OPENID20** Request for validation of OpenID 2.0 login.

### Gsasl\_callback\_function ()

```
int (*Gsasl_callback_function) (Gsasl *ctx,
                                Gsasl_session *sctx,
                                Gsasl_property prop);
```

Prototype of function that the application should implement. Use [gsasl\\_callback\\_set\(\)](#) to inform the library about your callback function.

It is called by the SASL library when it need some information from the application. Depending on the value of *prop*, it should either set some property (e.g., username or password) using [gsasl\\_property\\_set\(\)](#), or it should extract some properties (e.g., authentication and authorization identities) using [gsasl\\_property\\_fast\(\)](#) and use them to make a policy decision, perhaps returning GSASL\_AUTHENTICATION\_ERROR or GSASL\_OK depending on whether the policy permitted the operation.

**ctx** : libgsasl handle.

**sctx** : session handle, may be NULL.

**prop** : enumerated value of Gsasl\_property type.

**Returns** : Any valid return code, the interpretation of which depend on the *prop* value.

Since 0.2.0

### gsasl\_init ()

```
int                gsasl_init                (Gsasl **ctx);
```

This functions initializes libgsasl. The handle pointed to by *ctx* is valid for use with other libgsasl functions iff this function is successful. It also register all builtin SASL mechanisms, using [gsasl\\_register\(\)](#).

**ctx** : pointer to libgsasl handle.

**Returns** : GSASL\_OK iff successful, otherwise [GSASL\\_MALLOC\\_ERROR](#).

### gsasl\_done ()

```
void                gsasl_done                (Gsasl *ctx);
```

This function destroys a libgsasl handle. The handle must not be used with other libgsasl functions after this call.

**ctx** : libgsasl handle.

### gsasl\_check\_version ()

```
const char *        gsasl_check_version      (const char *req_version);
```

Check GNU SASL Library version.

See [GSASL\\_VERSION](#) for a suitable *req\_version* string.

This function is one of few in the library that can be used without a successful call to [gsasl\\_init\(\)](#).

**req\_version** : version string to compare with, or NULL.

**Returns** : Check that the version of the library is at minimum the one given as a string in *req\_version* and return the actual version string of the library; return NULL if the condition is not met. If NULL is passed to this function no check is done and only the version string is returned.

### gsasl\_callback\_set ()

```
void                gsasl_callback_set        (Gsasl *ctx,  
                                                Gsasl_callback_function cb);
```

Store the pointer to the application provided callback in the library handle. The callback will be used, via [gsasl\\_callback\(\)](#), by mechanisms to discover various parameters (such as username and passwords). The callback function will be called with a Gsasl\_property value indicating the requested behaviour. For example, for [GSASL\\_ANONYMOUS\\_TOKEN](#), the function is expected to invoke [gsasl\\_property\\_set\(CTX, GSASL\\_ANONYMOUS\\_TOKEN, "token"\)](#) where "token" is the anonymous token the application wishes the SASL mechanism to use. See the manual for the meaning of all parameters.

**ctx** : handle received from [gsasl\\_init\(\)](#).

**cb** : pointer to function implemented by application.

Since 0.2.0



**gsasl\_callback ()**

```
int                gsasl_callback                (Gsasl *ctx,  
                                                Gsasl_session *sctx,  
                                                Gsasl_property prop);
```

Invoke the application callback. The *prop* value indicate what the callback is expected to do. For example, for **GSASL\_ANONYMOUS\_TOKEN** the function is expected to invoke `gsasl_property_set(SCTX, GSASL_ANONYMOUS_TOKEN, "token")` where "token" is the anonymous token the application wishes the SASL mechanism to use. See the manual for the meaning of all parameters.

Note that if no callback has been set by the application, but the obsolete callback interface has been used, this function will translate the old callback interface into the new. This interface should be sufficient to invoke all callbacks, both new and old.

**ctx** : handle received from **gsasl\_init()**, may be NULL to derive it from *sctx*.

**sctx** : session handle.

**prop** : enumerated value of Gsasl\_property type.

**Returns** : Returns whatever the application callback returns, or **GSASL\_NO\_CALLBACK** if no application was known.

Since 0.2.0

**gsasl\_callback\_hook\_set ()**

```
void                gsasl_callback_hook_set      (Gsasl *ctx,  
                                                void *hook);
```

Store application specific data in the libgsasl handle.

The application data can be later (for instance, inside a callback) be retrieved by calling **gsasl\_callback\_hook\_get()**. This is normally used by the application to maintain a global state between the main program and callbacks.

**ctx** : libgsasl handle.

**hook** : opaque pointer to application specific data.

Since 0.2.0

**gsasl\_callback\_hook\_get ()**

```
void *              gsasl_callback_hook_get     (Gsasl *ctx);
```

Retrieve application specific data from libgsasl handle.

The application data is set using **gsasl\_callback\_hook\_set()**. This is normally used by the application to maintain a global state between the main program and callbacks.

**ctx** : libgsasl handle.

**Returns** : Returns the application specific data, or NULL.

Since 0.2.0



Make a copy of *len* sized *data* and store a zero terminated version of it in the session handle for the indicated property *prop*. You can immediately deallocate *data* after calling this function, without affecting the data stored in the session handle. Except for the length indicator, this function is identical to `gsasl_property_set`.

**sctx** : session handle.

**prop** : enumerated value of `Gsasl_property` type, indicating the type of data in *data*.

**data** : character string to store.

**len** : length of character string to store.

Since 0.2.0

### **gsasl\_property\_get ()**

```
const char *      gsasl_property_get      (Gsasl_session *sctx,  
                                           Gsasl_property prop);
```

Retrieve the data stored in the session handle for given property *prop*, possibly invoking the application callback to get the value. The pointer is to live data, and must not be deallocated or modified in any way.

This function will invoke the application callback, using `gsasl_callback()`, when a property value is not known.

If no value is known, and no callback is specified or if the callback fail to return data, and if any obsolete callback functions has been set by the application, this function will try to call these obsolete callbacks, and store the returned data as the corresponding property. This behaviour of this function will be removed when the obsolete callback interfaces are removed.

**sctx** : session handle.

**prop** : enumerated value of `Gsasl_property` type, indicating the type of data in *data*.

**Returns** : Return data for property, or NULL if no value known.

Since 0.2.0

### **gsasl\_property\_fast ()**

```
const char *      gsasl_property_fast     (Gsasl_session *sctx,  
                                           Gsasl_property prop);
```

Retrieve the data stored in the session handle for given property *prop*.

The pointer is to live data, and must not be deallocated or modified in any way.

This function will not invoke the application callback.

**sctx** : session handle.

**prop** : enumerated value of `Gsasl_property` type, indicating the type of data in *data*.

**Returns** : Return property value, if known, or NULL if no value known.

Since 0.2.0

---

**gsasl\_client\_mechlist ()**

```
int                gsasl_client_mechlist      (Gsasl *ctx,  
                                              char **out);
```

Return a newly allocated string containing SASL names, separated by space, of mechanisms supported by the libgsasl client. *out* is allocated by this function, and it is the responsibility of caller to deallocate it.

**ctx** : libgsasl handle.

**out** : newly allocated output character array.

**Returns** : Returns **GSASL\_OK** if successful, or error code.

**gsasl\_client\_support\_p ()**

```
int                gsasl_client_support_p    (Gsasl *ctx,  
                                              const char *name);
```

Decide whether there is client-side support for a specified mechanism.

**ctx** : libgsasl handle.

**name** : name of SASL mechanism.

**Returns** : Returns 1 if the libgsasl client supports the named mechanism, otherwise 0.

**gsasl\_client\_suggest\_mechanism ()**

```
const char *       gsasl_client_suggest_mechanism (Gsasl *ctx,  
                                                  const char *mechlist);
```

Given a list of mechanisms, suggest which to use.

**ctx** : libgsasl handle.

**mechlist** : input character array with SASL mechanism names, separated by invalid characters (e.g. SPC).

**Returns** : Returns name of "best" SASL mechanism supported by the libgsasl client which is present in the input string, or NULL if no supported mechanism is found.

**gsasl\_server\_mechlist ()**

```
int                gsasl_server_mechlist    (Gsasl *ctx,  
                                              char **out);
```

Return a newly allocated string containing SASL names, separated by space, of mechanisms supported by the libgsasl server. *out* is allocated by this function, and it is the responsibility of caller to deallocate it.

**ctx** : libgsasl handle.

**out** : newly allocated output character array.

**Returns** : Returns **GSASL\_OK** if successful, or error code.





Encode data according to negotiated SASL mechanism. This might mean that data is integrity or privacy protected. The *output* buffer is allocated by this function, and it is the responsibility of caller to deallocate it by calling `free(output)`.

**sctx** : libgsasl session handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : newly allocated output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if encoding was successful, otherwise an error code.

### gsasl\_decode ()

```
int                gsasl_decode                (Gsasl_session *sctx,
                                                const char *input,
                                                size_t input_len,
                                                char **output,
                                                size_t *output_len);
```

Decode data according to negotiated SASL mechanism. This might mean that data is integrity or privacy protected. The *output* buffer is allocated by this function, and it is the responsibility of caller to deallocate it by calling `free(output)`.

**sctx** : libgsasl session handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : newly allocated output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if encoding was successful, otherwise an error code.

### gsasl\_mechanism\_name ()

```
const char *      gsasl_mechanism_name      (Gsasl_session *sctx);
```

This function returns the name of the SASL mechanism used in the session.

**sctx** : libgsasl session handle.

**Returns** : Returns a zero terminated character array with the name of the SASL mechanism, or NULL if not known.

Since 0.2.28

### gsasl\_strerror ()

```
const char *      gsasl_strerror            (int err);
```

Convert return code to human readable string explanation of the reason for the particular error code.

This string can be used to output a diagnostic message to the user.

This function is one of few in the library that can be used without a successful call to **gsasl\_init()**.

**err** : libgsasl error code

**Returns** : Returns a pointer to a statically allocated string containing an explanation of the error code *err*.

**gsasl\_strerror\_name ()**

```
const char *      gsasl_strerror_name      (int err);
```

Convert return code to human readable string representing the error code symbol itself. For example, `gsasl_strerror_name(GSASL_OK)` returns the string "GSASL\_OK".

This string can be used to output a diagnostic message to the user.

This function is one of few in the library that can be used without a successful call to `gsasl_init()`.

**err** : libgsasl error code

**Returns** : Returns a pointer to a statically allocated string containing a string version of the error code *err*, or NULL if the error code is not known.

Since 0.2.29

**gsasl\_saslprep ()**

```
int              gsasl_saslprep            (const char *in,
                                           Gsasl_saslprep_flags flags,
                                           char **out,
                                           int *stringprepc);
```

Prepare string using SASLprep. On success, the *out* variable must be deallocated by the caller.

**in** : a UTF-8 encoded string.

**flags** : any SASLprep flag, e.g., `GSASL_ALLOW_UNASSIGNED`.

**out** : on exit, contains newly allocated output string.

**stringprepc** : if non-NULL, will hold precise stringprep return code.

**Returns** : Returns `GSASL_OK` on success, or `GSASL_SASLPREP_ERROR` on error.

Since 0.2.3

**gsasl\_simple\_getpass ()**

```
int              gsasl_simple_getpass      (const char *filename,
                                           const char *username,
                                           char **key);
```

Retrieve password for user from specified file. The buffer *key* contain the password if this function is successful. The caller is responsible for deallocating it.

The file should be on the UoW "MD5 Based Authentication" format, which means it is in text format with comments denoted by # first on the line, with user entries looking as "usernameTABpassword". This function removes CR and LF at the end of lines before processing. TAB, CR, and LF denote ASCII values 9, 13, and 10, respectively.

**filename** : filename of file containing passwords.

**username** : username string.

**key** : newly allocated output character array.

**Returns** : Return `GSASL_OK` if output buffer contains the password, `GSASL_AUTHENTICATION_ERROR` if the user could not be found, or other error code.



**gsasl\_base64\_to ()**

```
int                gsasl_base64_to                (const char *in,
                                                    size_t inlen,
                                                    char **out,
                                                    size_t *outlen);
```

Encode data as base64. The string is zero terminated, and *outlen* holds the length excluding the terminating zero. The *out* buffer must be deallocated by the caller.

***in*** : input byte array

***inlen*** : size of input byte array

***out*** : pointer to newly allocated output byte array

***outlen*** : pointer to size of newly allocated output byte array

**Returns** : Returns **GSASL\_OK** on success, or **GSASL\_MALLOC\_ERROR** if input was too large or memory allocation fail.

Since 0.2.2

**gsasl\_base64\_from ()**

```
int                gsasl_base64_from              (const char *in,
                                                    size_t inlen,
                                                    char **out,
                                                    size_t *outlen);
```

Decode Base64 data. The *out* buffer must be deallocated by the caller.

***in*** : input byte array

***inlen*** : size of input byte array

***out*** : pointer to newly allocated output byte array

***outlen*** : pointer to size of newly allocated output byte array

**Returns** : Returns **GSASL\_OK** on success, **GSASL\_BASE64\_ERROR** if input was invalid, and **GSASL\_MALLOC\_ERROR** on memory allocation errors.

Since 0.2.2

**gsasl\_nonce ()**

```
int                gsasl_nonce                    (char *data,
                                                    size_t datalen);
```

Store unpredictable data of given size in the provided buffer.

***data*** : output array to be filled with unpredictable random data.

***datalen*** : size of output array.

**Returns** : Returns **GSASL\_OK** iff successful.

**gsasl\_random ()**

```
int                gsasl_random                (char *data,  
                                                size_t datalen);
```

Store cryptographically strong random data of given size in the provided buffer.

**data** : output array to be filled with strong random data.

**datalen** : size of output array.

**Returns** : Returns **GSASL\_OK** iff successful.

**gsasl\_md5 ()**

```
int                gsasl_md5                  (const char *in,  
                                                size_t inlen,  
                                                char *out[16]);
```

Compute hash of data using MD5. The *out* buffer must be deallocated by the caller.

**in** : input character array of data to hash.

**inlen** : length of input character array of data to hash.

**out** : newly allocated character array with hash of data.

**Returns** : Returns **GSASL\_OK** iff successful.

**gsasl\_hmac\_md5 ()**

```
int                gsasl_hmac_md5             (const char *key,  
                                                size_t keylen,  
                                                const char *in,  
                                                size_t inlen,  
                                                char *outhash[16]);
```

Compute keyed checksum of data using HMAC-MD5. The *outhash* buffer must be deallocated by the caller.

**key** : input character array with key to use.

**keylen** : length of input character array with key to use.

**in** : input character array of data to hash.

**inlen** : length of input character array of data to hash.

**outhash** : newly allocated character array with keyed hash of data.

**Returns** : Returns **GSASL\_OK** iff successful.

**gsasl\_sha1 ()**

```
int                gsasl_sha1                (const char *in,
                                              size_t inlen,
                                              char *out[20]);
```

Compute hash of data using SHA1. The *out* buffer must be deallocated by the caller.

**in** : input character array of data to hash.

**inlen** : length of input character array of data to hash.

**out** : newly allocated character array with hash of data.

**Returns** : Returns **GSASL\_OK** iff successful.

Since 1.3

**gsasl\_hmac\_sha1 ()**

```
int                gsasl_hmac_sha1           (const char *key,
                                              size_t keylen,
                                              const char *in,
                                              size_t inlen,
                                              char *outhash[20]);
```

Compute keyed checksum of data using HMAC-SHA1. The *outhash* buffer must be deallocated by the caller.

**key** : input character array with key to use.

**keylen** : length of input character array with key to use.

**in** : input character array of data to hash.

**inlen** : length of input character array of data to hash.

**outhash** : newly allocated character array with keyed hash of data.

**Returns** : Returns **GSASL\_OK** iff successful.

Since 1.3

**gsasl\_free ()**

```
void                gsasl_free               (void *ptr);
```

Invoke `free(ptr)` to de-allocate memory pointer. Typically used on strings allocated by other libgsasl functions.

This is useful on Windows where libgsasl is linked to one CRT and the application is linked to another CRT. Then `malloc/free` will not use the same heap. This happens if you build libgsasl using mingw32 and the application with Visual Studio.

**ptr** : memory pointer

Since 0.2.19

## 1.2 gsasl-mech

gsasl-mech —

## Synopsis

```

int          (*Gsasl_init_function)          (Gsasl *ctx);
void         (*Gsasl_done_function)          (Gsasl *ctx);
int          (*Gsasl_start_function)         (Gsasl_session *sctx,
void **mech_data);
int          (*Gsasl_step_function)          (Gsasl_session *sctx,
void *mech_data,
const char *input,
size_t input_len,
char **output,
size_t *output_len);
void         (*Gsasl_finish_function)        (Gsasl_session *sctx,
void *mech_data);
int          (*Gsasl_code_function)          (Gsasl_session *sctx,
void *mech_data,
const char *input,
size_t input_len,
char **output,
size_t *output_len);

typedef      Gsasl_mechanism_functions;
typedef      Gsasl_mechanism;
int          gsasl_register                  (Gsasl *ctx,
const Gsasl_mechanism *mech);

```

## Description

### Details

#### Gsasl\_init\_function ()

```

int          (*Gsasl_init_function)          (Gsasl *ctx);

```

**ctx :**

**Returns :**

#### Gsasl\_done\_function ()

```

void         (*Gsasl_done_function)          (Gsasl *ctx);

```

**ctx :**

#### Gsasl\_start\_function ()

```

int          (*Gsasl_start_function)         (Gsasl_session *sctx,
void **mech_data);

```

**sctx :**

**mech\_data :**

**Returns :**

**Gsasl\_step\_function ()**

```
int (*Gsasl_step_function) (Gsasl_session *sctx,  
                             void *mech_data,  
                             const char *input,  
                             size_t input_len,  
                             char **output,  
                             size_t *output_len);
```

**sctx :**

**mech\_data :**

**input :**

**input\_len :**

**output :**

**output\_len :**

**Returns :**

**Gsasl\_finish\_function ()**

```
void (*Gsasl_finish_function) (Gsasl_session *sctx,  
                                void *mech_data);
```

**sctx :**

**mech\_data :**

**Gsasl\_code\_function ()**

```
int (*Gsasl_code_function) (Gsasl_session *sctx,  
                             void *mech_data,  
                             const char *input,  
                             size_t input_len,  
                             char **output,  
                             size_t *output_len);
```

**sctx :**

**mech\_data :**

**input :**

**input\_len :**

**output :**

**output\_len :**

**Returns :**

**Gsasl\_mechanism\_functions**

```
typedef struct Gsasl_mechanism_functions Gsasl_mechanism_functions;
```

**Gsasl\_mechanism**

```
typedef struct Gsasl_mechanism Gsasl_mechanism;
```

**gsasl\_register ()**

```
int                gsasl_register                (Gsasl *ctx,
                                                const Gsasl_mechanism *mech);
```

This function initialize given mechanism, and if successful, add it to the list of plugins that is used by the library.

**ctx** : pointer to libgsasl handle.

**mech** : plugin structure with information about plugin.

**Returns** : **GSASL\_OK** iff successful, otherwise **GSASL\_MALLOC\_ERROR**.

Since 0.2.0

**1.3 gsasl-compat**

gsasl-compat —

**Synopsis**

```
int                gsasl_client_listmech        (Gsasl *ctx,
                                                char *out,
                                                size_t *outlen);
int                gsasl_server_listmech       (Gsasl *ctx,
                                                char *out,
                                                size_t *outlen);
int                gsasl_client_step           (Gsasl_session *sctx,
                                                const char *input,
                                                size_t input_len,
                                                char *output,
                                                size_t *output_len);
int                gsasl_client_step_base64    (Gsasl_session *sctx,
                                                const char *b64input,
                                                char *b64output,
                                                size_t b64output_len);
int                gsasl_server_step           (Gsasl_session *sctx,
                                                const char *input,
                                                size_t input_len,
                                                char *output,
                                                size_t *output_len);
int                gsasl_server_step_base64   (Gsasl_session *sctx,
                                                const char *b64input,
                                                char *b64output,
                                                size_t b64output_len);
void               gsasl_client_finish         (Gsasl_session *sctx);
void               gsasl_server_finish         (Gsasl_session *sctx);
Gsasl *            gsasl_client_ctx_get       (Gsasl_session *sctx);
Gsasl *            gsasl_server_ctx_get       (Gsasl_session *sctx);
```

---

void	gsasl_client_application_data_set	(Gsasl_session *sctx, void *application_data);
void *	gsasl_client_application_data_get	(Gsasl_session *sctx);
void	gsasl_server_application_data_set	(Gsasl_session *sctx, void *application_data);
void *	gsasl_server_application_data_get	(Gsasl_session *sctx);
int	gsasl_randomize	(int strong, char *data, size_t datalen);
Gsasl *	gsasl_ctx_get	(Gsasl_session *sctx);
int	gsasl_encode_inline	(Gsasl_session *sctx, const char *input, size_t input_len, char *output, size_t *output_len);
int	gsasl_decode_inline	(Gsasl_session *sctx, const char *input, size_t input_len, char *output, size_t *output_len);
void	gsasl_application_data_set	(Gsasl *ctx, void *appdata);
void *	gsasl_application_data_get	(Gsasl *ctx);
void	gsasl_appinfo_set	(Gsasl_session *sctx, void *appdata);
void *	gsasl_appinfo_get	(Gsasl_session *sctx);
const char *	gsasl_server_suggest_mechanism	(Gsasl *ctx, const char *mechlist);
int	gsasl_base64_encode	(char const *src, size_t srclength, char *target, size_t targsize);
int	gsasl_base64_decode	(char const *src, char *target, size_t targsize);
char *	gsasl_stringprep_nfkc	(const char *in, ssize_t len);
char *	gsasl_stringprep_saslprep	(const char *in, int *stringprep_rc);
char *	gsasl_stringprep_trace	(const char *in, int *stringprep_rc);
int	gsasl_md5pwd_get_password	(const char *filename, const char *username, char *key, size_t *keylen);
int	(*Gsasl_client_callback_anonymous)	(Gsasl_session *sctx, char *out, size_t *outlen);
int	(*Gsasl_client_callback_authentication_id)	(Gsasl_session *sctx, char *out, size_t *outlen);
int	(*Gsasl_client_callback_authorization_id)	(Gsasl_session *sctx, char *out, size_t *outlen);
int	(*Gsasl_client_callback_password)	(Gsasl_session *sctx,

---

---

		char *out, size_t *outlen);
int	(*Gssasl_client_callback_passcode)	(Gssasl_session *sctx, char *out, size_t *outlen);
int	(*Gssasl_client_callback_pin)	(Gssasl_session *sctx, char *suggestion, char *out, size_t *outlen);
int	(*Gssasl_client_callback_service)	(Gssasl_session *sctx, char *service, size_t *servicelen, char *hostname, size_t *hostnamelen, char *servicename, size_t *servicenamelen);
Gssasl_qop	(*Gssasl_client_callback_qop)	(Gssasl_session *sctx, Gssasl_qop serverqops);
size_t	(*Gssasl_client_callback_maxbuf)	(Gssasl_session *sctx, size_t servermaxbuf);
int	(*Gssasl_client_callback_realm)	(Gssasl_session *sctx, char *out, size_t *outlen);
int	(*Gssasl_server_callback_retrieve)	(Gssasl_session *sctx, const char *authentication_id, const char *authorization_id, const char *realm, char *key, size_t *keylen);
int	(*Gssasl_server_callback_validate)	(Gssasl_session *sctx, const char *authorization_id, const char *authentication_id, const char *password);
int	(*Gssasl_server_callback_gssapi)	(Gssasl_session *sctx, const char *clientname, const char *authentication_id);
int	(*Gssasl_server_callback_secured)	(Gssasl_session *sctx, const char *authentication_id, const char *authorization_id, const char *passcode, char *pin, char *suggestpin, size_t *suggestpinlen);
int	(*Gssasl_server_callback_cram_md5)	(Gssasl_session *sctx, char *username, char *challenge, char *response);
int	(*Gssasl_server_callback_digest_md5)	(Gssasl_session *sctx, char *username, char *realm, char *secrethash);
int	(*Gssasl_server_callback_service)	(Gssasl_session *sctx, char *service, size_t *servicelen, char *hostname, size_t *hostnamelen);
int	(*Gssasl_server_callback_external)	(Gssasl_session *sctx);

---



---

```

int                (*Gsasl_server_callback_anonymous) (Gsasl_session *sctx,
                                                         const char *token);
int                (*Gsasl_server_callback_realm)     (Gsasl_session *sctx,
                                                         char *out,
                                                         size_t *outlen,
                                                         size_t nth);
Gsasl_qop          (*Gsasl_server_callback_qop)      (Gsasl_session *sctx);
size_t            (*Gsasl_server_callback_maxbuf)    (Gsasl_session *sctx);
Gsasl_cipher       (*Gsasl_server_callback_cipher)   (Gsasl_session *sctx);
void              gsasl_client_callback_authorization_id_set
                                                         (Gsasl *ctx,
                                                         Gsasl_client_callback_authorization_id cb);
Gsasl_client_callback_authorization_id gsasl_client_callback_authorization_id_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_authentication_id_set
                                                         (Gsasl *ctx,
                                                         Gsasl_client_callback_authentication_id cb);
Gsasl_client_callback_authentication_id gsasl_client_callback_authentication_id_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_anonymous_set (Gsasl *ctx,
                                                         Gsasl_client_callback_anonymous cb);
Gsasl_client_callback_anonymous gsasl_client_callback_anonymous_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_password_set  (Gsasl *ctx,
                                                         Gsasl_client_callback_password cb);
Gsasl_client_callback_password gsasl_client_callback_password_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_passcode_set  (Gsasl *ctx,
                                                         Gsasl_client_callback_passcode cb);
Gsasl_client_callback_passcode gsasl_client_callback_passcode_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_pin_set       (Gsasl *ctx,
                                                         Gsasl_client_callback_pin cb);
Gsasl_client_callback_pin gsasl_client_callback_pin_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_service_set   (Gsasl *ctx,
                                                         Gsasl_client_callback_service cb);
Gsasl_client_callback_service gsasl_client_callback_service_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_qop_set       (Gsasl *ctx,
                                                         Gsasl_client_callback_qop cb);
Gsasl_client_callback_qop gsasl_client_callback_qop_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_maxbuf_set    (Gsasl *ctx,
                                                         Gsasl_client_callback_maxbuf cb);
Gsasl_client_callback_maxbuf gsasl_client_callback_maxbuf_get
                                                         (Gsasl *ctx);
void              gsasl_client_callback_realm_set     (Gsasl *ctx,
                                                         Gsasl_client_callback_realm cb);
Gsasl_client_callback_realm gsasl_client_callback_realm_get
                                                         (Gsasl *ctx);
void              gsasl_server_callback_validate_set  (Gsasl *ctx,
                                                         Gsasl_server_callback_validate cb);
Gsasl_server_callback_validate gsasl_server_callback_validate_get
                                                         (Gsasl *ctx);
void              gsasl_server_callback_retrieve_set  (Gsasl *ctx,
                                                         Gsasl_server_callback_retrieve cb);

```

---

```

Gsasl_server_callback_retrieve  gsasl_server_callback_retrieve_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_cram_md5_set  (Gsasl *ctx,
                                Gsasl_server_callback_cram_md5 cb);
Gsasl_server_callback_cram_md5 gsasl_server_callback_cram_md5_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_digest_md5_set
                                (Gsasl *ctx,
                                Gsasl_server_callback_digest_md5 cb);
Gsasl_server_callback_digest_md5 gsasl_server_callback_digest_md5_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_external_set  (Gsasl *ctx,
                                Gsasl_server_callback_external cb);
Gsasl_server_callback_external gsasl_server_callback_external_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_anonymous_set  (Gsasl *ctx,
                                Gsasl_server_callback_anonymous cb);
Gsasl_server_callback_anonymous gsasl_server_callback_anonymous_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_realm_set      (Gsasl *ctx,
                                Gsasl_server_callback_realm cb);
Gsasl_server_callback_realm     gsasl_server_callback_realm_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_qop_set       (Gsasl *ctx,
                                Gsasl_server_callback_qop cb);
Gsasl_server_callback_qop       gsasl_server_callback_qop_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_maxbuf_set    (Gsasl *ctx,
                                Gsasl_server_callback_maxbuf cb);
Gsasl_server_callback_maxbuf     gsasl_server_callback_maxbuf_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_cipher_set    (Gsasl *ctx,
                                Gsasl_server_callback_cipher cb);
Gsasl_server_callback_cipher     gsasl_server_callback_cipher_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_securid_set   (Gsasl *ctx,
                                Gsasl_server_callback_securid cb);
Gsasl_server_callback_securid    gsasl_server_callback_securid_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_gssapi_set    (Gsasl *ctx,
                                Gsasl_server_callback_gssapi cb);
Gsasl_server_callback_gssapi     gsasl_server_callback_gssapi_get
                                (Gsasl *ctx);
void                            gsasl_server_callback_service_set   (Gsasl *ctx,
                                Gsasl_server_callback_service cb);
Gsasl_server_callback_service    gsasl_server_callback_service_get
                                (Gsasl *ctx);

```

## Description

## Details

### gsasl\_client\_listmech ()

int	gsasl_client_listmech	(Gsasl *ctx, char *out,
-----	-----------------------	----------------------------

```
size_t *outlen);
```

**Warning**

`gsasl_client_listmech` is deprecated and should not be used in newly-written code. Use `gsasl_client_mechlist()` instead.

Write SASL names, separated by space, of mechanisms supported by the libgsasl client to the output array. To find out how large the output array must be, call this function with a NULL `out` parameter.

**ctx** : libgsasl handle.

**out** : output character array.

**outlen** : input maximum size of output character array, on output contains actual length of output array.

**Returns** : Returns `GSASL_OK` if successful, or error code.

**gsasl\_server\_listmech ()**

```
int                gsasl_server_listmech                (Gsasl *ctx,
                                                         char *out,
                                                         size_t *outlen);
```

**Warning**

`gsasl_server_listmech` is deprecated and should not be used in newly-written code. Use `gsasl_server_mechlist()` instead.

Write SASL names, separated by space, of mechanisms supported by the libgsasl server to the output array. To find out how large the output array must be, call this function with a NULL `out` parameter.

**ctx** : libgsasl handle.

**out** : output character array.

**outlen** : input maximum size of output character array, on output contains actual length of output array.

**Returns** : Returns `GSASL_OK` if successful, or error code.

**gsasl\_client\_step ()**

```
int                gsasl_client_step                    (Gsasl_session *sctx,
                                                         const char *input,
                                                         size_t input_len,
                                                         char *output,
                                                         size_t *output_len);
```

**Warning**

`gsasl_client_step` is deprecated and should not be used in newly-written code. Use `gsasl_step()` instead.

Perform one step of SASL authentication in client. This reads data from server (specified with `input` and `input_len`), processes it (potentially invoking callbacks to the application), and writes data to server (into variables `output` and `output_len`).

The contents of the output buffer is unspecified if this functions returns anything other than **GSASL\_NEEDS\_MORE**.

**sctx** : libgsasl client handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if authenticated terminated successfully, **GSASL\_NEEDS\_MORE** if more data is needed, or error code.

### gsasl\_client\_step\_base64 ()

```
int                gsasl_client_step_base64      (Gsasl_session *sctx,
                                                  const char *b64input,
                                                  char *b64output,
                                                  size_t b64output_len);
```



#### Warning

`gsasl_client_step_base64` is deprecated and should not be used in newly-written code. Use `gsasl_step64()` instead.

This is a simple wrapper around `gsasl_client_step()` that base64 decodes the input and base64 encodes the output.

**sctx** : libgsasl client handle.

**b64input** : input base64 encoded byte array.

**b64output** : output base64 encoded byte array.

**b64output\_len** : size of output base64 encoded byte array.

**Returns** : See `gsasl_client_step()`.

### gsasl\_server\_step ()

```
int                gsasl_server_step            (Gsasl_session *sctx,
                                                  const char *input,
                                                  size_t input_len,
                                                  char *output,
                                                  size_t *output_len);
```



#### Warning

`gsasl_server_step` is deprecated and should not be used in newly-written code. Use `gsasl_step()` instead.

Perform one step of SASL authentication in server. This reads data from client (specified with `input` and `input_len`), processes it (potentially invoking callbacks to the application), and writes data to client (into variables `output` and `output_len`).

The contents of the output buffer is unspecified if this functions returns anything other than **GSASL\_NEEDS\_MORE**.

**sctx** : libgsasl server handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if authenticated terminated successfully, **GSASL\_NEEDS\_MORE** if more data is needed, or error code.

### gsasl\_server\_step\_base64 ()

```
int                gsasl_server_step_base64      (Gsasl_session *sctx,
                                                  const char *b64input,
                                                  char *b64output,
                                                  size_t b64output_len);
```



#### Warning

`gsasl_server_step_base64` is deprecated and should not be used in newly-written code. Use `gsasl_step64()` instead.

This is a simple wrapper around `gsasl_server_step()` that base64 decodes the input and base64 encodes the output.

**sctx** : libgsasl server handle.

**b64input** : input base64 encoded byte array.

**b64output** : output base64 encoded byte array.

**b64output\_len** : size of output base64 encoded byte array.

**Returns** : See `gsasl_server_step()`.

### gsasl\_client\_finish ()

```
void                gsasl_client_finish          (Gsasl_session *sctx);
```



#### Warning

`gsasl_client_finish` is deprecated and should not be used in newly-written code. Use `gsasl_finish()` instead.

Destroy a libgsasl client handle. The handle must not be used with other libgsasl functions after this call.

**sctx** : libgsasl client handle.

**gsasl\_server\_finish ()**

```
void gsasl_server_finish (Gsasl_session *sctx);
```

**Warning**

`gsasl_server_finish` is deprecated and should not be used in newly-written code. Use `gsasl_finish()` instead.

---

Destroy a libgsasl server handle. The handle must not be used with other libgsasl functions after this call.

**sctx** : libgsasl server handle.

**gsasl\_client\_ctx\_get ()**

```
Gsasl * gsasl_client_ctx_get (Gsasl_session *sctx);
```

**Warning**

`gsasl_client_ctx_get` is deprecated and should not be used in newly-written code. This function is not useful with the new 0.2.0 API.

---

Get the libgsasl handle given a libgsasl client handle.

**sctx** : libgsasl client handle

**Returns** : Returns the libgsasl handle given a libgsasl client handle.

**gsasl\_server\_ctx\_get ()**

```
Gsasl * gsasl_server_ctx_get (Gsasl_session *sctx);
```

**Warning**

`gsasl_server_ctx_get` is deprecated and should not be used in newly-written code. This function is not useful with the new 0.2.0 API.

---

Get the libgsasl handle given a libgsasl server handle.

**sctx** : libgsasl server handle

**Returns** : Returns the libgsasl handle given a libgsasl server handle.

---

**gsasl\_client\_application\_data\_set ()**

```
void                gsasl_client_application_data_set    (Gsasl_session *sctx,  
                                                         void *application_data);
```

**Warning**

`gsasl_client_application_data_set` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_set()` or `gsasl_session_hook_set()` instead.

---

Store application specific data in the libgsasl client handle. The application data can be later (for instance, inside a callback) be retrieved by calling `gsasl_client_application_data_get()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl client handle.

**application\_data** : opaque pointer to application specific data.

**gsasl\_client\_application\_data\_get ()**

```
void *              gsasl_client_application_data_get    (Gsasl_session *sctx);
```

**Warning**

`gsasl_client_application_data_get` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_get()` or `gsasl_session_hook_get()` instead.

---

Retrieve application specific data from libgsasl client handle. The application data is set using `gsasl_client_application_data_set()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl client handle.

**Returns** : Returns the application specific data, or NULL.

**gsasl\_server\_application\_data\_set ()**

```
void                gsasl_server_application_data_set    (Gsasl_session *sctx,  
                                                         void *application_data);
```

**Warning**

`gsasl_server_application_data_set` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_set()` or `gsasl_session_hook_set()` instead.

---

Store application specific data in the libgsasl server handle. The application data can be later (for instance, inside a callback) be retrieved by calling `gsasl_server_application_data_get()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl server handle.

**application\_data** : opaque pointer to application specific data.

---

**gsasl\_server\_application\_data\_get ()**

```
void *          gsasl_server_application_data_get    (Gsasl_session *sctx);
```

**Warning**

`gsasl_server_application_data_get` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_get()` or `gsasl_session_hook_get()` instead.

Retrieve application specific data from libgsasl server handle. The application data is set using `gsasl_server_application_data_set()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl server handle.

**Returns** : Returns the application specific data, or NULL.

**gsasl\_randomize ()**

```
int          gsasl_randomize          (int strong,
                                       char *data,
                                       size_t datalen);
```

**Warning**

`gsasl_randomize` is deprecated and should not be used in newly-written code. Use `gsasl_random()` or `gsasl_nonce()` instead.

Store cryptographically random data of given size in the provided buffer.

**strong** : 0 iff operation should not block, non-0 for very strong randomness.

**data** : output array to be filled with random data.

**datalen** : size of output array.

**Returns** : Returns `GSASL_OK` iff successful.

**gsasl\_ctx\_get ()**

```
Gsasl *          gsasl_ctx_get          (Gsasl_session *sctx);
```

**Warning**

`gsasl_ctx_get` is deprecated and should not be used in newly-written code. This function is not useful with the new 0.2.0 API.

Get the libgsasl handle given a libgsasl session handle.

**sctx** : libgsasl session handle

**Returns** : Returns the libgsasl handle given a libgsasl session handle.



**gsasl\_encode\_inline ()**

```
int                gsasl_encode_inline      (Gsasl_session *sctx,  
                                             const char *input,  
                                             size_t input_len,  
                                             char *output,  
                                             size_t *output_len);
```

**Warning**

`gsasl_encode_inline` is deprecated and should not be used in newly-written code. Use `gsasl_encode()` instead.

Encode data according to negotiated SASL mechanism. This might mean that data is integrity or privacy protected.

**sctx** : libgsasl session handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if encoding was successful, otherwise an error code.

Since 0.2.0

**gsasl\_decode\_inline ()**

```
int                gsasl_decode_inline      (Gsasl_session *sctx,  
                                             const char *input,  
                                             size_t input_len,  
                                             char *output,  
                                             size_t *output_len);
```

**Warning**

`gsasl_decode_inline` is deprecated and should not be used in newly-written code. Use `gsasl_decode()` instead.

Decode data according to negotiated SASL mechanism. This might mean that data is integrity or privacy protected.

**sctx** : libgsasl session handle.

**input** : input byte array.

**input\_len** : size of input byte array.

**output** : output byte array.

**output\_len** : size of output byte array.

**Returns** : Returns **GSASL\_OK** if encoding was successful, otherwise an error code.

Since 0.2.0

**gsasl\_application\_data\_set ()**

```
void                gsasl_application_data_set        (Gsasl *ctx,  
                                                    void *appdata);
```

**Warning**

`gsasl_application_data_set` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_set()` instead.

---

Store application specific data in the libgsasl handle. The application data can be later (for instance, inside a callback) be retrieved by calling `gsasl_application_data_get()`. It is normally used by the application to maintain state between the main program and the callback.

**ctx** : libgsasl handle.

**appdata** : opaque pointer to application specific data.

**gsasl\_application\_data\_get ()**

```
void *              gsasl_application_data_get        (Gsasl *ctx);
```

**Warning**

`gsasl_application_data_get` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_get()` instead.

---

Retrieve application specific data from libgsasl handle. The application data is set using `gsasl_application_data_set()`. It is normally used by the application to maintain state between the main program and the callback.

**ctx** : libgsasl handle.

**Returns** : Returns the application specific data, or NULL.

**gsasl\_appinfo\_set ()**

```
void                gsasl_appinfo_set                (Gsasl_session *sctx,  
                                                    void *appdata);
```

**Warning**

`gsasl_appinfo_set` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_set()` instead.

---

Store application specific data in the libgsasl session handle. The application data can be later (for instance, inside a callback) be retrieved by calling `gsasl_appinfo_get()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl session handle.

**appdata** : opaque pointer to application specific data.

---

**gsasl\_appinfo\_get ()**

```
void *          gsasl_appinfo_get          (Gsasl_session *sctx);
```

**Warning**

`gsasl_appinfo_get` is deprecated and should not be used in newly-written code. Use `gsasl_callback_hook_get()` instead.

Retrieve application specific data from libgsasl session handle. The application data is set using `gsasl_appinfo_set()`. It is normally used by the application to maintain state between the main program and the callback.

**sctx** : libgsasl session handle.

**Returns** : Returns the application specific data, or NULL.

**gsasl\_server\_suggest\_mechanism ()**

```
const char *    gsasl_server_suggest_mechanism  (Gsasl *ctx,  
                                                const char *mechlist);
```

**Warning**

`gsasl_server_suggest_mechanism` is deprecated and should not be used in newly-written code. This function was never useful, since it is the client that chose which mechanism to use.

Get name of "best" SASL mechanism supported by the libgsasl server which is present in the input string.

**ctx** : libgsasl handle.

**mechlist** : input character array with SASL mechanism names, separated by invalid characters (e.g. SPC).

**Returns** : Returns name of "best" SASL mechanism supported by the libgsasl server which is present in the input string.

**gsasl\_base64\_encode ()**

```
int             gsasl_base64_encode            (char const *src,  
                                                size_t srclength,  
                                                char *target,  
                                                size_t targsize);
```

**Warning**

`gsasl_base64_encode` is deprecated and should not be used in newly-written code. Use `gsasl_base64_to()` instead.

Encode data as base64. Converts characters, three at a time, starting at `src` into four base64 characters in the target area until the entire input buffer is encoded.

**src** : input byte array

**srclength** : size of input byte array

**target** : output byte array

**targsize** : size of output byte array

**Returns** : Returns the number of data bytes stored at the target, or -1 on error.

### gsasl\_base64\_decode ()

```
int                                gsasl_base64_decode        (char const *src,
                                                             char *target,
                                                             size_t targsize);
```



#### Warning

`gsasl_base64_decode` is deprecated and should not be used in newly-written code. Use `gsasl_base64_from()` instead.

Decode Base64 data. Skips all whitespace anywhere. Converts characters, four at a time, starting at (or after) `src` from Base64 numbers into three 8 bit bytes in the target area.

**src** : input byte array

**target** : output byte array

**targsize** : size of output byte array

**Returns** : Returns the number of data bytes stored at the target, or -1 on error.

### gsasl\_stringprep\_nfkc ()

```
char *                            gsasl_stringprep_nfkc      (const char *in,
                                                             ssize_t len);
```



#### Warning

`gsasl_stringprep_nfkc` is deprecated and should not be used in newly-written code. No replacement functionality in GNU SASL, use GNU Libidn instead. Note that in SASL, you most likely want to use SASLprep and not bare NFKC, see `gsasl_saslprep()`.

Converts a string into canonical form, standardizing such issues as whether a character with an accent is represented as a base character and combining accent or as a single precomposed character.

The normalization mode is NFKC (ALL COMPOSE). It standardizes differences that do not affect the text content, such as the above-mentioned accent representation. It standardizes the "compatibility" characters in Unicode, such as SUPERSCRIPT THREE to the standard forms (in this case DIGIT THREE). Formatting information may be lost but for most text operations such characters should be considered the same. It returns a result with composed forms rather than a maximally decomposed form.

**in** : a UTF-8 encoded string.

**len** : length of `str`, in bytes, or -1 if `str` is nul-terminated.

**Returns** : Return a newly allocated string, that is the NFKC normalized form of `str`, or NULL on error.

**gsasl\_stringprep\_saslprep ()**

```
char *          gsasl_stringprep_saslprep          (const char *in,
                                                    int *stringprep_rc);
```

**Warning**

`gsasl_stringprep_saslprep` is deprecated and should not be used in newly-written code. Use `gsasl_saslprep()` instead.

Process a Unicode string for comparison, according to the "SASLprep" stringprep profile. This function is intended to be used by Simple Authentication and Security Layer (SASL) mechanisms (such as PLAIN, CRAM-MD5, and DIGEST-MD5) as well as other protocols exchanging user names and/or passwords.

**in** : input ASCII or UTF-8 string with data to prepare according to SASLprep.

**stringprep\_rc** : pointer to output variable with stringprep error code, or NULL to indicate that you don't care about it.

**Returns** : Return a newly allocated string that is the "SASLprep" processed form of the input string, or NULL on error, in which case `stringprep_rc` contain the stringprep library error code.

**gsasl\_stringprep\_trace ()**

```
char *          gsasl_stringprep_trace          (const char *in,
                                                  int *stringprep_rc);
```

**Warning**

`gsasl_stringprep_trace` is deprecated and should not be used in newly-written code. No replacement functionality in GNU SASL, use GNU Libidn instead.

Process a Unicode string for use as trace information, according to the "trace" stringprep profile. The profile is designed for use with the SASL ANONYMOUS Mechanism.

**in** : input ASCII or UTF-8 string with data to prepare according to "trace".

**stringprep\_rc** : pointer to output variable with stringprep error code, or NULL to indicate that you don't care about it.

**Returns** : Return a newly allocated string that is the "trace" processed form of the input string, or NULL on error, in which case `stringprep_rc` contain the stringprep library error code.

**gsasl\_md5pwd\_get\_password ()**

```
int          gsasl_md5pwd_get_password          (const char *filename,
                                                  const char *username,
                                                  char *key,
                                                  size_t *keylen);
```

**Warning**

`gsasl_md5pwd_get_password` is deprecated and should not be used in newly-written code. Use `gsasl_simple_getpass()` instead.

Retrieve password for user from specified file. To find out how large the output array must be, call this function with out=NULL. The file should be on the UoW "MD5 Based Authentication" format, which means it is in text format with comments denoted by # first on the line, with user entries looking as "usernameTABpassword". This function removes CR and LF at the end of lines before processing. TAB, CR, and LF denote ASCII values 9, 13, and 10, respectively.

**filename** : filename of file containing passwords.

**username** : username string.

**key** : output character array.

**keylen** : input maximum size of output character array, on output contains actual length of output array.

**Returns** : Return GSASL\_OK if output buffer contains the password, GSASL\_AUTHENTICATION\_ERROR if the user could not be found, or other error code.

#### Gsasl\_client\_callback\_anonymous ()

```
int (*Gsasl_client_callback_anonymous) (Gsasl_session *sctx,  
                                         char *out,  
                                         size_t *outlen);
```

**sctx** :

**out** :

**outlen** :

**Returns** :

#### Gsasl\_client\_callback\_authentication\_id ()

```
int (*Gsasl_client_callback_authentication_id) (Gsasl_session *sctx,  
                                                  char *out,  
                                                  size_t *outlen);
```

**sctx** :

**out** :

**outlen** :

**Returns** :

#### Gsasl\_client\_callback\_authorization\_id ()

```
int (*Gsasl_client_callback_authorization_id) (Gsasl_session *sctx,  
                                                char *out,  
                                                size_t *outlen);
```

**sctx** :

**out** :

**outlen** :

**Returns** :

**Gsasl\_client\_callback\_password ()**

```
int (*Gsasl_client_callback_password) (Gsasl_session *sctx,  
                                       char *out,  
                                       size_t *outlen);
```

**sctx :**

**out :**

**outlen :**

**Returns :**

**Gsasl\_client\_callback\_passcode ()**

```
int (*Gsasl_client_callback_passcode) (Gsasl_session *sctx,  
                                       char *out,  
                                       size_t *outlen);
```

**sctx :**

**out :**

**outlen :**

**Returns :**

**Gsasl\_client\_callback\_pin ()**

```
int (*Gsasl_client_callback_pin) (Gsasl_session *sctx,  
                                   char *suggestion,  
                                   char *out,  
                                   size_t *outlen);
```

**sctx :**

**suggestion :**

**out :**

**outlen :**

**Returns :**

**Gsasl\_client\_callback\_service ()**

```
int (*Gsasl_client_callback_service) (Gsasl_session *sctx,  
                                       char *service,  
                                       size_t *servicelen,  
                                       char *hostname,  
                                       size_t *hostnamelen,  
                                       char *servicename,  
                                       size_t *servicenamelen);
```

**sctx :**

---

**service :**

**servicelen :**

**hostname :**

**hostnamelen :**

**servicename :**

**servicenamelen :**

**Returns :**

### Gsasl\_client\_callback\_qop ()

```
Gsasl_qop          (*Gsasl_client_callback_qop)      (Gsasl_session *sctx,  
                                                       Gsasl_qop serverqops);
```

**sctx :**

**serverqops :**

**Returns :**

### Gsasl\_client\_callback\_maxbuf ()

```
size_t            (*Gsasl_client_callback_maxbuf)    (Gsasl_session *sctx,  
                                                       size_t servermaxbuf);
```

**sctx :**

**servermaxbuf :**

**Returns :**

### Gsasl\_client\_callback\_realm ()

```
int               (*Gsasl_client_callback_realm)     (Gsasl_session *sctx,  
                                                       char *out,  
                                                       size_t *outlen);
```

**sctx :**

**out :**

**outlen :**

**Returns :**



**Gsasl\_server\_callback\_retrieve ()**

```
int (*Gsasl_server_callback_retrieve) (Gsasl_session *sctx,  
                                       const char *authentication_id,  
                                       const char *authorization_id,  
                                       const char *realm,  
                                       char *key,  
                                       size_t *keylen);
```

**sctx :**

**authentication\_id :**

**authorization\_id :**

**realm :**

**key :**

**keylen :**

**Returns :**

**Gsasl\_server\_callback\_validate ()**

```
int (*Gsasl_server_callback_validate) (Gsasl_session *sctx,  
                                       const char *authorization_id,  
                                       const char *authentication_id,  
                                       const char *password);
```

**sctx :**

**authorization\_id :**

**authentication\_id :**

**password :**

**Returns :**

**Gsasl\_server\_callback\_gssapi ()**

```
int (*Gsasl_server_callback_gssapi) (Gsasl_session *sctx,  
                                       const char *clientname,  
                                       const char *authentication_id);
```

**sctx :**

**clientname :**

**authentication\_id :**

**Returns :**

**Gsasl\_server\_callback\_secured ()**

```
int (*Gsasl_server_callback_secured) (Gsasl_session *sctx,  
                                       const char *authentication_id,  
                                       const char *authorization_id,  
                                       const char *passcode,  
                                       char *pin,  
                                       char *suggestpin,  
                                       size_t *suggestpinlen);
```

**sctx :**

**authentication\_id :**

**authorization\_id :**

**passcode :**

**pin :**

**suggestpin :**

**suggestpinlen :**

**Returns :**

**Gsasl\_server\_callback\_cram\_md5 ()**

```
int (*Gsasl_server_callback_cram_md5) (Gsasl_session *sctx,  
                                       char *username,  
                                       char *challenge,  
                                       char *response);
```

**sctx :**

**username :**

**challenge :**

**response :**

**Returns :**

**Gsasl\_server\_callback\_digest\_md5 ()**

```
int (*Gsasl_server_callback_digest_md5) (Gsasl_session *sctx,  
                                       char *username,  
                                       char *realm,  
                                       char *secrethash);
```

**sctx :**

**username :**

**realm :**

**secrethash :**

**Returns :**

**Gsasl\_server\_callback\_service ()**

```
int (*Gsasl_server_callback_service) (Gsasl_session *sctx,  
                                     char *service,  
                                     size_t *servicelen,  
                                     char *hostname,  
                                     size_t *hostnamelen);
```

**sctx :**

**service :**

**servicelen :**

**hostname :**

**hostnamelen :**

**Returns :**

**Gsasl\_server\_callback\_external ()**

```
int (*Gsasl_server_callback_external) (Gsasl_session *sctx);
```

**sctx :**

**Returns :**

**Gsasl\_server\_callback\_anonymous ()**

```
int (*Gsasl_server_callback_anonymous) (Gsasl_session *sctx,  
                                         const char *token);
```

**sctx :**

**token :**

**Returns :**

**Gsasl\_server\_callback\_realm ()**

```
int (*Gsasl_server_callback_realm) (Gsasl_session *sctx,  
                                     char *out,  
                                     size_t *outlen,  
                                     size_t nth);
```

**sctx :**

**out :**

**outlen :**

**nth :**

**Returns :**

**Gsasl\_server\_callback\_qop ()**

```
Gsasl_qop          (*Gsasl_server_callback_qop)      (Gsasl_session *sctx);
```

**sctx :****Returns :****Gsasl\_server\_callback\_maxbuf ()**

```
size_t            (*Gsasl_server_callback_maxbuf)    (Gsasl_session *sctx);
```

**sctx :****Returns :****Gsasl\_server\_callback\_cipher ()**

```
Gsasl_cipher      (*Gsasl_server_callback_cipher)    (Gsasl_session *sctx);
```

**sctx :****Returns :****gsasl\_client\_callback\_authorization\_id\_set ()**

```
void              gsasl_client_callback_authorization_id_set
                  (Gsasl *ctx,
                   Gsasl_client_callback_authorization_id ←
                   cb);
```

**Warning**

`gsasl_client_callback_authorization_id_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the authorization identity. The function can be later retrieved using `gsasl_client_callback_authorization_id_get()`.

**ctx :** libgsasl handle.**cb :** callback function

**gsasl\_client\_callback\_authorization\_id\_get ()**

```
Gsasl_client_callback_authorization_id  gsasl_client_callback_authorization_id_get
                                         (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_authorization_id_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_authorization_id_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_authorization_id_set()`.

**gsasl\_client\_callback\_authentication\_id\_set ()**

```
void                                     gsasl_client_callback_authentication_id_set
                                         (Gsasl *ctx,
                                          Gsasl_client_callback_authentication_id cb);
```

**Warning**

`gsasl_client_callback_authentication_id_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the authentication identity. The function can be later retrieved using `gsasl_client_callback_authentication_id_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_authentication\_id\_get ()**

```
Gsasl_client_callback_authentication_id  gsasl_client_callback_authentication_id_get
                                         (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_authentication_id_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_authentication_id_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_authentication_id_set()`.

**gsasl\_client\_callback\_anonymous\_set ()**

```
void                gsasl_client_callback_anonymous_set (Gsasl *ctx,  
                                                         Gsasl_client_callback_anonymous cb ←  
                                                         );
```

**Warning**

`gsasl_client_callback_anonymous_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the anonymous token, which usually is the users email address. The function can be later retrieved using `gsasl_client_callback_anonymous_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_anonymous\_get ()**

```
Gsasl_client_callback_anonymous  gsasl_client_callback_anonymous_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_anonymous_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_anonymous_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_anonymous_set()`.

**gsasl\_client\_callback\_password\_set ()**

```
void                gsasl_client_callback_password_set (Gsasl *ctx,  
                                                         Gsasl_client_callback_password cb) ←  
                                                         ;
```

**Warning**

`gsasl_client_callback_password_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the password. The function can be later retrieved using `gsasl_client_callback_password_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_password\_get ()**

```
Gsasl_client_callback_password  gsasl_client_callback_password_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_password_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_password_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_password_set()`.

**gsasl\_client\_callback\_passcode\_set ()**

```
void                            gsasl_client_callback_passcode_set  (Gsasl *ctx,  
                                                                    Gsasl_client_callback_passcode cb) ←  
                                                                    ;
```

**Warning**

`gsasl_client_callback_passcode_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the passcode. The function can be later retrieved using `gsasl_client_callback_passcode_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_passcode\_get ()**

```
Gsasl_client_callback_passcode  gsasl_client_callback_passcode_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_passcode_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_passcode_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_passcode_set()`.

**gsasl\_client\_callback\_pin\_set ()**

```
void                gsasl_client_callback_pin_set      (Gsasl *ctx,  
                                                       Gsasl_client_callback_pin cb);
```

**Warning**

`gsasl_client_callback_pin_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to chose a new pin, possibly suggested by the server, for the SECURID mechanism. This is not normally invoked, but only when the server requests it. The function can be later retrieved using `gsasl_client_callback_pin_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_pin\_get ()**

```
Gsasl_client_callback_pin  gsasl_client_callback_pin_get  
                                                                    (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_pin_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_pin_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_pin_set()`.

**gsasl\_client\_callback\_service\_set ()**

```
void                gsasl_client_callback_service_set  (Gsasl *ctx,  
                                                       Gsasl_client_callback_service cb);
```

**Warning**

`gsasl_client_callback_service_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to set the name of the service. The service buffer should be a registered GSSAPI host-based service name, hostname the name of the server. Servicename is used by DIGEST-MD5 and should be the name of generic server in case of a replicated service. The function can be later retrieved using `gsasl_client_callback_service_get()`.

**ctx** : libgsasl handle.

**cb** : callback function



**gsasl\_client\_callback\_service\_get ()**

```
Gsasl_client_callback_service gsasl_client_callback_service_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_service_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_service_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_service_set()`.

**gsasl\_client\_callback\_qop\_set ()**

```
void gsasl_client_callback_qop_set (Gsasl *ctx,  
                                    Gsasl_client_callback_qop cb);
```

**Warning**

`gsasl_client_callback_qop_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to determine the qop to use after looking at what the server offered. The function can be later retrieved using `gsasl_client_callback_qop_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_qop\_get ()**

```
Gsasl_client_callback_qop gsasl_client_callback_qop_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_qop_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_qop_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_qop_set()`.

**gsasl\_client\_callback\_maxbuf\_set ()**

```
void                gsasl_client_callback_maxbuf_set    (Gsasl *ctx,  
                                                         Gsasl_client_callback_maxbuf cb);
```

**Warning**

`gsasl_client_callback_maxbuf_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to inform the server of the largest buffer the client is able to receive when using the DIGEST-MD5 "auth-int" or "auth-conf" Quality of Protection (qop). If this directive is missing, the default value 65536 will be assumed. The function can be later retrieved using `gsasl_client_callback_maxbuf_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_maxbuf\_get ()**

```
Gsasl_client_callback_maxbuf  gsasl_client_callback_maxbuf_get  
                              (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_maxbuf_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_maxbuf_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_maxbuf_set()`.

**gsasl\_client\_callback\_realm\_set ()**

```
void                gsasl_client_callback_realm_set    (Gsasl *ctx,  
                                                         Gsasl_client_callback_realm cb);
```

**Warning**

`gsasl_client_callback_realm_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the client to know which realm it belongs to. The realm is used by the server to determine which username and password to use. The function can be later retrieved using `gsasl_client_callback_realm_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_client\_callback\_realm\_get ()**

```
Gsasl_client_callback_realm  gsasl_client_callback_realm_get
                              (Gsasl *ctx);
```

**Warning**

`gsasl_client_callback_realm_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_client_callback_realm_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_client_callback_realm_set()`.

**gsasl\_server\_callback\_validate\_set ()**

```
void                          gsasl_server_callback_validate_set  (Gsasl *ctx,
                                                                    Gsasl_server_callback_validate cb) ←
                                                                    ;
```

**Warning**

`gsasl_server_callback_validate_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for deciding if user is authenticated using authentication identity, authorization identity and password. The function can be later retrieved using `gsasl_server_callback_validate_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_validate\_get ()**

```
Gsasl_server_callback_validate  gsasl_server_callback_validate_get
                              (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_validate_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_validate_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_validate_set()`.

**gsasl\_server\_callback\_retrieve\_set ()**

```
void                gsasl_server_callback_retrieve_set  (Gsasl *ctx,  
                                                         Gsasl_server_callback_retrieve cb) ←  
                                                         ;
```

**Warning**

`gsasl_server_callback_retrieve_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for deciding if user is authenticated using authentication identity, authorization identity and password. The function can be later retrieved using `gsasl_server_callback_retrieve_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_retrieve\_get ()**

```
Gsasl_server_callback_retrieve  gsasl_server_callback_retrieve_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_retrieve_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_retrieve_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_retrieve_set()`.

**gsasl\_server\_callback\_cram\_md5\_set ()**

```
void                gsasl_server_callback_cram_md5_set  (Gsasl *ctx,  
                                                         Gsasl_server_callback_cram_md5 cb) ←  
                                                         ;
```

**Warning**

`gsasl_server_callback_cram_md5_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for deciding if user is authenticated using CRAM-MD5 challenge and response. The function can be later retrieved using `gsasl_server_callback_cram_md5_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_cram\_md5\_get ()**

```
Gsasl_server_callback_cram_md5  gsasl_server_callback_cram_md5_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_cram_md5_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_cram_md5_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_cram_md5_set()`.

**gsasl\_server\_callback\_digest\_md5\_set ()**

```
void                                gsasl_server_callback_digest_md5_set  
                                (Gsasl *ctx,  
                                Gsasl_server_callback_digest_md5  ←  
                                cb);
```

**Warning**

`gsasl_server_callback_digest_md5_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for retrieving the secret hash of the username, realm and password for use in the DIGEST-MD5 mechanism. The function can be later retrieved using `gsasl_server_callback_digest_md5_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_digest\_md5\_get ()**

```
Gsasl_server_callback_digest_md5  gsasl_server_callback_digest_md5_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_digest_md5_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_digest_md5_set()`.

**ctx** : libgsasl handle.

**Returns** : Return the callback earlier set by calling `gsasl_server_callback_digest_md5_set()`.

**gsasl\_server\_callback\_external\_set ()**

```
void                gsasl_server_callback_external_set  (Gsasl *ctx,  
                                                         Gsasl_server_callback_external cb) ↵  
                                                         ;
```

**Warning**

`gsasl_server_callback_external_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for deciding if user is authenticated out of band. The function can be later retrieved using `gsasl_server_callback_external_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_external\_get ()**

```
Gsasl_server_callback_external  gsasl_server_callback_external_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_external_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_external_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_external_set()`.

**gsasl\_server\_callback\_anonymous\_set ()**

```
void                gsasl_server_callback_anonymous_set (Gsasl *ctx,  
                                                         Gsasl_server_callback_anonymous cb ↵  
                                                         );
```

**Warning**

`gsasl_server_callback_anonymous_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for deciding if user is permitted anonymous access. The function can be later retrieved using `gsasl_server_callback_anonymous_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_anonymous\_get ()**

```
Gsasl_server_callback_anonymous  gsasl_server_callback_anonymous_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_anonymous_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

---

Get the callback earlier set by calling `gsasl_server_callback_anonymous_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_anonymous_set()`.

**gsasl\_server\_callback\_realm\_set ()**

```
void                                gsasl_server_callback_realm_set    (Gsasl *ctx,  
                                                                    Gsasl_server_callback_realm cb);
```

**Warning**

`gsasl_server_callback_realm_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

---

Specify the callback function to use in the server to know which realm it serves. The realm is used by the user to determine which username and password to use. The function can be later retrieved using `gsasl_server_callback_realm_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_realm\_get ()**

```
Gsasl_server_callback_realm  gsasl_server_callback_realm_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_realm_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

---

Get the callback earlier set by calling `gsasl_server_callback_realm_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_realm_set()`.

---

**gsasl\_server\_callback\_qop\_set ()**

```
void                gsasl_server_callback_qop_set      (Gsasl *ctx,  
                                                       Gsasl_server_callback_qop cb);
```

**Warning**

`gsasl_server_callback_qop_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server to know which quality of protection it accepts. The quality of protection eventually used is selected by the client though. It is currently used by the DIGEST-MD5 mechanism. The function can be later retrieved using `gsasl_server_callback_qop_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_qop\_get ()**

```
Gsasl_server_callback_qop  gsasl_server_callback_qop_get  
                                                                    (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_qop_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_qop_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_qop_set()`.

**gsasl\_server\_callback\_maxbuf\_set ()**

```
void                gsasl_server_callback_maxbuf_set  (Gsasl *ctx,  
                                                       Gsasl_server_callback_maxbuf cb);
```

**Warning**

`gsasl_server_callback_maxbuf_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server to inform the client of the largest buffer the server is able to receive when using the DIGEST-MD5 "auth-int" or "auth-conf" Quality of Protection (qop). If this directive is missing, the default value 65536 will be assumed. The function can be later retrieved using `gsasl_server_callback_maxbuf_get()`.

**ctx** : libgsasl handle.

**cb** : callback function



**gsasl\_server\_callback\_maxbuf\_get ()**

```
Gsasl_server_callback_maxbuf  gsasl_server_callback_maxbuf_get
                               (Gsasl *ctx);
```

**Warning**

gsasl\_server\_callback\_maxbuf\_get is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses [gsasl\\_callback\\_set\(\)](#) to set the application callback, and uses [gsasl\\_callback\(\)](#) or [gsasl\\_property\\_get\(\)](#) to invoke the callback for certain properties.

---

Get the callback earlier set by calling [gsasl\\_server\\_callback\\_maxbuf\\_set\(\)](#).

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling [gsasl\\_server\\_callback\\_maxbuf\\_set\(\)](#).

**gsasl\_server\_callback\_cipher\_set ()**

```
void                          gsasl_server_callback_cipher_set  (Gsasl *ctx,
                                                                Gsasl_server_callback_cipher cb);
```

**Warning**

gsasl\_server\_callback\_cipher\_set is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses [gsasl\\_callback\\_set\(\)](#) to set the application callback, and uses [gsasl\\_callback\(\)](#) or [gsasl\\_property\\_get\(\)](#) to invoke the callback for certain properties.

---

Specify the callback function to use in the server to inform the client of the cipher suites supported. The DES and 3DES ciphers must be supported for interoperability. It is currently used by the DIGEST-MD5 mechanism. The function can be later retrieved using [gsasl\\_server\\_callback\\_cipher\\_get\(\)](#).

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_cipher\_get ()**

```
Gsasl_server_callback_cipher  gsasl_server_callback_cipher_get
                               (Gsasl *ctx);
```

**Warning**

gsasl\_server\_callback\_cipher\_get is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses [gsasl\\_callback\\_set\(\)](#) to set the application callback, and uses [gsasl\\_callback\(\)](#) or [gsasl\\_property\\_get\(\)](#) to invoke the callback for certain properties.

---

Get the callback earlier set by calling [gsasl\\_server\\_callback\\_cipher\\_set\(\)](#).

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling [gsasl\\_server\\_callback\\_cipher\\_set\(\)](#).

---

**gsasl\_server\_callback\_secured\_set ()**

```
void                gsasl_server_callback_secured_set    (Gsasl *ctx,  
                                                         Gsasl_server_callback_secured cb);
```

**Warning**

`gsasl_server_callback_secured_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for validating a user via the SECURID mechanism. The function should return `GSASL_OK` if user authenticated successfully, `GSASL_SECURID_SERVER_NEED_ADDITIONAL_PASSCODE` if it wants another passcode, `GSASL_SECURID_SERVER_NEED_NEW_PIN` if it wants a PIN change, or an error. When (and only when) `GSASL_SECURID_SERVER_NEED_NEW_PIN` is returned, `suggestpin` can be populated with a PIN code the server suggests, and `suggestpinlen` set to the length of the PIN. The function can be later retrieved using `gsasl_server_callback_secured_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_secured\_get ()**

```
Gsasl_server_callback_secured  gsasl_server_callback_secured_get  
                                (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_secured_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_secured_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_secured_set()`.

**gsasl\_server\_callback\_gssapi\_set ()**

```
void                gsasl_server_callback_gssapi_set    (Gsasl *ctx,  
                                                         Gsasl_server_callback_gssapi cb);
```

**Warning**

`gsasl_server_callback_gssapi_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server for checking if a GSSAPI user is authorized for username (by, e.g., calling `krb5_kuserok`). The function should return `GSASL_OK` if the user should be permitted access, or an error code such as `GSASL_AUTHENTICATION_ERROR` on failure. The function can be later retrieved using `gsasl_server_callback_gssapi_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_gssapi\_get ()**

```
Gsasl_server_callback_gssapi  gsasl_server_callback_gssapi_get
                               (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_gssapi_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_gssapi_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_gssapi_set()`.

**gsasl\_server\_callback\_service\_set ()**

```
void                          gsasl_server_callback_service_set  (Gsasl *ctx,
                                                                Gsasl_server_callback_service cb);
```

**Warning**

`gsasl_server_callback_service_set` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Specify the callback function to use in the server to set the name of the service. The service buffer should be a registered GSSAPI host-based service name, hostname the name of the server. The function can be later retrieved using `gsasl_server_callback_service_get()`.

**ctx** : libgsasl handle.

**cb** : callback function

**gsasl\_server\_callback\_service\_get ()**

```
Gsasl_server_callback_service  gsasl_server_callback_service_get
                               (Gsasl *ctx);
```

**Warning**

`gsasl_server_callback_service_get` is deprecated and should not be used in newly-written code. This function is part of the old callback interface. The new interface uses `gsasl_callback_set()` to set the application callback, and uses `gsasl_callback()` or `gsasl_property_get()` to invoke the callback for certain properties.

Get the callback earlier set by calling `gsasl_server_callback_service_set()`.

**ctx** : libgsasl handle.

**Returns** : Returns the callback earlier set by calling `gsasl_server_callback_service_set()`.

## Chapter 2

# Index

### G

Gsasl, 10  
GSASL\_API, 5  
gsasl\_appinfo\_get, 39  
gsasl\_appinfo\_set, 38  
gsasl\_application\_data\_get, 38  
gsasl\_application\_data\_set, 38  
gsasl\_base64\_decode, 40  
gsasl\_base64\_encode, 39  
gsasl\_base64\_from, 21  
gsasl\_base64\_to, 21  
gsasl\_callback, 13  
Gsasl\_callback\_function, 11  
gsasl\_callback\_hook\_get, 13  
gsasl\_callback\_hook\_set, 13  
gsasl\_callback\_set, 12  
gsasl\_check\_version, 12  
Gsasl\_cipher, 9  
gsasl\_client\_application\_data\_get, 35  
gsasl\_client\_application\_data\_set, 35  
Gsasl\_client\_callback\_anonymous, 42  
gsasl\_client\_callback\_anonymous\_get, 50  
gsasl\_client\_callback\_anonymous\_set, 50  
Gsasl\_client\_callback\_authentication\_id, 42  
gsasl\_client\_callback\_authentication\_id\_get, 49  
gsasl\_client\_callback\_authentication\_id\_set, 49  
Gsasl\_client\_callback\_authorization\_id, 42  
gsasl\_client\_callback\_authorization\_id\_get, 49  
gsasl\_client\_callback\_authorization\_id\_set, 48  
Gsasl\_client\_callback\_maxbuf, 44  
gsasl\_client\_callback\_maxbuf\_get, 54  
gsasl\_client\_callback\_maxbuf\_set, 54  
Gsasl\_client\_callback\_passcode, 43  
gsasl\_client\_callback\_passcode\_get, 51  
gsasl\_client\_callback\_passcode\_set, 51  
Gsasl\_client\_callback\_password, 43  
gsasl\_client\_callback\_password\_get, 51  
gsasl\_client\_callback\_password\_set, 50  
Gsasl\_client\_callback\_pin, 43  
gsasl\_client\_callback\_pin\_get, 52  
gsasl\_client\_callback\_pin\_set, 52  
Gsasl\_client\_callback\_qop, 44  
gsasl\_client\_callback\_qop\_get, 53  
gsasl\_client\_callback\_qop\_set, 53  
Gsasl\_client\_callback\_realm, 44  
gsasl\_client\_callback\_realm\_get, 55  
gsasl\_client\_callback\_realm\_set, 54  
Gsasl\_client\_callback\_service, 43  
gsasl\_client\_callback\_service\_get, 53  
gsasl\_client\_callback\_service\_set, 52  
gsasl\_client\_ctx\_get, 34  
gsasl\_client\_finish, 33  
gsasl\_client\_listmech, 30  
gsasl\_client\_mechlist, 16  
gsasl\_client\_start, 17  
gsasl\_client\_step, 31  
gsasl\_client\_step\_base64, 32  
gsasl\_client\_suggest\_mechanism, 16  
gsasl\_client\_support\_p, 16  
Gsasl\_code\_function, 25  
gsasl\_ctx\_get, 36  
gsasl\_decode, 19  
gsasl\_decode\_inline, 37  
gsasl\_done, 12  
Gsasl\_done\_function, 24  
gsasl\_encode, 18  
gsasl\_encode\_inline, 37  
gsasl\_finish, 18  
Gsasl\_finish\_function, 25  
gsasl\_free, 23  
gsasl\_hmac\_md5, 22  
gsasl\_hmac\_sha1, 23  
gsasl\_init, 12  
Gsasl\_init\_function, 24  
gsasl\_md5, 22  
gsasl\_md5pwd\_get\_password, 41  
Gsasl\_mechanism, 26  
Gsasl\_mechanism\_functions, 25  
gsasl\_mechanism\_name, 19  
gsasl\_nonce, 21  
Gsasl\_property, 10  
gsasl\_property\_fast, 15  
gsasl\_property\_get, 15  
gsasl\_property\_set, 14  
gsasl\_property\_set\_raw, 14  
Gsasl\_qop, 9

---

gsasl\_random, 22  
gsasl\_randomize, 36  
Gsasl\_rc, 6  
gsasl\_register, 26  
gsasl\_saslprep, 20  
Gsasl\_saslprep\_flags, 9  
gsasl\_server\_application\_data\_get, 36  
gsasl\_server\_application\_data\_set, 35  
Gsasl\_server\_callback\_anonymous, 47  
gsasl\_server\_callback\_anonymous\_get, 59  
gsasl\_server\_callback\_anonymous\_set, 58  
Gsasl\_server\_callback\_cipher, 48  
gsasl\_server\_callback\_cipher\_get, 61  
gsasl\_server\_callback\_cipher\_set, 61  
Gsasl\_server\_callback\_cram\_md5, 46  
gsasl\_server\_callback\_cram\_md5\_get, 57  
gsasl\_server\_callback\_cram\_md5\_set, 56  
Gsasl\_server\_callback\_digest\_md5, 46  
gsasl\_server\_callback\_digest\_md5\_get, 57  
gsasl\_server\_callback\_digest\_md5\_set, 57  
Gsasl\_server\_callback\_external, 47  
gsasl\_server\_callback\_external\_get, 58  
gsasl\_server\_callback\_external\_set, 58  
Gsasl\_server\_callback\_gssapi, 45  
gsasl\_server\_callback\_gssapi\_get, 63  
gsasl\_server\_callback\_gssapi\_set, 62  
Gsasl\_server\_callback\_maxbuf, 48  
gsasl\_server\_callback\_maxbuf\_get, 61  
gsasl\_server\_callback\_maxbuf\_set, 60  
Gsasl\_server\_callback\_qop, 48  
gsasl\_server\_callback\_qop\_get, 60  
gsasl\_server\_callback\_qop\_set, 60  
Gsasl\_server\_callback\_realm, 47  
gsasl\_server\_callback\_realm\_get, 59  
gsasl\_server\_callback\_realm\_set, 59  
Gsasl\_server\_callback\_retrieve, 45  
gsasl\_server\_callback\_retrieve\_get, 56  
gsasl\_server\_callback\_retrieve\_set, 56  
Gsasl\_server\_callback\_securid, 46  
gsasl\_server\_callback\_securid\_get, 62  
gsasl\_server\_callback\_securid\_set, 62  
Gsasl\_server\_callback\_service, 47  
gsasl\_server\_callback\_service\_get, 63  
gsasl\_server\_callback\_service\_set, 63  
Gsasl\_server\_callback\_validate, 45  
gsasl\_server\_callback\_validate\_get, 55  
gsasl\_server\_callback\_validate\_set, 55  
gsasl\_server\_ctx\_get, 34  
gsasl\_server\_finish, 34  
gsasl\_server\_listmech, 31  
gsasl\_server\_mechlist, 16  
gsasl\_server\_start, 17  
gsasl\_server\_step, 32  
gsasl\_server\_step\_base64, 33  
gsasl\_server\_suggest\_mechanism, 39  
gsasl\_server\_support\_p, 17  
Gsasl\_session, 10  
gsasl\_session\_hook\_get, 14  
gsasl\_session\_hook\_set, 14  
gsasl\_sha1, 23  
gsasl\_simple\_getpass, 20  
Gsasl\_start\_function, 24  
gsasl\_step, 17  
gsasl\_step64, 18  
Gsasl\_step\_function, 25  
gsasl\_strerror, 19  
gsasl\_strerror\_name, 20  
gsasl\_stringprep\_nfkc, 40  
gsasl\_stringprep\_saslprep, 41  
gsasl\_stringprep\_trace, 41  
GSASL\_VERSION, 6  
GSASL\_VERSION\_MAJOR, 6  
GSASL\_VERSION\_MINOR, 6  
GSASL\_VERSION\_NUMBER, 6  
GSASL\_VERSION\_PATCH, 6

---