CRL & OCSP report for testevc1e.emsign.com (eMudhra Technologies Limited)

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

- testevc1e.emsign.com
- emSign EV SSL CA - C1

testevc1e.emsign.com

Certificate details for testevc1e.emsign.com (At position 1 in certificate chain)

Serial number:
hex: e1b57974c2f05a640224
int: 1065880071157325054083620
Issued by: emSign EV SSL CA - C1
Public Key Algorithm: RSA
Not valid before: Feb 22, 2018 5:17:51 PM
Not valid after: Feb 23, 2018 5:17:51 PM
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 testevc1e.emsign.com

Upgrade or renew to an EV SSL Certificates for only € 99 ($ 121 or £ 87)

Certificate Revocation List (CRL)

This CRL was cached at Feb 23, 2018 5:45:23 PM

http://crl.emsign.com?emSignEVSSLCAC1.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl.emsign.com?emSignEVSSLCAC1.crl
Size: 532 bytes (DER data)
Response time: 457.596007ms
This update: Feb 22, 2018 6:18:27 PM
Next update: Mar 1, 2018 6:18:27 PM
Revoked: No
Revoked certificates in CRL: 2

Relevant server response headers

Date: Feb 23, 2018 5:45:20 PM
Last Modified: Feb 22, 2018 6:18:27 PM
Expires: Mar 1, 2018 6:18:27 PM

- 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 Feb 24, 2018 12:54:31 PM

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

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.emSign.com
Size: 1605 bytes (DER)
Response time: 626.477729ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: emSign EV SSL OCSP - C1
Issued by: emSign EV SSL CA - C1

Signing certificate validity: Feb 20, 2018 12:00:00 AM - Feb 20, 2019 12:00:00 AM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Feb 24, 2018 12:54:31 PM
Next update: Feb 26, 2018 12:54:31 PM
Produced at: Feb 24, 2018 12:54:32 PM
Status: Good

Relevant server response headers

Date: Feb 24, 2018 12:54:32 PM
Last Modified: Feb 24, 2018 12:54:32 PM
Expires: Feb 26, 2018 12:54:32 PM

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
- 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)

This OCSP response was cached at Feb 24, 2018 12:54:23 PM

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

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.emSign.com
Size: 1605 bytes (DER)
Response time: 649.360668ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: emSign EV SSL OCSP - C1
Issued by: emSign EV SSL CA - C1

Signing certificate validity: Feb 20, 2018 12:00:00 AM - Feb 20, 2019 12:00:00 AM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Feb 24, 2018 12:54:31 PM
Next update: Feb 26, 2018 12:54:31 PM
Produced at: Feb 24, 2018 12:54:32 PM
Status: Good

Relevant server response headers

Date: Feb 24, 2018 12:54:32 PM
Last Modified: Feb 24, 2018 12:54:32 PM
Expires: Feb 26, 2018 12:54:32 PM

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
- 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 EV SSL CA - C1 (CA Certificate)

Certificate details for emSign EV SSL CA - C1 (At position 2 in certificate chain)
Serial number:
hex: badfd29b3f1e678c6960
int: 88248896553496041360096
Issued by: emSign Root CA - C1
Public Key Algorithm: RSA
Not valid before: Feb 19, 2018 12:00:00 AM
Not valid after: Feb 19, 2033 12:00:00 AM
Organization: eMudhra Inc
Organization unit: emSign PKI
Country: US

- 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 emSign EV SSL CA - C1

Certificate Revocation List (CRL)

This CRL was cached at Feb 23, 2018 5:45:23 PM

http://crl.emsign.com?RootCAC1.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl.emsign.com?RootCAC1.crl
Size: 468 bytes (DER data)
Response time: 444.126192ms
This update: Feb 19, 2018 7:08:00 PM
Next update: Aug 18, 2018 7:08:00 PM
Revoked: No
Revoked certificates in CRL: 0

Relevant server response headers

Date: Feb 23, 2018 5:45:20 PM
Last Modified: Feb 19, 2018 7:08:00 PM
Expires: Aug 18, 2018 7:08:00 PM

- 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
- Revocation information is updated at least once every twelve months
- The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
- 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)

Check the revocation status for another website

Created by Paul van Brouwershaven

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