NAME

BN_new, BN_init, BN_clear, BN_free, BN_clear_free - allocate and free BIGNUMs

SYNOPSIS

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

BIGNUM *BN_new(void);

void BN_init(BIGNUM *);

void BN_clear(BIGNUM *a);

void BN_free(BIGNUM *a);

void BN_clear_free(BIGNUM *a);
```

DESCRIPTION

BN_new() allocates and initializes a **BIGNUM** structure. *BN_init()* initializes an existing uninitialized **BIGNUM**.

BN_clear() is used to destroy sensitive data such as keys when they are no longer needed. It erases the memory used by **a** and sets it to the value 0.

BN_free() frees the components of the **BIGNUM**, and if it was created by *BN_new()*, also the structure itself. *BN_clear_free()* additionally overwrites the data before the memory is returned to the system.

RETURN VALUES

BN_new() returns a pointer to the **BIGNUM**. If the allocation fails, it returns **NULL** and sets an error code that can be obtained by *ERR_get_error(3)* .

BN_init(), *BN_clear()*, *BN_free()* and *BN_clear_free()* have no return values.

SEE ALSO

bn(3) , *ERR_get_error(3)*

HISTORY

BN_new(), *BN_clear()*, *BN_free()* and *BN_clear_free()* are available in all versions on SSLeay and OpenSSL. *BN_init()* was added in SSLeay 0.9.1b.