

**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.