



**Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!**

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_SIGNATURE-Siphash.7ssl'***

***\$ man EVP\_SIGNATURE-Siphash.7ssl***

EVP\_SIGNATURE-HMAC(7SSL)                      OpenSSL                      EVP\_SIGNATURE-HMAC(7SSL)

**NAME**

EVP\_SIGNATURE-HMAC, EVP\_SIGNATURE-Siphash, 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-Siphash(7), EVP\_MAC-Poly1305(7) and EVP\_MAC-CMAC(7) for details.

See L<EVP\_PKEY-HMAC(7)>, L<EVP\_PKEY-Siphash(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-Siphash(7),  
EVP\_PKEY-Poly1305(7), EVP\_PKEY-CMAC(7), EVP\_MAC-HMAC(7), EVP\_MAC-Siphash(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>.

3.0.2

2024-02-16

EVP\_SIGNATURE-HMAC(7SSL)