

NAME

EVP_MD-SHA2 – The SHA2 EVP_MD implementation

DESCRIPTION

Support for computing SHA2 digests through the **EVP_MD** API.

Identities

This implementation includes the following varieties:

- Available with the FIPS provider as well as the default provider:

SHA2-224

Known names are “SHA2-224”, “SHA-224” and “SHA224”.

SHA2-256

Known names are “SHA2-256”, “SHA-256” and “SHA256”.

SHA2-384

Known names are “SHA2-384”, “SHA-384” and “SHA384”.

SHA2-512

Known names are “SHA2-512”, “SHA-512” and “SHA512”.

- Available with the default provider:

SHA2-512/224

Known names are “SHA2-512/224”, “SHA-512/224” and “SHA512-224”.

SHA2-512/256

Known names are “SHA2-512/256”, “SHA-512/256” and “SHA512-256”.

Gettable Parameters

This implementation supports the common gettable parameters described in **EVP_MD-common** (7).

SEE ALSO

provider-digest (7), **OSSL_PROVIDER-FIPS** (7), **OSSL_PROVIDER-default** (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>](https://www.openssl.org/source/license.html).