NAME

gsasl_scram_secrets_from_password - API function

SYNOPSIS

#include <gsasl.h>

int gsasl_scram_secrets_from_password(Gsasl_hash *hash***, const char *** *password***, unsigned int** *iteration_count***, const char *** *salt***, size_t** *saltlen***, char *** *salted_password***, char *** *client_key***, char *** *server_key***, char *** *stored_key***);**

ARGUMENTS

Gsasl_hash hash
: a **Gsasl_hash** element, e.g., **GSASL_HASH_SHA256**.

const char * password
: input parameter with password.

unsigned int iteration_count
: number of PBKDF2 rounds to apply.

const char * salt
: input character array of *saltlen* length with salt for PBKDF2.

size_t saltlen
: length of *salt* .

char * salted_password
: pre-allocated output array with derived salted password.

char * client_key
: pre-allocated output array with derived client key.

char * server_key
: pre-allocated output array with derived server key.

char * stored_key
: pre-allocated output array with derived stored key.

DESCRIPTION

Helper function to generate SCRAM secrets from a password. The *salted_password* , *client_key* , *server_key* , and *stored_key* buffers must have room to hold digest for

given *hash* , use **GSASL_HASH_MAX_SIZE** which is sufficient for all hashes.

Return value: Returns **GSASL_OK** if successful, or error code.

SINCE

1.10

REPORTING BUGS

Report bugs to <bug-gsasl@gnu.org>.
General guidelines for reporting bugs: http://www.gnu.org/gethelp/
GNU SASL home page: http://www.gnu.org/software/gsasl/

COPYRIGHT

SEE ALSO

The full documentation for **gsasl** is maintained as a Texinfo manual. If the **info** and **gsasl** programs are properly installed at your site, the command

info gsasl

should give you access to the complete manual. As an alternative you may obtain the manual from:

http://www.gnu.org/software/gsasl/manual/