

NAME

BN_CTX_start, BN_CTX_get, BN_CTX_end - use temporary **BIGNUM** variables

SYNOPSIS

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

```
void BN_CTX_start(BN_CTX *ctx);
```

```
BIGNUM *BN_CTX_get(BN_CTX *ctx);
```

```
void BN_CTX_end(BN_CTX *ctx);
```

DESCRIPTION

These functions are used to obtain temporary **BIGNUM** variables from a **BN_CTX** (which can be created by using **BN_CTX_new(3)**) in order to save the overhead of repeatedly creating and freeing **BIGNUM**s in functions that are called from inside a loop.

A function must call **BN_CTX_start()** first. Then, **BN_CTX_get()** may be called repeatedly to obtain temporary **BIGNUM**s. All **BN_CTX_get()** calls must be made before calling any other functions that use the **ctx** as an argument.

Finally, **BN_CTX_end()** must be called before returning from the function. If **ctx** is **NULL**, nothing is done. When **BN_CTX_end()** is called, the **BIGNUM** pointers obtained from **BN_CTX_get()** become invalid.

RETURN VALUES

BN_CTX_start() and **BN_CTX_end()** return no values.

BN_CTX_get() returns a pointer to the **BIGNUM**, or **NULL** on error. Once **BN_CTX_get()** has failed, the subsequent calls will return **NULL** as well, so it is sufficient to check the return value of the last **BN_CTX_get()** call. In case of an error, an error code is set, which can be obtained by **ERR_get_error(3)**.

SEE ALSO

BN_CTX_new(3)

COPYRIGHT

Copyright 2000-2016 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>.