

**NAME**

EVP\_MAC-Poly1305 – The Poly1305 EVP\_MAC implementation

**DESCRIPTION**

Support for computing Poly1305 MACs through the **EVP\_MAC** API.

**Identity**

This implementation is identified with this name and properties, to be used with **EVP\_MAC\_fetch()**:

“POLY1305”, “provider=default”

**Supported parameters**

The general description of these parameters can be found in “PARAMETERS” in **EVP\_MAC**(3).

The following parameter can be set with **EVP\_MAC\_CTX\_set\_params()**:

“key” (**OSSL\_MAC\_PARAM\_KEY**) <octet string>

Sets the MAC key. Setting this parameter is identical to passing *key* to **EVP\_MAC\_init**(3).

The following parameters can be retrieved with **EVP\_MAC\_CTX\_get\_params()**:

“size” (**OSSL\_MAC\_PARAM\_SIZE**) <unsigned integer>

Gets the MAC size.

The “size” parameter can also be retrieved with **EVP\_MAC\_CTX\_get\_mac\_size()**. The length of the “size” parameter should not exceed that of an **unsigned int**.

**NOTES**

The OpenSSL implementation of the Poly 1305 MAC corresponds to RFC 7539.

It is critical to never reuse the key. The security implication noted in RFC 8439 applies equally to the OpenSSL implementation.

**SEE ALSO**

**EVP\_MAC\_CTX\_get\_params**(3), **EVP\_MAC\_CTX\_set\_params**(3), “PARAMETERS” in **EVP\_MAC**(3), **OSSL\_PARAM**(3)

**COPYRIGHT**

Copyright 2018–2021 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>>.