NAME

SRP_Calc_server_key, SRP_Calc_A, SRP_Calc_B_ex, SRP_Calc_B, SRP_Calc_u_ex, SRP_Calc_u, SRP_Calc_x_ex, SRP_Calc_x, SRP_Calc_client_key_ex, SRP_Calc_client_key - SRP authentication primitives

SYNOPSIS

```
#include <openssl/srp.h>
```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining **OPENSSL_API_COMPAT** with a suitable version value, see **openssl_user_macros**(7):

```
/* server side .... */
BIGNUM *SRP_Calc_server_key(const BIGNUM *A, const BIGNUM *v, const BIGNUM *u,
                            const BIGNUM *b, const BIGNUM *N);
BIGNUM *SRP_Calc_B_ex(const BIGNUM *b, const BIGNUM *N, const BIGNUM *g,
                      const BIGNUM *v, OSSL_LIB_CTX *libctx, const char *propq);
BIGNUM *SRP_Calc_B(const BIGNUM *b, const BIGNUM *N, const BIGNUM *g,
                   const BIGNUM *v);

BIGNUM *SRP_Calc_u_ex(const BIGNUM *A, const BIGNUM *B, const BIGNUM *N,
                      OSSL_LIB_CTX *libctx, const char *propq);
BIGNUM *SRP_Calc_u(const BIGNUM *A, const BIGNUM *B, const BIGNUM *N);

/* client side .... */
BIGNUM *SRP_Calc_client_key_ex(const BIGNUM *N, const BIGNUM *B, const BIGNUM *g,
                               const BIGNUM *x, const BIGNUM *a, const BIGNUM *u,
                               OSSL_LIB_CTX *libctx, const char *propq);
BIGNUM *SRP_Calc_client_key(const BIGNUM *N, const BIGNUM *B, const BIGNUM *g,
                            const BIGNUM *x, const BIGNUM *a, const BIGNUM *u);
BIGNUM *SRP_Calc_x_ex(const BIGNUM *s, const char *user, const char *pass,
                      OSSL_LIB_CTX *libctx, const char *propq);
BIGNUM *SRP_Calc_x(const BIGNUM *s, const char *user, const char *pass);
BIGNUM *SRP_Calc_A(const BIGNUM *a, const BIGNUM *N, const BIGNUM *g);
```

DESCRIPTION

All of the functions described on this page are deprecated. There are no available replacement functions at this time.

The SRP functions described on this page are used to calculate various parameters and keys used by SRP as defined in RFC2945. The server key and *B* and *u* parameters are used on the server side and are

calculated via **SRP_Calc_server_key()**, **SRP_Calc_B_ex()**, **SRP_Calc_B()**, **SRP_Calc_u_ex()** and **SRP_Calc_u()**. The client key and **x** and **A** parameters are used on the client side and are calculated via the functions **SRP_Calc_client_key_ex()**, **SRP_Calc_client_key()**, **SRP_Calc_x_ex()**, **SRP_Calc_x()** and **SRP_Calc_A()**. See RFC2945 for a detailed description of their usage and the meaning of the various BIGNUM parameters to these functions.

Most of these functions come in two forms. Those that take a *libctx* and *propq* parameter, and those that don't. Any cryptogrpahic functions that are fetched and used during the calculation use the provided *libctx* and *propq*. See "ALGORITHM FETCHING" in **crypto**(7) for more details. The variants that do not take a *libctx* and *propq* parameter use the default library context and property query string. The **SRP_Calc_server_key()** and **SRP_Calc_A()** functions do not have a form that takes *libctx* or *propq* parameters because they do not need to fetch any cryptographic algorithms.

RETURN VALUES

All these functions return the calculated key or parameter, or NULL on error.

SEE ALSO

openssl-srp(1), **SRP_VBASE_new**(3), **SRP_user_pwd_new**(3)

HISTORY

SRP_Calc_B_ex, SRP_Calc_u_ex, SRP_Calc_client_key_ex and SRP_Calc_x_ex were introduced in OpenSSL 3.0.

All of the other functions were added in OpenSSL 1.0.1.

All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2020-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.