CRL & OCSP report for expeu.ca.darkmatter.ae (Dark Matter L.L.C.)

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

- expeu.ca.darkmatter.ae
- DarkMatter Secure CA

---

expeu.ca.darkmatter.ae

Certificate details for expeu.ca.darkmatter.ae (At position 1 in certificate chain)

- **Serial number:**
  - **hex:** 633ad3ae74479fac
  - **int:** 7150260104632704940

- **Issued by:** DarkMatter Secure CA

- **Public Key Algorithm:** ECDSA

- **Not valid before:** Feb 6, 2018 1:23:12 PM
- **Not valid after:** Feb 7, 2018 1:23:12 PM

- **Organization:** Dark Matter L.L.C.
- **State / Province:** Abu Dhabi
- **Locality:** Abu Dhabi
- **Country:** AE

- 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 expeu.ca.darkmatter.ae

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

---

Email Security Software

Protect your network from email borne threats w/ GFI MailEssentials. Free Trial. gfi

---

Certificate Revocation List (CRL)
This CRL was cached at May 21, 2018 4:24:00 PM

http://crl1.darkmatter.ae/dmsecureca.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl1.darkmatter.ae/dmsecureca.crl
Size: 1478 bytes (DER data)
Response time: 839.709533ms
This update: May 21, 2018 4:51:43 AM
Next update: May 24, 2018 4:51:43 AM
Revoked: No
Revoked certificates in CRL: 19

Relevant server response headers

Date: May 21, 2018 4:24:21 PM
Last Modified: Jan 1, 1 4:00:00 AM
Expires: Jan 1, 1 4:00:00 AM

Server and network information

Server Software: Apache

- 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 should be 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 cache header not set (RFC 5019, section 6.2)
- Expires cache header not set (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)

This CRL was cached at May 21, 2018 4:24:00 PM

http://crl2.darkmatter.ae/dmsecureca.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl2.darkmatter.ae/dmsecureca.crl
Size: 1478 bytes (DER data)
Response time: 860.041076ms
This update: May 21, 2018 4:51:43 AM
Next update: May 24, 2018 4:51:43 AM
Revoked: No
Revoked certificates in CRL: 19

Relevant server response headers

Date: May 21, 2018 4:24:21 PM
Last Modified: Jan 1, 1 4:00:00 AM
Expires: Jan 1, 1 4:00:00 AM

Server and network information

Server Software: Apache

- 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 should be 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 cache header not set (RFC 5019, section 6.2)
- Expires cache header not set (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 May 22, 2018 11:44:03 AM

http://ocsp.darkmatter.ae (GET)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.darkmatter.ae
Size: 1725 bytes (DER)
Response time: 451.450652ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: DarkMatter OCSP Authority Signature
Issued by: DarkMatter Secure CA
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: May 22, 2018 11:43:57 AM
Next update: May 24, 2018 11:43:57 AM
Produced at: May 22, 2018 11:43:57 AM
Status: Good

Relevant server response headers

Date: May 22, 2018 11:43:57 AM
Last Modified: May 22, 2018 11:43:57 AM
Expires: May 24, 2018 11:43:57 AM

Server and network information

Server Software: Apache

- 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 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)

This OCSP response was cached at May 22, 2018 11:43:55 AM

http://ocsp.darkmatter.ae (POST)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.darkmatter.ae
Size: 1725 bytes (DER)
Response time: 441.4704ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: DarkMatter OCSP Authority Signature
Issued by: DarkMatter Secure CA
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: May 22, 2018 11:43:57 AM
Next update: May 24, 2018 11:43:57 AM
Produced at: May 22, 2018 11:43:57 AM
Status: Good

Relevant server response headers

Date: May 22, 2018 11:43:57 AM
Last Modified: Jan 1, 1 4:00:00 AM
Expires: Jan 1, 1 4:00:00 AM

Server and network information

Server Software: Apache

- 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 cache header not set (RFC 5019, section 6.2)
- Expires cache header not set (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)

DarkMatter Secure CA (CA Certificate)

Certificate details for DarkMatter Secure CA

Serial number:
- hex: 627a61b10e7f5f27be3beb5e94cf7ff448dee1c5
- int: 562210296595941878767856233473751741071091491269

Issued by: QuoVadis Root CA 2 G3
Public Key Algorithm: RSA
Not valid before: Apr 19, 2017 10:27:31 PM
Not valid after: Apr 19, 2025 10:27:31 PM
Organization: DarkMatter LLC
Country: AE

- 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

Certificate Revocation List (CRL)

This CRL was cached at Mar 10, 2018 4:14:34 PM

http://crl1.darkmatter.ae/qvrca2g3.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl1.darkmatter.ae/qvrca2g3.crl
Size: 845 bytes (DER data)
Response time: 1.154862109s
This update: Dec 22, 2017 7:51:22 PM
Next update: Jun 20, 2018 7:51:22 PM
Revoked: No
Revoked certificates in CRL: 2

Relevant server response headers

Date: Mar 10, 2018 4:14:23 PM
Last Modified: Mar 10, 2018 4:10:03 PM
Expires: Jan 1, 1 4:00:00 AM

Server and network information

Server Software: AmazonS3

- Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- This CRL file is DER encoded
- Response is already valid
- Response is not expired
- ThisUpdate is more 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 not the same as ThisUpdate (RFC 5019, section 6.2)
• Expires cache header not set (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)

This CRL was cached at Mar 10, 2018 4:14:35 PM

http://crl2.darkmatter.ae/qvrca2g3.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl2.darkmatter.ae/qvrca2g3.crl
Size: 845 bytes (DER data)
Response time: 837.575563ms
This update: Dec 22, 2017 7:51:22 PM
Next update: Jun 20, 2018 7:51:22 PM
Revoked: No
Revoked certificates in CRL: 2

Relevant server response headers

Date: Mar 10, 2018 4:14:24 PM
Last Modified: Mar 10, 2018 4:10:03 PM
Expires: Jan 1, 1 4:00:00 AM

Server and network information

Server Software: AmazonS3

• Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
• This CRL file is DER encoded
• Response is already valid
• Response is not expired
• ThisUpdate is more 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 not the same as ThisUpdate (RFC 5019, section 6.2)
• Expires cache header not set (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
© 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.