CRL & OCSP report for testevg3e.emsign.com (eMudhra Technologies Limited)

☑ Certificate details   ☑ CRL Checks   ☑ OCSP Checks
☑ Error   ☑ Warning   ☑ Success   ☑ Info
☑ Raw data   Refresh

- testevg3e.emsign.com
- emSign ECC EV SSL CA - G3

testevg3e.emsign.com

Certificate details for testevg3e.emsign.com   (At position 0 in certificate chain)
Serial number:
  hex: ed33c6fbf2bfb5a4eaac
  int: 1120155978708608967043756
Issued by: emSign ECC EV SSL CA - G3
Public Key Algorithm: ECDSA
Not valid before: Thursday, 22 February 2018 11:53 UTC
Not valid after: Friday, 23 February 2018 11:53 UTC
Company registration number: 60368
Organization: eMudhra Technologies Limited
State / Province: Karnataka
Locality: Bangalore
Country: IN

- This certificate does not contain any links to an LDAP server
- This certificate does not contain any internal server links
- This certificate does not contain any links with an unknown format

Check certificate compliance for testevg3e.emsign.com.

Certificate Revocation List (CRL)

This CRL was cached at Monday, 26 February 2018 10:41 UTC

http://crl.emsign.com?emSignECCEVSSLCAG3.crl

CRL information

Source: CRL Distribution Points in Certificate
Location: http://crl.emsign.com?emSignECCEVSSLCAG3.crl
Size: 362 bytes (DER data)
Response time: 455.276778ms
This update: Thursday, 22 February 2018 12:08 UTC
Next update: Thursday, 1 March 2018 12:08 UTC

Revoked: No
Revoked certificates in CRL: 1

Relevant server response headers

Date: Monday, 26 February 2018 10:41 GMT
Last Modified: Thursday, 22 February 2018 12:08 GMT
Expires: Thursday, 1 March 2018 12:08 GMT

- Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- This CRL file is DER encoded
- Issuer field is byte-for-byte equivalent with issuers subject
- Response is already valid
- Response is not expired
- ThisUpdate is less than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3)
- The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
- Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
- NextUpdate is after the date in the Expires cache header
- The Cache-Control max-age header does not outlive NextUpdate
- ThisUpdate has a date before NextUpdate
- Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

Online Certificate Status Protocol (OCSP)

This OCSP response was cached at Monday, 26 February 2018 10:41 UTC

http://ocsp.emSign.com (POST)   Good

OCSP response information

Source: Authority Information Access in Certificate
Location: http://ocsp.emSign.com (POST)
Size: 1157 bytes (DER data)
Response time: 632.597231ms
Signature algorithm: ECDSA-SHA384
Signature type: CA Delegated
Signed by: emSign ECC EV SSL OCSP - G3
Issued by: emSign ECC EV SSL CA - G3
Signing certificate validity: 2018-02-19 - 2019-02-19
Signing certificate algorithm: ECDSA-SHA384
Reported statuses: 1
This update: Monday, 26 February 2018 10:41 UTC
Next update: Wednesday, 28 February 2018 10:41 UTC
Produced at: Monday, 26 February 2018 10:41 UTC
Status: Good

Relevant server response headers

Date: Monday, 26 February 2018 10:41 GMT
Last Modified: Monday, 26 February 2018 10:41 GMT

Expires: Wednesday, 28 February 2018 10:41 GMT

Server and network information

Server Software: Apache-Coyote/1.1

- OCSP signing certificate is already valid
- OCSP signing certificate is not expired
- OCSP signing certificate does not expire before NextUpdate
- OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- OCSP signing certificate does contain the OCSP No Check extension
- OCSP response is valid for at least 8 hours (Microsoft)
- OCSP response is available at least 8 hours before the current period expires or at ½ the validity if valid for more than 16 hours (Microsoft)
- Content-Type in response is set to 'application/ocsp-response'
- Response is already valid
- Response is not expired
- ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements)
  If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it must update that service at least every four days.
- The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
- Last-Modified header is not the same as ThisUpdate (RFC 5019, section 6.2)
- NextUpdate is 1s before the date in the Expires cache header
- The Cache-Control max-age header does not outlive NextUpdate
- ThisUpdate has a date before NextUpdate
- Expires cache header is not the same as the NextUpdate field (RFC 5019 section 6.2)

This OCSP response was cached at Monday, 26 February 2018 10:41 UTC

http://ocsp.emSign.com (GET)   Good

OCSP response information

Source: Authority Information Access in Certificate
Location: http://ocsp.emSign.com (GET)
Size: 1158 bytes (DER data)
Response time: 641.07952ms
Signature algorithm: ECDSA-SHA384
Signature type: CA Delegated
Signed by: emSign ECC EV SSL OCSP - G3
Issued by: emSign ECC EV SSL CA - G3
Signing certificate validity: 2018-02-19 - 2019-02-19
Signing certificate algorithm: ECDSA-SHA384
Reported statuses: 1
This update: Monday, 26 February 2018 10:41 UTC
Next update: Wednesday, 28 February 2018 10:41 UTC
Produced at: Monday, 26 February 2018 10:41 UTC
Status: Good

Relevant server response headers

Date: Monday, 26 February 2018 10:41 GMT
Last Modified: Monday, 26 February 2018 10:41 GMT
Expires: Wednesday, 28 February 2018 10:41 GMT

Server and network information

Server Software: Apache-Coyote/1.1

- OCSP requests is smaller than 255 bytes
- OCSP signing certificate is already valid
- OCSP signing certificate is not expired
- OCSP signing certificate does not expire before NextUpdate
- OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- OCSP signing certificate does contain the OCSP No Check extension
- OCSP response is valid for at least 8 hours (Microsoft)
- OCSP response is available at least 8 hours before the current period expires or at ½ the validity if valid for more than 16 hours (Microsoft)
- Content-Type in response is set to 'application/ocsp-response'
- Response is already valid
- Response is not expired
- ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements)
- The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
- Last-Modified header is not the same as ThisUpdate (RFC 5019, section 6.2)
- NextUpdate is 1s before the date in the Expires cache header
- The Cache-Control max-age header does not outlive NextUpdate
- ThisUpdate has a date before NextUpdate
- Expires cache header is not the same as the NextUpdate field (RFC 5019 section 6.2)

emSign ECC EV SSL CA - G3 (CA Certificate)

Certificate details for emSign ECC EV SSL CA - G3   (At position 1 in certificate chain)
Serial number:
    hex: 1fe3e6c68debbec263e
    int: 9412337563025552451134
Issued by: emSign ECC Root CA - G3
Public Key Algorithm: ECDSA
Not valid before: Sunday, 18 February 2018 18:30 UTC
Not valid after: Friday, 18 February 2033 18:30 UTC
Organization: eMudhra Technologies Limited
Organization unit: emSign PKI
Country: IN
We could not identify the issuer for this certificate

- This certificate does not contain any links to an LDAP server
- This certificate does not contain any internal server links
- This certificate does not contain any links with an unknown format

This certificate contains no information about authoritative CRL(s) or OCSP servers

Check the revocation status for another website

Created by [Paul van Brouwershaven](#)

© 2015 - 2017 [Digitorus B.V.](#)

Revoked certificates can't and should not be trusted, these certificate will cause errors like "NET::ERR_CERT_REVOKED" in browsers.

Check the revocation status for another website