



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

### ***Rocky Enterprise Linux 9.2 Manual Pages on command 'OCSP\_resp\_get0\_signature.3ossl'***

***\$ man OCSP\_resp\_get0\_signature.3ossl***

OCSP\_RESP\_FIND\_STATUS(3ossl)    OpenSSL    OCSP\_RESP\_FIND\_STATUS(3ossl)

NAME

OCSP\_resp\_find\_status, OCSP\_resp\_count, OCSP\_resp\_get0, OCSP\_resp\_find,  
OCSP\_single\_get0\_status, OCSP\_resp\_get0\_produced\_at,  
OCSP\_resp\_get0\_signature, OCSP\_resp\_get0\_tbs\_sigalg,  
OCSP\_resp\_get0\_respdata, OCSP\_resp\_get0\_certs, OCSP\_resp\_get0\_signer,  
OCSP\_resp\_get0\_id, OCSP\_resp\_get1\_id, OCSP\_check\_validity,  
OCSP\_basic\_verify - OCSP response utility functions

SYNOPSIS

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

int OCSP_resp_find_status(OCSP_BASICRESP *bs, OCSP_CERTID *id, int *status,
    int *reason,
    ASN1_GENERALIZEDTIME **revtime,
    ASN1_GENERALIZEDTIME **thisupd,
    ASN1_GENERALIZEDTIME **nextupd);

int OCSP_resp_count(OCSP_BASICRESP *bs);

OCSP_SINGLERESP *OCSP_resp_get0(OCSP_BASICRESP *bs, int idx);

int OCSP_resp_find(OCSP_BASICRESP *bs, OCSP_CERTID *id, int last);
```

```

int OCSP_single_get0_status(OCSP_SINGLERESP *single, int *reason,
    ASN1_GENERALIZEDTIME **revtime,
    ASN1_GENERALIZEDTIME **thisupd,
    ASN1_GENERALIZEDTIME **nextupd);

const ASN1_GENERALIZEDTIME *OCSP_resp_get0_produced_at(
    const OCSP_BASICRESP* single);

const ASN1_OCTET_STRING *OCSP_resp_get0_signature(const OCSP_BASICRESP *bs);
const X509_ALGOR *OCSP_resp_get0_tbs_sigalg(const OCSP_BASICRESP *bs);
const OCSP_RESPDATA *OCSP_resp_get0_respdata(const OCSP_BASICRESP *bs);
const STACK_OF(X509) *OCSP_resp_get0_certs(const OCSP_BASICRESP *bs);
int OCSP_resp_get0_signer(OCSP_BASICRESP *bs, X509 **signer,
    STACK_OF(X509) *extra_certs);
int OCSP_resp_get0_id(const OCSP_BASICRESP *bs,
    const ASN1_OCTET_STRING **pid,
    const X509_NAME **pname);
int OCSP_resp_get1_id(const OCSP_BASICRESP *bs,
    ASN1_OCTET_STRING **pid,
    X509_NAME **pname);
int OCSP_check_validity(ASN1_GENERALIZEDTIME *thisupd,
    ASN1_GENERALIZEDTIME *nextupd,
    long sec, long maxsec);
int OCSP_basic_verify(OCSP_BASICRESP *bs, STACK_OF(X509) *certs,
    X509_STORE *st, unsigned long flags);

```

## DESCRIPTION

OCSP\_resp\_find\_status() searches bs for an OCSP response for id. If it is successful the fields of the response are returned in \*status, \*reason, \*revtime, \*thisupd and \*nextupd. The \*status value will be one of V\_OCSP\_CERTSTATUS\_GOOD, V\_OCSP\_CERTSTATUS\_REVOKED or V\_OCSP\_CERTSTATUS\_UNKNOWN. The \*reason and \*revtime fields are only set if the status is V\_OCSP\_CERTSTATUS\_REVOKED. If set the \*reason field will be set to the revocation reason which will be one of OCSP\_REVOKED\_STATUS\_NOSTATUS, OCSP\_REVOKED\_STATUS\_UNSPECIFIED, OCSP\_REVOKED\_STATUS\_KEYCOMPROMISE, OCSP\_REVOKED\_STATUS\_CACOMPROMISE,

OCSP\_REVOKED\_STATUS\_AFFILIATIONCHANGED, OCSP\_REVOKED\_STATUS\_SUPERSEDED,  
OCSP\_REVOKED\_STATUS\_CESSATIONOFOPERATION,  
OCSP\_REVOKED\_STATUS\_CERTIFICATEHOLD or  
OCSP\_REVOKED\_STATUS\_REMOVEFROMCRL.

OCSP\_resp\_count() returns the number of OCSP\_SINGLERESP structures in  
bs.

OCSP\_resp\_get0() returns the OCSP\_SINGLERESP structure in bs  
corresponding to index idx, where idx runs from 0 to

OCSP\_resp\_count(bs) - 1.

OCSP\_resp\_find() searches bs for id and returns the index of the first  
matching entry after last or starting from the beginning if last is -1.

OCSP\_single\_get0\_status() extracts the fields of single in \*reason,  
\*revtime, \*thisupd and \*nextupd.

OCSP\_resp\_get0\_produced\_at() extracts the producedAt field from the  
single response bs.

OCSP\_resp\_get0\_signature() returns the signature from bs.

OCSP\_resp\_get0\_tbs\_sigalg() returns the signatureAlgorithm from bs.

OCSP\_resp\_get0\_respdata() returns the tbsResponseData from bs.

OCSP\_resp\_get0\_certs() returns any certificates included in bs.

OCSP\_resp\_get0\_signer() attempts to retrieve the certificate that  
directly signed bs. The OCSP protocol does not require that this  
certificate is included in the certs field of the response, so  
additional certificates can be supplied via the extra\_certs if the  
certificates that may have signed the response are known via some out-  
of-band mechanism.

OCSP\_resp\_get0\_id() gets the responder id of bs. If the responder ID is  
a name then <\*pname> is set to the name and \*pid is set to NULL. If the  
responder ID is by key ID then \*pid is set to the key ID and \*pname is  
set to NULL.

OCSP\_resp\_get1\_id() is the same as OCSP\_resp\_get0\_id() but leaves  
ownership of \*pid and \*pname with the caller, who is responsible for  
freeing them unless the function returns 0.

OCSP\_check\_validity() checks the validity of its thisupd and nextupd

arguments, which will be typically obtained from `OCSP_resp_find_status()` or `OCSP_single_get0_status()`. If `sec` is nonzero it indicates how many seconds leeway should be allowed in the check. If `maxsec` is positive it indicates the maximum age of this upd in seconds. `OCSP_basic_verify()` checks that the basic response message `bs` is correctly signed and that the signer certificate can be validated. It takes `st` as the trusted store and `certs` as a set of untrusted intermediate certificates. The function first tries to find the signer certificate of the response in `certs`. It then searches the certificates the responder may have included in `bs` unless `flags` contains `OCSP_NOINTERN`. It fails if the signer certificate cannot be found. Next, unless `flags` contains `OCSP_NOSIGS`, the function checks the signature of `bs` and fails on error. Then the function already returns success if `flags` contains `OCSP_NOVERIFY` or if the signer certificate was found in `certs` and `flags` contains `OCSP_TRUSTOTHER`. Otherwise the function continues by validating the signer certificate. If `flags` contains `OCSP_PARTIAL_CHAIN` it takes intermediate CA certificates in `st` as trust anchors. For more details, see the description of `X509_V_FLAG_PARTIAL_CHAIN` in "VERIFICATION FLAGS" in `X509_VERIFY_PARAM_set_flags(3)`. If `flags` contains `OCSP_NOCHAIN` it ignores all certificates in `certs` and in `bs`, else it takes them as untrusted intermediate CA certificates and uses them for constructing the validation path for the signer certificate. Certificate revocation status checks using CRLs is disabled during path validation if the signer certificate contains the `id-pkix-ocsp-no-check` extension. After successful path validation the function returns success if the `OCSP_NOCHECKS` flag is set. Otherwise it verifies that the signer certificate meets the OCSP issuer criteria including potential delegation. If this does not succeed and the `OCSP_NOEXPLICIT` flag is not set the function checks for explicit trust for OCSP signing in the root CA certificate.

## RETURN VALUES

`OCSP_resp_find_status()` returns 1 if `id` is found in `bs` and 0 otherwise.

OCSP\_resp\_count() returns the total number of OCSP\_SINGLERESP fields in bs or -1 on error.

OCSP\_resp\_get0() returns a pointer to an OCSP\_SINGLERESP structure or NULL on error, such as idx being out of range.

OCSP\_resp\_find() returns the index of id in bs (which may be 0) or -1 on error, such as when id was not found.

OCSP\_single\_get0\_status() returns the status of single or -1 if an error occurred.

OCSP\_resp\_get0\_produced\_at() returns the producedAt field from bs.

OCSP\_resp\_get0\_signature() returns the signature from bs.

OCSP\_resp\_get0\_tbs\_sigalg() returns the signatureAlgorithm field from bs.

OCSP\_resp\_get0\_respdata() returns the tbsResponseData field from bs.

OCSP\_resp\_get0\_certs() returns any certificates included in bs.

OCSP\_resp\_get0\_signer() returns 1 if the signing certificate was located, or 0 if not found or on error.

OCSP\_resp\_get0\_id() and OCSP\_resp\_get1\_id() return 1 on success, 0 on failure.

OCSP\_check\_validity() returns 1 if thisupd and nextupd are valid time values and the current time + sec is not before thisupd and, if maxsec >= 0, the current time - maxsec is not past nextupd. Otherwise it returns 0 to indicate an error.

OCSP\_basic\_verify() returns 1 on success, 0 on verification not successful, or -1 on a fatal error such as malloc failure.

## NOTES

Applications will typically call OCSP\_resp\_find\_status() using the certificate ID of interest and then check its validity using OCSP\_check\_validity(). They can then take appropriate action based on the status of the certificate.

An OCSP response for a certificate contains thisUpdate and nextUpdate fields. Normally the current time should be between these two values.

To account for clock skew the maxsec field can be set to nonzero in OCSP\_check\_validity(). Some responders do not set the nextUpdate field,

this would otherwise mean an ancient response would be considered valid: the `maxsec` parameter to `OCSP_check_validity()` can be used to limit the permitted age of responses.

The values written to `*revtime`, `*thisupd` and `*nextupd` by `OCSP_resp_find_status()` and `OCSP_single_get0_status()` are internal pointers which MUST NOT be freed up by the calling application. Any or all of these parameters can be set to `NULL` if their value is not required.

#### SEE ALSO

`crypto(7)`, `OCSP_cert_to_id(3)`, `OCSP_request_add1_nonce(3)`,  
`OCSP_REQUEST_new(3)`, `OCSP_response_status(3)`, `OCSP_sendreq_new(3)`,  
`X509_VERIFY_PARAM_set_flags(3)`

#### COPYRIGHT

Copyright 2015-2021 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>.

3.0.7                    2023-07-13    OCSP\_RESP\_FIND\_STATUS(3openssl)