NAME

BN_copy, BN_dup, BN_with_flags - copy BIGNUMs

SYNOPSIS

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

BIGNUM *BN_copy(BIGNUM *to, const BIGNUM *from);

BIGNUM *BN_dup(const BIGNUM *from);

void BN_with_flags(BIGNUM *dest, const BIGNUM *b, int flags);
```

DESCRIPTION

BN_copy() copies **from** to **to**. **BN_dup()** creates a new **BIGNUM** containing the value **from**.

BN_with_flags creates a **temporary** shallow copy of **b** in **dest**. It places significant restrictions on the copied data. Applications that do no adhere to these restrictions may encounter unexpected side effects or crashes. For that reason use of this function is discouraged. Any flags provided in **flags** will be set in **dest** in addition to any flags already set in **b**. For example this might commonly be used to create a temporary copy of a BIGNUM with the **BN_FLG_CONSTTIME** flag set for constant time operations. The temporary copy in **dest** will share some internal state with **b**. For this reason the following restrictions apply to the use of **dest**:

- **dest** should be a newly allocated BIGNUM obtained via a call to **BN_new()**. It should not have been used for other purposes or initialised in any way.
- **dest** must only be used in "read-only" operations, i.e. typically those functions where the relevant parameter is declared "const".
- **dest** must be used and freed before any further subsequent use of **b**

RETURN VALUES

BN_copy() returns **to** on success, NULL on error. **BN_dup()** returns the new **BIGNUM**, and NULL on error. The error codes can be obtained by **ERR_get_error**(3).

SEE ALSO

ERR_get_error(3)

COPYRIGHT