NAME

EVP_SIGNATURE−ECDSA − The EVP_PKEY ECDSA signature implementation.

DESCRIPTION

Support for computing ECDSA signatures. See **EVP_PKEY−EC** (7) for information related to EC keys.

ECDSA Signature Parameters

The following signature parameters can be set using **EVP_PKEY_CTX_set_params()**. This may be called after **EVP_PKEY_sign_init()** or **EVP_PKEY_verify_init()**, and before calling **EVP_PKEY_sign()** or **EVP_PKEY_verify()**.

''digest'' (**OSSL_SIGNATURE_PARAM_DIGEST**) <UTF8 string>
''properties'' (**OSSL_SIGNATURE_PARAM_PROPERTIES**) <UTF8 string>
These parameters are described in **provider−signature** (7).

The following signature parameters can be retrieved using **EVP_PKEY_CTX_get_params()**.

''algorithm-id'' (**OSSL_SIGNATURE_PARAM_ALGORITHM_ID**) <octet string>
''digest'' (**OSSL_SIGNATURE_PARAM_DIGEST**) <UTF8 string>
The parameters are described in **provider−signature** (7).

SEE ALSO

EVP_PKEY_CTX_set_params (3), **EVP_PKEY_sign** (3), **EVP_PKEY_verify** (3), **provider−signature** (7),

COPYRIGHT