NAME

EVP_PKEY−FFC − EVP_PKEY DSA and DH/DHX shared FFC parameters.

DESCRIPTION

Finite field cryptography (FFC) is a method of implementing discrete logarithm cryptography using finite field mathematics. DSA is an example of FFC and Diffie-Hellman key establishment algorithms specified in SP800−56A can also be implemented as FFC.

The **DSA**, **DH** and **DHX** keytypes are implemented in OpenSSL's default and FIPS providers. The implementations support the basic DSA, DH and DHX keys, containing the public and private keys *pub* and *priv* as well as the three main domain parameters *p*, *q* and *g*.

For **DSA** (and **DH** that is not a named group) the FIPS186−4 standard specifies that the values used for FFC parameter generation are also required for parameter validation. This means that optional FFC domain parameter values for *seed*, *pcounter* and *gindex* may need to be stored for validation purposes. For **DH** the *seed* and *pcounter* can be stored in ASN1 data (but the *gindex* is not). For **DSA** however, these fields are not stored in the ASN1 data so they need to be stored externally if validation is required.

The **DH** key type uses PKCS#3 format which saves p and g, but not the 'q' value. The **DHX** key type uses X9.42 format which saves the value of 'q' and this must be used for FIPS186−4.

FFC parameters

In addition to the common parameters that all keytypes should support (see ''Common parameters'' in **provider−keymgmt** (7)), the **DSA**, **DH** and **DHX** keytype implementations support the following.

''pub'' (**OSSL_PKEY_PARAM_PUB_KEY**) <unsigned integer>
The public key value.

''priv'' (**OSSL_PKEY_PARAM_PRIV_KEY**) <unsigned integer>
The private key value.

FFC DSA, DH and DHX domain parameters

''p'' (**OSSL_PKEY_PARAM_FFC_P**) <unsigned integer>
A DSA or Diffie-Hellman prime ''p'' value.

''g'' (**OSSL_PKEY_PARAM_FFC_G**) <unsigned integer>
A DSA or Diffie-Hellman generator ''g'' value.

FFC DSA and DHX domain parameters

''q'' (**OSSL_PKEY_PARAM_FFC_Q**) <unsigned integer>
A DSA or Diffie-Hellman prime ''q'' value.

''seed'' (**OSSL_PKEY_PARAM_FFC_SEED**) <octet string>
An optional domain parameter *seed* value used during generation and validation of *p*, *q* and canonical *g*. For validation this needs to set the *seed* that was produced during generation.

''gindex'' (**OSSL_PKEY_PARAM_FFC_GINDEX**) <integer>
Sets the index to use for canonical generation and verification of the generator *g*. Set this to a positive value from 0..FF to use this mode. This *gindex* can then be reused during key validation to verify the value of *g*. If this value is not set or is −1 then unverifiable generation of the generator *g* will be used.

''pcounter'' (**OSSL_PKEY_PARAM_FFC_PCOUNTER**) <integer>
An optional domain parameter *counter* value that is output during generation of *p*. This value must be saved if domain parameter validation is required.

''hindex'' (**OSSL_PKEY_PARAM_FFC_H**) <integer>
For unverifiable generation of the generator *g* this value is output during generation of *g*. Its value is the first integer larger than one that satisfies g = h^j mod p (where g != 1 and ''j'' is the cofactor).

''j'' (**OSSL_PKEY_PARAM_FFC_COFACTOR**) <unsigned integer>
An optional informational cofactor parameter that should equal to (p − 1) / q.

"validate-pq" (**OSSL_PKEY_PARAM_FFC_VALIDATE_PQ**) <unsigned integer>
"validate-g" (**OSSL_PKEY_PARAM_FFC_VALIDATE_G**) <unsigned integer>
These boolean values are used during FIPS186-4 or FIPS186-2 key validation checks (See **EVP_PKEY_param_check**(3)) to select validation options. By default *validate-pq* and *validate-g* are both set to 1 to check that p,q and g are valid. Either of these may be set to 0 to skip a test, which is mainly useful for testing purposes.

"validate-legacy" (**OSSL_PKEY_PARAM_FFC_VALIDATE_LEGACY**) <unsigned integer>
This boolean value is used during key validation checks (See **EVP_PKEY_param_check**(3)) to select the validation type. The default value of 0 selects FIPS186-4 validation. Setting this value to 1 selects FIPS186-2 validation.

FFC key generation parameters

The following key generation types are available for DSA and DHX algorithms:

"type" (**OSSL_PKEY_PARAM_FFC_TYPE**) <UTF8 string>
Sets the type of parameter generation. The shared valid values are:

"fips186_4"
The current standard.

"fips186_2"
The old standard that should only be used for legacy purposes.

"default"
This can choose one of "fips186_4" or "fips186_2" depending on other parameters set for parameter generation.

"pbits" (**OSSL_PKEY_PARAM_FFC_PBITS**) <unsigned integer>
Sets the size (in bits) of the prime 'p'.

"qbits" (**OSSL_PKEY_PARAM_FFC_QBITS**) <unsigned integer>
Sets the size (in bits) of the prime 'q'.

For "fips186_4" this can be either 224 or 256. For "fips186_2" this has a size of 160.

"digest" (**OSSL_PKEY_PARAM_FFC_DIGEST**) <UTF8 string>
Sets the Digest algorithm to be used as part of the Key Generation Function associated with the given Key Generation *ctx*. This must also be set for key validation.

"properties" (**OSSL_PKEY_PARAM_FFC_DIGEST_PROPS**) <UTF8 string>
Sets properties to be used upon look up of the implementation for the selected Digest algorithm for the Key Generation Function associated with the given key generation *ctx*. This may also be set for key validation.

"seed" (**OSSL_PKEY_PARAM_FFC_SEED**) <octet string>
For "fips186_4" or "fips186_2" generation this sets the *seed* data to use instead of generating a random seed internally. This should be used for testing purposes only. This will either produce fixed values for the generated parameters OR it will fail if the seed did not generate valid primes.

"gindex" (**OSSL_PKEY_PARAM_FFC_GINDEX**) <integer>
"pcounter" (**OSSL_PKEY_PARAM_FFC_PCOUNTER**) <integer>
"hindex" (**OSSL_PKEY_PARAM_FFC_H**) <integer>
These types are described above.

CONFORMING TO

The following sections of SP800-56Ar3:

5.5.1.1 FFC Domain Parameter Selection/Generation

The following sections of FIPS 186-4:

A.1.1.2 Generation of Probable Primes p and q Using an Approved Hash Function.

A.2.3 Generation of canonical generator g.
A.2.1 Unverifiable Generation of the Generator g.

SEE ALSO

EVP_PKEY−DSA (7), **EVP_PKEY−DH** (7), **EVP_SIGNATURE−DSA** (7), **EVP_KEYEXCH−DH** (7) **EVP_KEYMGMT** (3), **EVP_PKEY** (3), **provider−keymgmt** (7), **OSSL_PROVIDER−default** (7), **OSSL_PROVIDER−FIPS** (7),

COPYRIGHT