NAME

DH_get_1024_160, DH_get_2048_224, DH_get_2048_256, BN_get0_nist_prime_192, BN_get0_nist_prime_224, BN_get0_nist_prime_256, BN_get0_nist_prime_384, BN_get0_nist_prime_521, BN_get_rfc2409_prime_768, BN_get_rfc2409_prime_1024, BN_get_rfc3526_prime_1536, BN_get_rfc3526_prime_2048, BN_get_rfc3526_prime_3072, BN_get_rfc3526_prime_4096, BN_get_rfc3526_prime_6144, BN_get_rfc3526_prime_8192 - Create standardized public primes or DH pairs

SYNOPSIS

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

const BIGNUM *BN_get0_nist_prime_192(void);
const BIGNUM *BN_get0_nist_prime_224(void);
const BIGNUM *BN_get0_nist_prime_256(void);
const BIGNUM *BN_get0_nist_prime_384(void);
const BIGNUM *BN_get0_nist_prime_521(void);

BIGNUM *BN_get_rfc2409_prime_768(BIGNUM *bn);
BIGNUM *BN_get_rfc2409_prime_1024(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_1536(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_2048(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_3072(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_4096(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_6144(BIGNUM *bn);
BIGNUM *BN_get_rfc3526_prime_8192(BIGNUM *bn);
```

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):

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

DH *DH_get_1024_160(void);
DH *DH_get_2048_224(void);
DH *DH_get_2048_256(void);
```

DESCRIPTION

DH_get_1024_160(), **DH_get_2048_224()**, and **DH_get_2048_256()** each return a DH object for the IETF RFC 5114 value. These functions are deprecated. Applications should instead use **EVP_PKEY_CTX_set_dh_rfc5114()** and **EVP_PKEY_CTX_set_dhx_rfc5114()** as described in **EVP_PKEY_CTX_ctrl**(3) or by setting the **OSSL_PKEY_PARAM_GROUP_NAME** as specified in

"DH parameters" in **EVP_PKEY-DH**(7)) to one of "dh_1024_160", "dh_2048_224" or "dh_2048_256".

BN_get0_nist_prime_192(), **BN_get0_nist_prime_224()**, **BN_get0_nist_prime_256()**, **BN_get0_nist_prime_384()**, and **BN_get0_nist_prime_521()** functions return a BIGNUM for the specific NIST prime curve (e.g., P-256).

BN_get_rfc2409_prime_768(), **BN_get_rfc2409_prime_1024()**, **BN_get_rfc3526_prime_1536()**, **BN_get_rfc3526_prime_2048()**, **BN_get_rfc3526_prime_3072()**, **BN_get_rfc3526_prime_4096()**, **BN_get_rfc3526_prime_6144()**, and **BN_get_rfc3526_prime_8192()** functions return a BIGNUM for the specified size from IETF RFC 2409. If **bn** is not NULL, the BIGNUM will be set into that location as well.

RETURN VALUES

Defined above.

HISTORY

The functions **DH_get_1024_160()**, **DH_get_2048_224()** and **DH_get_2048_256()** were deprecated in OpenSSL 3.0.

COPYRIGHT