

**NAME**

OCSP\_request\_add1\_nonce, OCSP\_basic\_add1\_nonce, OCSP\_check\_nonce, OCSP\_copy\_nonce -  
OCSP nonce functions

**SYNOPSIS**

```
#include <openssl/ocsp.h>
```

```
int OCSP_request_add1_nonce(OCSP_REQUEST *req, unsigned char *val, int len);
int OCSP_basic_add1_nonce(OCSP_BASICRESP *resp, unsigned char *val, int len);
int OCSP_copy_nonce(OCSP_BASICRESP *resp, OCSP_REQUEST *req);
int OCSP_check_nonce(OCSP_REQUEST *req, OCSP_BASICRESP *resp);
```

**DESCRIPTION**

**OCSP\_request\_add1\_nonce()** adds a nonce of value **val** and length **len** to OCSP request **req**. If **val** is **NULL** a random nonce is used. If **len** is zero or negative a default length will be used (currently 16 bytes).

**OCSP\_basic\_add1\_nonce()** is identical to **OCSP\_request\_add1\_nonce()** except it adds a nonce to OCSP basic response **resp**.

**OCSP\_check\_nonce()** compares the nonce value in **req** and **resp**.

**OCSP\_copy\_nonce()** copies any nonce value present in **req** to **resp**.

**RETURN VALUES**

**OCSP\_request\_add1\_nonce()** and **OCSP\_basic\_add1\_nonce()** return 1 for success and 0 for failure.

**OCSP\_copy\_nonce()** returns 1 if a nonce was successfully copied, 2 if no nonce was present in **req** and 0 if an error occurred.

**OCSP\_check\_nonce()** returns the result of the nonce comparison between **req** and **resp**. The return value indicates the result of the comparison. If nonces are present and equal 1 is returned. If the nonces are absent 2 is returned. If a nonce is present in the response only 3 is returned. If nonces are present and unequal 0 is returned. If the nonce is present in the request only then -1 is returned.

**NOTES**

For most purposes the nonce value in a request is set to a random value so the **val** parameter in **OCSP\_request\_add1\_nonce()** is usually **NULL**.

An OCSP nonce is typically added to an OCSP request to thwart replay attacks by checking the same

nonce value appears in the response.

Some responders may include a nonce in all responses even if one is not supplied.

Some responders cache OCSP responses and do not sign each response for performance reasons. As a result they do not support nonces.

The return values of **OCSP\_check\_nonce()** can be checked to cover each case. A positive return value effectively indicates success: nonces are both present and match, both absent or present in the response only. A nonzero return additionally covers the case where the nonce is present in the request only: this will happen if the responder doesn't support nonces. A zero return value indicates present and mismatched nonces: this should be treated as an error condition.

#### **SEE ALSO**

**crypto(7), OCSP\_cert\_to\_id(3), OCSP\_REQUEST\_new(3), OCSP\_resp\_find\_status(3), OCSP\_response\_status(3), OCSP\_sendreq\_new(3)**

#### **COPYRIGHT**

Copyright 2015-2020 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>.