## COLLABORATORS

<table>
<thead>
<tr>
<th>ACTION</th>
<th>NAME</th>
<th>DATE</th>
<th>SIGNATURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRITTEN BY</td>
<td>August 2, 2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## REVISION HISTORY

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>DATE</th>
<th>DESCRIPTION</th>
<th>NAME</th>
</tr>
</thead>
</table>
## GNU SASL API Reference Manual

1. **gsasl** .................................................. 3
2. **gsasl-mech** ........................................... 35
3. **gsasl-compat** ........................................... 37

## Index

1. **GNU SASL API Reference Manual** 1
   1.1 **gsasl** .................................................. 3
   1.2 **gsasl-mech** ........................................... 35
   1.3 **gsasl-compat** ........................................... 37

2. **Index** .................................................. 79
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.
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.
1.1 gsasl

gsasl —

Functions

<table>
<thead>
<tr>
<th>Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>int</td>
<td>(*Gsasl_callback_function) ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_init ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_done ()</td>
</tr>
<tr>
<td>const char *</td>
<td>gsasl_check_version ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_callback_set ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_callback ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_callback_hook_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_callback_hook_get ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_session_hook_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_session_hook_get ()</td>
</tr>
<tr>
<td>Function</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><code>void</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_property_set()</code></td>
<td></td>
</tr>
<tr>
<td><code>void</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_property_set_raw()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_property_get()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_property_fast()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_client_mechlist()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_client_support_p()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_client_suggest_mechanism()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_server_mechlist()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_server_support_p()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_client_start()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_server_start()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_step()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_step64()</code></td>
<td></td>
</tr>
<tr>
<td><code>void</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_finish()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_encode()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_decode()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_mechanism_name()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_strerror()</code></td>
<td></td>
</tr>
<tr>
<td><code>const char *</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_strerror_name()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_saslprep()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_simple_getpass()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_base64_to()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_base64_from()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_nonce()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_random()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_md5()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_hmac_md5()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_sha1()</code></td>
<td></td>
</tr>
<tr>
<td><code>int</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_hmac_sha1()</code></td>
<td></td>
</tr>
<tr>
<td><code>void</code></td>
<td></td>
</tr>
<tr>
<td><code>gsasl_free()</code></td>
<td></td>
</tr>
</tbody>
</table>

### Types and Values

```c
#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;
```

### Description

#### Functions

`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.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>session handle, may be NULL.</td>
</tr>
<tr>
<td>prop</td>
<td>enumerated value of Gsasl_property type.</td>
</tr>
</tbody>
</table>

**Returns**

Any valid return code, the interpretation of which depend on the `prop` value.

Since: 0.2.0

gasl_init()

```
int
gasl_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()`.

**Parameters**

| ctx | pointer to libgsasl handle. |

**Returns**

GSASL_OK iff successful, otherwise `GSASL_MALLOC_ERROR`.

gasl_done()

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

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

**Parameters**
gsasl_check_version ()

```c
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().

**Parameters**

- `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 ()

```c
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.

**Parameters**

- `ctx` handle received from gsasl_init().
- `cb` pointer to function implemented by application.

Since: 0.2.0

gsasl_callback ()

```c
int
gsasl_callback (Gsasl *ctx,
                Gsasl_session *sctx,
                Gsasl_property prop);
```
Invoke the application callback. The prop value indicates 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.

### Parameters

| 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()`

```c
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.

### Parameters

| ctx  | libgsasl handle. |
| hook | opaque pointer to application specific data. |

Since: 0.2.0

#### `gsasl_callback_hook_get()`

```c
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.

### Parameters
### gsasl_session_hook_set()

```c
void
gsasl_session_hook_set (Gsasl_session *sctx,
    void *hook);
```

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_session_hook_get()`. This is normally used by the application to maintain a per-session state between the main program and callbacks.

**Parameters**

- **sctx**
  - libgsasl session handle.

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

**Since:** 0.2.14

### gsasl_session_hook_get()

```c
void~*
gsasl_session_hook_get (Gsasl_session *sctx);
```

Retrieve application specific data from libgsasl session handle.

The application data is set using `gsasl_callback_hook_set()`. This is normally used by the application to maintain a per-session state between the main program and callbacks.

**Parameters**

- **sctx**
  - libgsasl session handle.

**Returns**

Returns the application specific data, or NULL.

**Since:** 0.2.14

### gsasl_property_set()

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

---
Make a copy of \textit{data} and store it in the session handle for the indicated property \textit{prop}.

You can immediately deallocate \textit{data} after calling this function, without affecting the data stored in the session handle.

\textbf{Parameters}

\begin{center}
\begin{tabular}{|l|}
\hline
\textbf{sctx} & session handle. \\
\textbf{prop} & enumerated value of \texttt{Gsasl\_property} type, indicating the type of data in \textit{data}. \\
\textbf{data} & zero terminated character string to store. \\
\hline
\end{tabular}
\end{center}

Since: 0.2.0

\texttt{gsasl\_property\_set\_raw ()}

\begin{verbatim}
void
gsasl\_property\_set\_raw (Gsasl\_session *sctx,
   Gsasl\_property prop,
   const char *data,
   size_t len);
\end{verbatim}

Make a copy of \textit{len} sized \textit{data} and store a zero terminated version of it in the session handle for the indicated property \textit{prop}.

You can immediately deallocate \textit{data} after calling this function, without affecting the data stored in the session handle.

Except for the length indicator, this function is identical to \texttt{gsasl\_property\_set}.

\textbf{Parameters}

\begin{center}
\begin{tabular}{|l|}
\hline
\textbf{sctx} & session handle. \\
\textbf{prop} & enumerated value of \texttt{Gsasl\_property} type, indicating the type of data in \textit{data}. \\
\textbf{data} & character string to store. \\
\textbf{len} & length of character string to store. \\
\hline
\end{tabular}
\end{center}

Since: 0.2.0

\texttt{gsasl\_property\_get ()}

\begin{verbatim}
const char*
gsasl\_property\_get (Gsasl\_session *sctx,
   Gsasl\_property prop);
\end{verbatim}

Retrieve the data stored in the session handle for given property \textit{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.

**Parameters**

<table>
<thead>
<tr>
<th>sctx</th>
<th>session handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>prop</td>
<td>enumerated value of Gsasl_property type, indicating the type of data in data.</td>
</tr>
</tbody>
</table>

**Returns**

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

Since: 0.2.0

---

### gsasl_property_fast ()

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>sctx</th>
<th>session handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>prop</td>
<td>enumerated value of Gsasl_property type, indicating the type of data in data.</td>
</tr>
</tbody>
</table>

**Returns**

Return property value, if known, or NULL if no value known.

Since: 0.2.0

---

### gsasl_client_mechlist ()

```c
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.
Parameters

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx</td>
<td>libgsasl handle.</td>
</tr>
<tr>
<td>out</td>
<td>newly allocated output character array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK if successful, or error code.

gasl_client_support_p ()

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

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

Parameters

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx</td>
<td>libgsasl handle.</td>
</tr>
<tr>
<td>name</td>
<td>name of SASL mechanism.</td>
</tr>
</tbody>
</table>

Returns

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

gasl_client_suggest_mechanism ()

```c
const char**
gasl_client_suggest_mechanism (Gsasl *ctx,
                                const char *mechlist);
```

Given a list of mechanisms, suggest which to use.

Parameters

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx</td>
<td>libgsasl handle.</td>
</tr>
<tr>
<td>mechlist</td>
<td>input character array with SASL mechanism names, separated by invalid characters (e.g. SPC).</td>
</tr>
</tbody>
</table>

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.

gasl_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.

Parameters

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>out</td>
<td>newly allocated output character array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK if successful, or error code.

gsasl_server_support_p ()

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

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

Parameters

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>name of SASL mechanism.</td>
</tr>
</tbody>
</table>

Returns

Returns 1 if the libgsasl server supports the named mechanism, otherwise 0.

gsasl_client_start ()

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

This functions initiates a client SASL authentication. This function must be called before any other gsasl_client_*() function is called.

Parameters

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mech</td>
<td>name of SASL mechanism.</td>
</tr>
<tr>
<td>sctx</td>
<td>pointer to client handle.</td>
</tr>
</tbody>
</table>
Returns

Returns `GSASL_OK` if successful, or error code.

**gsasl_server_start ()**

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

This function initiates a server SASL authentication. This function must be called before any other `gsasl_server_*( )` function is called.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mech</td>
<td>name of SASL mechanism.</td>
</tr>
<tr>
<td>sctx</td>
<td>pointer to server handle.</td>
</tr>
</tbody>
</table>

Returns

Returns `GSASL_OK` if successful, or error code.

**gsasl_step ()**

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

Perform one step of SASL authentication. This reads data from the other end (from `input` and `input_len`), processes it (potentially invoking callbacks to the application), and writes data to server (into newly allocated variable `output` and `output_len` that indicate the length of `output`).

The contents of the `output` buffer is unspecified if this function returns anything other than `GSASL_OK` or `GSASL_NEEDS_MORE`. If this function return `GSASL_OK` or `GSASL_NEEDS_MORE`, however, the `output` buffer is allocated by this function, and it is the responsibility of caller to deallocate it by calling `free(output)`.

**Parameters**

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl session handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>input byte array.</td>
</tr>
<tr>
<td>input_len</td>
<td>size of input byte array.</td>
</tr>
<tr>
<td>output</td>
<td>newly allocated output byte array.</td>
</tr>
<tr>
<td>output_len</td>
<td>pointer to output variable with size of output byte array.</td>
</tr>
</tbody>
</table>
Returns

Returns `GSASL_OK` if authenticated terminated successfully, `GSASL_NEEDS_MORE` if more data is needed, or error code.

### gsasl_step64 ()

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

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

The contents of the `b64output` buffer is unspecified if this functions returns anything other than `GSASL_OK` or `GSASL_NEEDS_MORE`. If this function return `GSASL_OK` or `GSASL_NEEDS_MORE`, however, the `b64output` buffer is allocated by this function, and it is the responsibility of caller to deallocate it by calling `free(b64output)`.

### Parameters

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl client handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b64input</td>
<td>input base64 encoded byte array.</td>
</tr>
<tr>
<td>b64output</td>
<td>newly allocated output base64 encoded byte array.</td>
</tr>
</tbody>
</table>

### Returns

Returns `GSASL_OK` if authenticated terminated successfully, `GSASL_NEEDS_MORE` if more data is needed, or error code.

### gsasl_finish ()

```c
void gsasl_finish (Gsasl_session *sctx);
```

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

### Parameters

| sctx | libgsasl session handle. |

### gsasl_encode ()

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

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)`. 
Parameters

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl session handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>input byte array.</td>
</tr>
<tr>
<td>input_len</td>
<td>size of input byte array.</td>
</tr>
<tr>
<td>output</td>
<td>newly allocated output byte array.</td>
</tr>
<tr>
<td>output_len</td>
<td>size of output byte array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK if encoding was successful, otherwise an error code.

gsasl_decode()

```c
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).

Parameters

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl session handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>input byte array.</td>
</tr>
<tr>
<td>input_len</td>
<td>size of input byte array.</td>
</tr>
<tr>
<td>output</td>
<td>newly allocated output byte array.</td>
</tr>
<tr>
<td>output_len</td>
<td>size of output byte array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK if encoding was successful, otherwise an error code.

gsasl_mechanism_name()

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

This function returns the name of the SASL mechanism used in the session. The pointer must not be deallocated by the caller.

Parameters

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl session handle.</th>
</tr>
</thead>
</table>
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()`

```c
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()`.

Parameters

- **err** | libgsasl error code |

Returns

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

`gsasl_strerror_name()`

```c
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()`.

Parameters

- **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()`

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

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

**Parameters**

<table>
<thead>
<tr>
<th>in</th>
<th>a UTF-8 encoded string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>flags</td>
<td>any SASLprep flag, e.g., GSASL_ALLOW_UNASSIGNED.</td>
</tr>
<tr>
<td>out</td>
<td>on exit, contains newly allocated output string.</td>
</tr>
<tr>
<td>stringpreprc</td>
<td>if non-NULL, will hold precise stringprep return code.</td>
</tr>
</tbody>
</table>

**Returns**

Returns GSASL_OK on success, or GSASL_SASLPREP_ERROR on error.

**gsasl_simple_getpass()**

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>filename</th>
<th>filename of file containing passwords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>username string.</td>
</tr>
<tr>
<td>key</td>
<td>newly allocated output character array.</td>
</tr>
</tbody>
</table>

**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()**

```c
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.

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>input byte array</td>
</tr>
<tr>
<td>inlen</td>
<td>size of input byte array</td>
</tr>
<tr>
<td>out</td>
<td>pointer to newly allocated output byte array</td>
</tr>
<tr>
<td>outlen</td>
<td>pointer to size of newly allocated output byte array</td>
</tr>
</tbody>
</table>

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.

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>input byte array</td>
</tr>
<tr>
<td>inlen</td>
<td>size of input byte array</td>
</tr>
<tr>
<td>out</td>
<td>pointer to newly allocated output byte array</td>
</tr>
<tr>
<td>outlen</td>
<td>pointer to size of newly allocated output byte array</td>
</tr>
</tbody>
</table>

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.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>output array to be filled with unpredictable random data.</td>
</tr>
<tr>
<td>datalen</td>
<td>size of output array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK iff successful.

`gsasl_random ()`

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

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>output array to be filled with strong random data.</td>
</tr>
<tr>
<td>datalen</td>
<td>size of output array.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK iff successful.

`gsasl_md5 ()`

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

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>input character array of data to hash.</td>
</tr>
<tr>
<td>inlen</td>
<td>length of input character array of data to hash.</td>
</tr>
<tr>
<td>out</td>
<td>newly allocated 16-byte character array with hash of data.</td>
</tr>
</tbody>
</table>

Returns

Returns GSASL_OK iff successful.
gsasl_hmac_md5()

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

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>input character array with key to use.</td>
</tr>
<tr>
<td>keylen</td>
<td>length of input character array with key to use.</td>
</tr>
<tr>
<td>in</td>
<td>input character array of data to hash.</td>
</tr>
<tr>
<td>inlen</td>
<td>length of input character array of data to hash.</td>
</tr>
<tr>
<td>outhash</td>
<td>newly allocated 16-byte character array with keyed hash of data.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` iff successful.

gsasl_sha1()

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

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>input character array of data to hash.</td>
</tr>
<tr>
<td>inlen</td>
<td>length of input character array of data to hash.</td>
</tr>
<tr>
<td>out</td>
<td>newly allocated 20-byte character array with hash of data.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` iff successful.

Since: 1.3
gsasl_hmac_sha1()

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

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>input character array with key to use.</td>
</tr>
<tr>
<td>keylen</td>
<td>length of input character array with key to use.</td>
</tr>
<tr>
<td>in</td>
<td>input character array of data to hash.</td>
</tr>
<tr>
<td>inlen</td>
<td>length of input character array of data to hash.</td>
</tr>
<tr>
<td>outhash</td>
<td>newly allocated 20-byte character array with keyed hash of data.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` iff successful.

Since: 1.3

gsasl_free()

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptr</td>
<td>memory pointer</td>
</tr>
</tbody>
</table>

Since: 0.2.19

**Types and Values**

**GSASL_API**

```c
#define GSASL_API __attribute__((__visibility__("default")))
```
GSASL_VERSION

#define GSASL_VERSION "1.8.1"

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 8

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 1

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 0x010801

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

Error codes for library functions.

Members
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSASL_OK</td>
<td>Successful return code, guaranteed to be always 0.</td>
</tr>
<tr>
<td>GSASL_NEEDS_MORE</td>
<td>Mechanism expects another round-trip.</td>
</tr>
<tr>
<td>GSASL_UNKNOWN_MECHANISM</td>
<td>Application requested an unknown mechanism.</td>
</tr>
<tr>
<td>GSASL_MECHANISM_CALLED_TOO_MANY_TIMES</td>
<td>Application requested too many round trips from mechanism.</td>
</tr>
<tr>
<td>GSASL_MALLOC_ERROR</td>
<td>Memory allocation failed.</td>
</tr>
<tr>
<td>GSASL_BASE64_ERROR</td>
<td>Base64 encoding/decoding failed.</td>
</tr>
<tr>
<td>GSASL_CRYPTO_ERROR</td>
<td>Cryptographic error.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>GSASL_SASLPREP_ERROR</td>
<td>Failed to prepare internationaized string.</td>
</tr>
<tr>
<td>GSASL_MECHANISM_PARSE_ERROR</td>
<td>Mechanism could not parse input.</td>
</tr>
<tr>
<td>GSASL_AUTHENTICATION_ERROR</td>
<td>Authentication has failed.</td>
</tr>
<tr>
<td>GSASL_INTEGRITY_ERROR</td>
<td>Application data integrity check failed.</td>
</tr>
<tr>
<td>GSASL_NO_CLIENT_CODE</td>
<td>Library was built with client functionality.</td>
</tr>
<tr>
<td>GSASL_NO_SERVER_CODE</td>
<td>Library was built with server functionality.</td>
</tr>
<tr>
<td>GSASL_NO_CALLBACK</td>
<td>Application did not provide a callback.</td>
</tr>
<tr>
<td>GSASL_NO_ANONYMOUS_TOKEN</td>
<td>Could not get required anonymous token.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>GSASL_NO_AUTHID</td>
<td>Could not get required authentication identity (username).</td>
</tr>
<tr>
<td>GSASL_NO_AUTHZID</td>
<td>Could not get required authorization identity.</td>
</tr>
<tr>
<td>GSASL_NO_PASSWORD</td>
<td>Could not get required password.</td>
</tr>
<tr>
<td>GSASL_NO_PASSCODE</td>
<td>Could not get required SecureID PIN.</td>
</tr>
<tr>
<td>GSASL_NO_PIN</td>
<td>Could not get required SecureID PIN.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>GSASL_NO_SERVICE</td>
<td>Could not get required service name.</td>
</tr>
<tr>
<td>GSASL_NO_HOSTNAME</td>
<td>Could not get required hostname.</td>
</tr>
<tr>
<td>GSASL_NO_CB_TLS_UNIQUE</td>
<td>Could not get required tls-unique CB.</td>
</tr>
<tr>
<td>GSASL_NO_SAML20_IDP_IDENTIFIER</td>
<td>Could not get required SAML IdP.</td>
</tr>
<tr>
<td>GSASL_NO_SAML20_REDIRECT_URL</td>
<td>Could not get required SAML redirect URL.</td>
</tr>
<tr>
<td>GSASL_NO_OPENID20_REDIRECT_URL</td>
<td>Could not get required OpenID redirect URL.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_RELEASE_BUFFER_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>GSASL_GSSAPI_IMPORT_NAME_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_INIT_SEC_CONTEXT_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_ACCEPT_SEC_CONTEXT_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_UNWRAP_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_WRAP_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_ACQUIRE_CRED_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_DISPLAY_NAME_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_UNSUPPORTED_PROTECTION_ERROR</td>
<td>An unsupported quality-of-protection layer was requested.</td>
</tr>
<tr>
<td>GSASL_KERBEROS_V5_INIT_ERROR</td>
<td>Initial error in KERBEROS_V5.</td>
</tr>
<tr>
<td>GSASL_KERBEROS_V5_INTERNAL_ERROR</td>
<td>General error in KERBEROS_V5.</td>
</tr>
<tr>
<td>GSASL_SHISHI_ERROR</td>
<td>Same as GSASL_KERBEROS_V5_INTERNAL_ERROR.</td>
</tr>
<tr>
<td>GSASL_SECURID_SERVER_NEED_ADDITIONAL_PASSCODE</td>
<td>SecurID mechanism needs an additional passcode.</td>
</tr>
<tr>
<td>GSASL_SECURID_SERVER_NEED_NEW_PIN</td>
<td>SecurID mechanism needs a new PIN.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_ENCAPSULATE_TOKEN_ERROR</td>
<td>GSS-API library call error.</td>
</tr>
</tbody>
</table>
enum 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.

Members

<table>
<thead>
<tr>
<th>Gsasl_qop</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSASL_QOP_AUTH</td>
<td>Authentication only.</td>
</tr>
<tr>
<td>GSASL_QOP_AUTH_INT</td>
<td>Authentication and integrity.</td>
</tr>
<tr>
<td>GSASL_QOP_AUTH_CONF</td>
<td>Authentication, integrity and confidentiality.</td>
</tr>
</tbody>
</table>
enum 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.

Members

<table>
<thead>
<tr>
<th>Gsasl_cipher</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSASL_CIPHER_DES</td>
<td>Cipher DES</td>
</tr>
<tr>
<td>GSASL_CIPHER_3DES</td>
<td>Cipher 3DES</td>
</tr>
<tr>
<td>GSASL_CIPHER_RC4</td>
<td>Cipher RC4</td>
</tr>
<tr>
<td>GSASL_CIPHER_RC4_40</td>
<td>Cipher RC4 with 40-bit keys.</td>
</tr>
<tr>
<td>GSASL_CIPHER_RC4_56</td>
<td>Cipher RC4 with 56-bit keys.</td>
</tr>
<tr>
<td>GSASL_CIPHER_AES</td>
<td>Cipher AES</td>
</tr>
</tbody>
</table>

enum Gsasl_saslprep_flags

Flags for the SASLprep function, see `gsasl_saslprep()`. For background, see the GNU Libidn documentation.

Members

<table>
<thead>
<tr>
<th>Gsasl_saslprep_flags</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSASL_ALLOW_UNASSIGNED</td>
<td>Allow unassigned code points.</td>
</tr>
</tbody>
</table>

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

Callback/property types.

#### Members

<table>
<thead>
<tr>
<th>Enum Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSASL_AUTHID</td>
<td>Authentication identity (username).</td>
</tr>
<tr>
<td>GSASL_AUTHZID</td>
<td>Authorization identity.</td>
</tr>
<tr>
<td>GSASL_PASSWORD</td>
<td>Password.</td>
</tr>
<tr>
<td>GSASL_ANONYMOUS_TOKEN</td>
<td>Anonymous identifier.</td>
</tr>
<tr>
<td>GSASL_SERVICE</td>
<td>Service name</td>
</tr>
<tr>
<td>GSASL_HOSTNAME</td>
<td>Host name.</td>
</tr>
<tr>
<td>GSASL_GSSAPI_DISPLAY_NAME</td>
<td>GSS-API credential principal name.</td>
</tr>
<tr>
<td>GSASL_PASSCODE</td>
<td>SecurID passcode.</td>
</tr>
<tr>
<td>GSASL_SUGGESTED_PIN</td>
<td>SecurID suggested PIN.</td>
</tr>
<tr>
<td>GSASL_PIN</td>
<td>SecurID PIN.</td>
</tr>
<tr>
<td>GSASL_REALM</td>
<td>User realm.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GSASL_DIGEST_MD5_HASHED_PASSWORD</td>
<td>Pre-computed hashed DIGEST-MD5 password, to avoid storing passwords in the clear.</td>
</tr>
<tr>
<td>GSASL_QOPS</td>
<td>Set of quality-of-protection values.</td>
</tr>
<tr>
<td>GSASL_QOP</td>
<td>Quality-of-protection value.</td>
</tr>
<tr>
<td>GSASL_SCRAM_ITER</td>
<td>Number of iterations in password-to-key hashing.</td>
</tr>
<tr>
<td>GSASL_SCRAM_SALT</td>
<td>Salt for password-to-key hashing.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GSASL_SCRAM_SALTED_PASSWORD</td>
<td>Pre-computed salted SCRAM key, to avoid recomputation and storing passwords in the clear.</td>
</tr>
<tr>
<td>GSASL_CB_TLS_UNIQUE</td>
<td>Base64 encoded tls-unique channel binding.</td>
</tr>
<tr>
<td>GSASL_SAML20_IDP_IDENTIFIER</td>
<td>SAML2.0 user IdP URL.</td>
</tr>
<tr>
<td>GSASL_SAML20_REDIRECT_URL</td>
<td>SAML2.0 URL to access in browser.</td>
</tr>
<tr>
<td>GSASL_OPENID20_REDIRECT_URL</td>
<td>OpenID 2.0 URL to access in browser.</td>
</tr>
<tr>
<td>GSASL_OPENID20_OUTCOME_DATA</td>
<td>OpenID 2.0 authentication outcome data.</td>
</tr>
</tbody>
</table>
GSASL_SAML20_AUTHENTICATE_IN_BROWSER

Request to perform SAML 2.0 authentication in browser.

GSASL_OPENID20_AUTHENTICATE_IN_BROWSER

Request to perform OpenID 2.0 authentication 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.
1.2 gsasl-mech

gsasl-mech —

Functions

<table>
<thead>
<tr>
<th>Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>int</td>
<td>(*Gsasl_init_function) ()</td>
</tr>
<tr>
<td>void</td>
<td>(*Gsasl_done_function) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_start_function) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_step_function) ()</td>
</tr>
<tr>
<td>void</td>
<td>(*Gsasl_finish_function) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_code_function) ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_register ()</td>
</tr>
</tbody>
</table>

Types and Values
struct Gsasl_mechanism_functions
struct Gsasl_mechanism

Description

Functions

Gsasl_init_function ()

int (*Gsasl_init_function) (Gsasl *ctx);

Gsasl_done_function ()

void (*Gsasl_done_function) (Gsasl *ctx);

Gsasl_start_function ()

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

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);

Gsasl_finish_function ()

void (*Gsasl_finish_function) (Gsasl_session *sctx,
                                void *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);
**gsasl_register ()**

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>pointer to libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mech</td>
<td>plugin structure with information about plugin.</td>
</tr>
</tbody>
</table>

**Returns**

GSASL_OK iff successful, otherwise GSASL_MALLOC_ERROR.

Since: 0.2.0

**Types and Values**

`struct Gsasl_mechanism_functions`

```c
struct Gsasl_mechanism_functions {
  Gsasl_init_function init;
  Gsasl_done_function done;
  Gsasl_start_function start;
  Gsasl_step_function step;
  Gsasl_finish_function finish;
  Gsasl_code_function encode;
  Gsasl_code_function decode;
};
```

`struct Gsasl_mechanism`

```c
struct Gsasl_mechanism {
  const char *name;
  struct Gsasl_mechanism_functions client;
  struct Gsasl_mechanism_functions server;
};
```

### 1.3 gsasl-compat

gasl-compat —
Functions

<table>
<thead>
<tr>
<th>int</th>
<th>gsasl_client_listmech ()</th>
</tr>
</thead>
<tbody>
<tr>
<td>int</td>
<td>gsasl_server_listmech ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_client_step ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_client_step_base64 ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_server_step ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_server_step_base64 ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_client_finish ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_server_finish ()</td>
</tr>
<tr>
<td>Gsasl *</td>
<td>gsasl_client_ctx_get ()</td>
</tr>
<tr>
<td>Gsasl *</td>
<td>gsasl_server_ctx_get ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_client_application_data_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_client_application_data_get ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_server_application_data_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_server_application_data_get ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_randomize ()</td>
</tr>
<tr>
<td>Gsasl *</td>
<td>gsasl_ctx_get ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_encode_inline ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_decode_inline ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_application_data_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_application_data_get ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_appinfo_set ()</td>
</tr>
<tr>
<td>void *</td>
<td>gsasl_appinfo_get ()</td>
</tr>
<tr>
<td>const char *</td>
<td>gsasl_server_suggest_mechanism ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_base64_encode ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_base64_decode ()</td>
</tr>
<tr>
<td>char *</td>
<td>gsasl_stringprep_nfkc ()</td>
</tr>
<tr>
<td>char *</td>
<td>gsasl_stringprep_saslprep ()</td>
</tr>
<tr>
<td>char *</td>
<td>gsasl_stringprep_trace ()</td>
</tr>
<tr>
<td>int</td>
<td>gsasl_md5pwd_get_password ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_anonymous) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_authentication_id) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_authorization_id) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_password) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_passcode) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_pin) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_service) ()</td>
</tr>
<tr>
<td>Gsasl_qop</td>
<td>(*Gsasl_client_callback_qop) ()</td>
</tr>
<tr>
<td>size_t</td>
<td>(*Gsasl_client_callback_maxbuf) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_client_callback_realm) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_retrieve) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_validate) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_gssapi) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_secureid) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_cram_md5) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_digest_md5) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_service) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_external) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_anonymous) ()</td>
</tr>
<tr>
<td>int</td>
<td>(*Gsasl_server_callback_realm) ()</td>
</tr>
<tr>
<td>Gsasl_qop</td>
<td>(*Gsasl_server_callback_qop) ()</td>
</tr>
<tr>
<td>size_t</td>
<td>(*Gsasl_server_callback_maxbuf) ()</td>
</tr>
<tr>
<td>Gsasl_cipher</td>
<td>(*Gsasl_server_callback_cipher) ()</td>
</tr>
<tr>
<td>void</td>
<td>gsasl_client_callback_authorization_id_set ()</td>
</tr>
<tr>
<td>Gsasl_client_callback_authorization_id</td>
<td>gsasl_client_callback_authorization_id_get ()</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>gsasl_client_listmech ()</td>
<td></td>
</tr>
</tbody>
</table>

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>out</td>
<td>output character array.</td>
</tr>
<tr>
<td>outlen</td>
<td>input maximum size of output character array, on output contains actual length of output array.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` if successful, or error code.

```c
int gsasl_client_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.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>out</td>
<td>output character array.</td>
</tr>
<tr>
<td>outlen</td>
<td>input maximum size of output character array, on output contains actual length of output array.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` if successful, or error code.
gsasl_client_step()

```c
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*.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl client handle.</td>
</tr>
<tr>
<td>input</td>
<td>input byte array.</td>
</tr>
<tr>
<td>input_len</td>
<td>size of input byte array.</td>
</tr>
<tr>
<td>output</td>
<td>output byte array.</td>
</tr>
<tr>
<td>output_len</td>
<td>size of output byte array.</td>
</tr>
</tbody>
</table>

**Returns**

Returns *GSASL_OK* if authenticated terminated successfully, *GSASL_NEEDS_MORE* if more data is needed, or error code.

gsasl_client_step_base64()

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl client handle.</td>
</tr>
</tbody>
</table>
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 function returns anything other than GSASL_NEEDS_MORE.

### Parameters

<table>
<thead>
<tr>
<th>sctx</th>
<th>libgsasl server handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>input byte array.</td>
</tr>
<tr>
<td>input_len</td>
<td>size of input byte array.</td>
</tr>
<tr>
<td>output</td>
<td>output byte array.</td>
</tr>
<tr>
<td>output_len</td>
<td>size of output byte array.</td>
</tr>
</tbody>
</table>

### Returns

Returns GSASL_OK if authenticated terminated successfully, GSASL_NEEDS_MORE if more data is needed, or error code.

---

**Warning**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl server handle.</td>
</tr>
<tr>
<td>b64input</td>
<td>input base64 encoded byte array.</td>
</tr>
<tr>
<td>b64output</td>
<td>output base64 encoded byte array.</td>
</tr>
<tr>
<td>b64output_len</td>
<td>size of output base64 encoded byte array.</td>
</tr>
</tbody>
</table>

**Returns**

See `gsasl_server_step()`.

---

`gsasl_client_finish()`

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

Warning: The function `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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl client handle.</td>
</tr>
</tbody>
</table>

`gsasl_server_finish()`

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

Warning: The function `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.

Parameters

sctx | libgsasl server handle |

\textbf{gsasl\_server\_ctx\_get ()}

\begin{verbatim}
Gsasl~*
gsasl_server_ctx_get (Gsasl_session *sctx);
\end{verbatim}

\begin{center}
\textbf{Warning}

\textit{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.
\end{center}

Get the libgsasl handle given a libgsasl client handle.

Parameters

sctx | libgsasl client handle |

\textbf{Returns}

Returns the libgsasl handle given a libgsasl client handle.

\textbf{gsasl\_server\_ctx\_get ()}

\begin{verbatim}
Gsasl~*
gsasl_server_ctx_get (Gsasl_session *sctx);
\end{verbatim}

\begin{center}
\textbf{Warning}

\textit{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.
\end{center}

Get the libgsasl handle given a libgsasl server handle.

Parameters

sctx | libgsasl server handle |

\textbf{Returns}

Returns the libgsasl handle given a libgsasl server handle.
gsasl_client_application_data_set ()

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

**Warning**

脱颖 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.

**Parameters**

- `sctx` : libgsasl client handle.
- `application_data` : opaque pointer to application specific data.

gsasl_client_application_data_get ()

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

**Warning**

脱颖 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.

**Parameters**

- `sctx` : libgsasl client handle.

**Returns**

Returns the application specific data, or NULL.

gsasl_server_application_data_set ()

```c
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.

Parameters

- `sctx` (libgsasl server handle.
- `application_data` (opaque pointer to application specific data).

`gsasl_server_application_data_get()`

```c
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.

Parameters

- `sctx` (libgsasl server handle.

Returns

Returns the application specific data, or NULL.

`gsasl_randomize()`

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strong</td>
<td>0 if operation should not block, non-0 for very strong randomness.</td>
</tr>
<tr>
<td>data</td>
<td>output array to be filled with random data.</td>
</tr>
<tr>
<td>datalen</td>
<td>size of output array.</td>
</tr>
</tbody>
</table>

**Returns**

Returns `GSASL_OK` iff successful.

```c
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.

Get the libgsasl handle given a libgsasl session handle.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl session handle</td>
</tr>
</tbody>
</table>

**Returns**

Returns the libgsasl handle given a libgsasl session handle.

```c
gsasl_ctx_get (Gsasl_session *sctx);
```
Encode data according to negotiated SASL mechanism. This might mean that data is integrity or privacy protected.

**Parameters**

- **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

```c
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.

**Parameters**

- **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

```c
void gsasl_application_data_set (Gsasl *ctx,
                                 void *appdata);
```
Warning \texttt{gsasl_application_data_set} is deprecated and should not be used in newly-written code. Use \texttt{gsasl_callback_hook_set()} instead.

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

### Parameters

| ctx | libgsasl handle. |
| appdata | opaque pointer to application specific data. |

**gsasl_application_data_get()**

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

Warning \texttt{gsasl_application_data_get} is deprecated and should not be used in newly-written code. Use \texttt{gsasl_callback_hook_get()} instead.

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

### Parameters

| ctx | libgsasl handle. |

**Returns**

Returns the application specific data, or NULL.

**gsasl_appinfo_set()**

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

Warning \texttt{gsasl_appinfo_set} is deprecated and should not be used in newly-written code. Use \texttt{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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl session handle.</td>
</tr>
<tr>
<td>appdata</td>
<td>opaque pointer to</td>
</tr>
<tr>
<td></td>
<td>application specific data.</td>
</tr>
</tbody>
</table>

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sctx</td>
<td>libgsasl session handle.</td>
</tr>
</tbody>
</table>

**Returns**

Returns the application specific data, or NULL.

```c
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.

**Parameters**
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()**

```c
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.

**Parameters**

<table>
<thead>
<tr>
<th>src</th>
<th>input byte array</th>
</tr>
</thead>
<tbody>
<tr>
<td>srclength</td>
<td>size of input byte array</td>
</tr>
<tr>
<td>target</td>
<td>output byte array</td>
</tr>
<tr>
<td>targsize</td>
<td>size of output byte array</td>
</tr>
</tbody>
</table>

**Returns**

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

**gsasl_base64_decode()**

```c
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.

### Parameters

<table>
<thead>
<tr>
<th>src</th>
<th>input byte array</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>output byte array</td>
</tr>
<tr>
<td>targsize</td>
<td>size of output byte array</td>
</tr>
</tbody>
</table>

### Returns

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

#### gsasl_stringprep_nfkc ()

```c
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.

### Parameters

<table>
<thead>
<tr>
<th>in</th>
<th>a UTF-8 encoded string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>len</td>
<td>length of str, in bytes, or -1 if str is nul-terminated.</td>
</tr>
</tbody>
</table>

### Returns

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

#### gsasl_stringprep_saslprep ()

```c
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.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>in</code></td>
<td>input ASCII or UTF-8 string with data to prepare according to SASLprep.</td>
</tr>
<tr>
<td><code>stringprep_rc</code></td>
<td>pointer to output variable with stringprep error code, or NULL to indicate that you don’t care about it.</td>
</tr>
</tbody>
</table>

### 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.

```c
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.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>in</code></td>
<td>input ASCII or UTF-8 string with data to prepare according to &quot;trace&quot;.</td>
</tr>
<tr>
<td><code>stringprep_rc</code></td>
<td>pointer to output variable with stringprep error code, or NULL to indicate that you don’t care about it.</td>
</tr>
</tbody>
</table>
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.

```c
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 "username\TABpassword". 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.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>filename of file containing passwords.</td>
</tr>
<tr>
<td>username</td>
<td>username string.</td>
</tr>
<tr>
<td>key</td>
<td>output character array.</td>
</tr>
<tr>
<td>keylen</td>
<td>input maximum size of output character array, on output contains actual length of output array.</td>
</tr>
</tbody>
</table>

**Returns**

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

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

**Gsasl_client_callback_anonymous ()**

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

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

Gsasl_client_callback_authorization_id ()

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

Gsasl_client_callback_password ()

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

Gsasl_client_callback_passcode ()

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

Gsasl_client_callback_pin ()

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

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);
Gsasl_client_callback_qop ()

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

Gsasl_client_callback_maxbuf ()

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

Gsasl_client_callback_realm ()

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

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);

Gsasl_server_callback_validate ()

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

Gsasl_server_callback_gssapi ()

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

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

Gsasl_server_callback_cram_md5 ()

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

Gsasl_server_callback_digest_md5 ()

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

Gsasl_server_callback_service ()

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

Gsasl_server_callback_external ()

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

Gsasl_server_callback_anonymous ()

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

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

**Gsasl_server_callback_qop ()**

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

**Gsasl_server_callback_maxbuf ()**

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

**Gsasl_server_callback_cipher ()**

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

**gsasl_client_callback_authorization_id_set ()**

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>
gsasl_client_callback_authorization_id_get ()

Gsasl_client_callback_authorization_id

#define 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()`.

**Parameters**

- **ctx**: libgsasl handle.

**Returns**

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

---

`gsasl_client_callback_authentication_id_set` ()


```
void

#define 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()`.

**Parameters**

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

---

`gsasl_client_callback_authentication_id_get` ()

Gsasl_client_callback_authentication_id

#define gsasl_client_callback_authentication_id_get
((Gsasl *ctx,
   Gsasl_client_callback_authentication_id cb);

---
(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().

**Parameters**

*ctx*  
libgsasl handle.

**Returns**

Returns the callback earlier set by calling gsasl_client_callback_authentication_id_set().

**gsasl_client_callback_anonymous_set ()**

```c
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().

**Parameters**

*ctx*  
libgsasl handle.

*cb*  
callback function

**gsasl_client_callback_anonymous_get ()**

```c
Gsasl_client_callback_anonymous
gsasl_client_callback_anonymous_get (Gsasl *ctx);
```
Get the callback earlier set by calling `gsasl_client_callback_anonymous_set()`.

**Parameters**

| ctx | libgsasl handle. |

**Returns**

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

### `gsasl_client_callback_password_set()`

```c
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()`.

**Parameters**

| ctx | libgsasl handle. |
| cb | callback function |

```c
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()`.
Parameters

ctx | libgsasl handle.

Returns

Returns the callback earlier set by calling gsasl_client_callback_password_set().

**gsasl_client_callback_passcode_set()**

```c
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().

Parameters

ctx | libgsasl handle.

cb | callback function

**gsasl_client_callback_passcode_get()**

```c
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().

Parameters

ctx | libgsasl handle.

Returns

Returns the callback earlier set by calling gsasl_client_callback_passcode_set().
gsasl_client_callback_pin_set ()

```c
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()`.

**Parameters**

- `ctx` : libgsasl handle.
- `cb` : callback function

gsasl_client_callback_pin_get ()

```c
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()`.

**Parameters**

- `ctx` : libgsasl handle.

**Returns**

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

gsasl_client_callback_service_set ()

```c
void
gsasl_client_callback_service_set (Gsasl *ctx,
    Gsasl_client_callback_service cb);
```
Warning \texttt{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 \texttt{gsasl_callback_set()} to set the application callback, and uses \texttt{gsasl_callback()} or \texttt{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 \texttt{gsasl_client_callback_service_get()}.

**Parameters**

\begin{itemize}
  \item \texttt{ctx} \hspace{2cm} libgsasl handle.
  \item \texttt{cb} \hspace{2cm} callback function
\end{itemize}

\texttt{gsasl_client_callback_service_set ()}

\begin{verbatim}
Gsasl_client_callback_service

sgasl_client_callback_service_set (Gsasl *ctx);
\end{verbatim}

Warning \texttt{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 \texttt{gsasl_callback_set()} to set the application callback, and uses \texttt{gsasl_callback()} or \texttt{gsasl_property_get()} to invoke the callback for certain properties.

Get the callback earlier set by calling \texttt{gsasl_client_callback_service_set()}.

**Parameters**

\begin{itemize}
  \item \texttt{ctx} \hspace{2cm} libgsasl handle.
\end{itemize}

**Returns**

Returns the callback earlier set by calling \texttt{gsasl_client_callback_service_set()}.

\texttt{gsasl_client_callback_qop_set ()}

\begin{verbatim}
void

gsasl_client_callback_qop_set (Gsasl *ctx,
   Gsasl_client_callback_qop cb);
\end{verbatim}

Warning \texttt{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 \texttt{gsasl_callback_set()} to set the application callback, and uses \texttt{gsasl_callback()} or \texttt{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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
</table>

**Returns**

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

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

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

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
</table>

**Returns**

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

`gsasl_client_callback_realm_set()

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

`gsasl_client_callback_realm_get()

```c
Gsasl_client_callback.realm
```

```c
Gsasl_client_callback_realm_get (Gsasl *ctx);
```
gsasl_client_callback_realm_get (Gsasl *ctx);

**Warning**
gasl_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().

**Parameters**

| ctx | libgsasl handle. |

**Returns**

Returns the callback earlier set by calling gsasl_client_callback_realm_set().

gasl_server_callback_validate_set ()

```c
void
gasl_server_callback_validate_set (Gsasl *ctx,
                                   Gsasl_server_callback_validate cb);
```

**Warning**
gasl_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().

**Parameters**

| ctx | libgsasl handle. |
| cb | callback function |

gasl_server_callback_validate_get ()

```c
Gsasl_server_callback_validate

gasl_server_callback_validate_get (Gsasl *ctx);
```

**Warning**
gasl_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()`.

**Parameters**

- **ctx**: libgsasl handle.

**Returns**

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

### `gsasl_server_callback_retrieve_set ()`

```c
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()`.

**Parameters**

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

### `gsasl_server_callback_retrieve_get ()`

```c
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()`.

**Parameters**
Returns

Returns the callback earlier set by calling gsasl_server_callback_retrieve_set().

gsasl_server_callback_cram_md5_set()

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

**gsasl_server_callback_cram_md5_get()**

```c
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()`.

**Parameters**

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
</table>

**Returns**

Returns the callback earlier set by calling `gsasl_server_callback_cram_md5_set()`.
gsasl_server_callback_digest_md5_set ()

```c
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().

**Parameters**

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

### gsasl_server_callback_digest_md5_get ()

```c
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().

**Parameters**

- **ctx**: libgsasl handle.

**Returns**

Return the callback earlier set by calling gsasl_server_callback_digest_md5_set().

### gsasl_server_callback_external_set ()

```c
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().

Parameters

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

gsasl_server_callback_external_get()

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().

Parameters

| ctx | libgsasl handle. |

Returns

Returns the callback earlier set by calling gsasl_server_callback_external_set().

gsasl_server_callback_anonymous_set()

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().

void
gsasl_server_callback_anonymous_set (Gsasl *ctx,
                                    Gsasl_server_callback_anonymous cb);
Parameters

ctx | libgsasl handle.

cb | callback function

gsasl_server_callback_anonymous_get ()

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().

Parameters

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().

Parameters

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().

Parameters

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().

Parameters

cctx | 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().

Parameters

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().

Parameters

cctx 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().
Parameters

ctx | libgsasl handle.

Returns

Returns the callback earlier set by calling gsasl_server_callback_maxbuf_set().

gsasl_server_callback_cipher_set ()

```c
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().

Parameters

ctx | libgsasl handle.

branch

cb | callback function

Get the callback earlier set by calling gsasl_server_callback_cipher_set().

Parameters

ctx | libgsasl handle.
Returns

Returns the callback earlier set by calling `gsasl_server_callback_cipher_set()`.

```c
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 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_cipher_get()`.

**Parameters**

- `ctx`: libgsasl handle.
- `cb`: callback function

```c
Gsasl_server_callback_cipher
int
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_get()`.

**Parameters**

- `ctx`: libgsasl handle.

**Returns**

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

```c
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()`.

**Parameters**

- `ctx` libgsasl handle.
- `cb` callback function

gsasl_server_callback_gssapi_get ()

```c
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()`.

**Parameters**

- `ctx` libgsasl handle.

**Returns**

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

gasl_server_callback_service_set ()

```c
void
gasl_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()`.

Parameters

<table>
<thead>
<tr>
<th>ctx</th>
<th>libgsasl handle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cb</td>
<td>callback function</td>
</tr>
</tbody>
</table>

`gsasl_server_callback_service_get()`

```c
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()`.

Parameters

| ctx  | libgsasl handle. |

Returns

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

Types and Values
Chapter 2

Index

G
Gsasl, 30
GSASL_API, 21
gsasl_appinfo_get, 50
gsasl_appinfo_set, 49
gsasl_application_data_get, 49
gsasl_application_data_set, 48
gsasl_base64_decode, 51
gsasl_base64_encode, 51
gsasl_base64_from, 18
gsasl_base64_to, 17
gsasl_callback, 6
Gsasl_callback_function, 4
gsasl_callback_hook_get, 7
gsasl_callback_hook_set, 7
gsasl_callback_set, 6
gsasl_check_version, 6
Gsasl_cipher, 30
gsasl_client_application_data_get, 45
gsasl_client_application_data_set, 45
Gsasl_client_callback_anonymous, 54
gsasl_client_callback_anonymous_get, 60
gsasl_client_callback_anonymous_set, 60
Gsasl_client_callback_authentication_id, 54
gsasl_client_callback_authentication_id_get, 59
gsasl_client_callback_authentication_id_set, 59
Gsasl_client_callback_authorization_id, 55
gsasl_client_callback_authorization_id_get, 59
gsasl_client_callback_authorization_id_set, 58
Gsasl_client_callback_maxbuf, 56
gsasl_client_callback_maxbuf_get, 66
gsasl_client_callback_maxbuf_set, 65
Gsasl_client_callback_passcode, 55
gsasl_client_callback_passcode_get, 62
gsasl_client_callback_passcode_set, 62
Gsasl_client_callback_password, 55
gsasl_client_callback_password_get, 61
gsasl_client_callback_password_set, 61
Gsasl_client_callback_pin, 55
gsasl_client_callback_pin_get, 63
gsasl_client_callback_pin_set, 63
Gsasl_client_callback_qop, 56
gsasl_client_callback_qop_get, 65
gsasl_client_callback_qop_set, 64
Gsasl_client_callback_qop_set, 64
Gsasl_client_callback Realm, 56
gsasl_client_callback Realm_get, 66
gsasl_client_callback Realm_set, 66
Gsasl_client_callback Service, 55
gsasl_client_callback Service_get, 64
gsasl_client_callback Service_set, 63
gsasl_client_ctx_get, 44
gsasl_client_finish, 43
gsasl_client_listmech, 39
gsasl_client_mechlist, 10
gsasl_client_start, 12
gsasl_client_step, 41
gsasl_client_step_base64, 41
gsasl_client_suggest_mechanism, 11
gsasl_client_support_p, 11
Gsasl_code_function, 36
gsasl_ctx_get, 47
gsasl_decode, 15
gsasl_decode_inline, 48
gsasl_done, 5
Gsasl_done_function, 36
gsasl_encode, 14
gsasl_encode_inline, 47
gsasl_finish, 14
Gsasl_finish_function, 36
gsasl_free, 21
gsasl_hmac_md5, 20
gsasl_hmac_sha1, 21
gsasl_init, 5
Gsasl_init_function, 36
gsasl_md5, 19
gsasl_md5pwd_get_password, 54
Gsasl_mechanism, 37
Gsasl_mechanism_functions, 37
Gsasl_mechanism_name, 15
gsaslNonce, 18
Gsasl_property, 31
gsasl_property_fast, 10
gsasl_property_get, 9
gsasl_property_set, 8
gsasl_property_set_raw, 9
Gsasl_qop, 29