

NAME

EVP_SIGNATURE-HMAC, EVP_SIGNATURE-Siphhash, EVP_SIGNATURE-Poly1305,
EVP_SIGNATURE-CMAC – The legacy EVP_PKEY MAC signature implementations

DESCRIPTION

The algorithms described here have legacy support for creating MACs using **EVP_DigestSignInit**(3) and related functions. This is not the preferred way of creating MACs. Instead you should use the newer **EVP_MAC_init**(3) functions. This mechanism is provided for backwards compatibility with older versions of OpenSSL.

The same signature parameters can be set using **EVP_PKEY_CTX_set_params**() as can be set via **EVP_MAC_CTX_set_params**() for the underlying EVP_MAC. See **EVP_MAC-HMAC**(7), **EVP_MAC-Siphhash**(7), **EVP_MAC-Poly1305**(7) and **EVP_MAC-CMAC**(7) for details.

See L<EVP_PKEY-HMAC(7)>, L<EVP_PKEY-Siphhash(7)>, L<EVP_PKEY-Poly1305(7)> or L<EVP_PKEY-CMAC(7)> for details about parameters that are supported during the creation of an EVP_PKEY.

SEE ALSO

EVP_MAC_init(3), **EVP_DigestSignInit**(3), **EVP_PKEY-HMAC**(7), **EVP_PKEY-Siphhash**(7), **EVP_PKEY-Poly1305**(7), **EVP_PKEY-CMAC**(7), **EVP_MAC-HMAC**(7), **EVP_MAC-Siphhash**(7), **EVP_MAC-Poly1305**(7), **EVP_MAC-CMAC**(7), **provider-signature**(7),

COPYRIGHT

Copyright 2020 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the “License”). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <<https://www.openssl.org/source/license.html>>.