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

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

One of the certificates in this chain can't be trusted!

One or more certificate in this chain can't be trusted because of revocation or an server error. Revoked certificates can't be trusted and will cause errors like "NET::ERR_CERT_REVOKED" in browsers

- revrd.ca.darkmatter.ae
- DarkMatter Secure CA
- QuoVadis Root CA 2 G3

revrd.ca.darkmatter.ae

Certificate details for revrd.ca.darkmatter.ae
Serial number: 
  hex: 60953da667a97999
  int: 6959536584083995033
Issued by: DarkMatter Secure CA
Public Key Algorithm: RSA
Not valid before: Feb 5, 2018 3:55:34 PM
Not valid after: Feb 5, 2020 3:55:34 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 revrd.ca.darkmatter.ae

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

This CRL was cached at May 21, 2018 4:25:58 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: 864.553296ms
This update: May 21, 2018 4:51:43 AM
Next update: May 24, 2018 4:51:43 AM
Revoked at: Feb 7, 2018 3:07:22 PM
Revoked certificates in CRL: 19

Relevant server response headers

Date: May 21, 2018 4:26:01 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 4:25:58 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: 844.318503ms
This update: May 21, 2018 4:51:43 AM
Next update: May 24, 2018 4:51:43 AM
Revoked at: Feb 7, 2018 3:07:22 PM
Revoked certificates in CRL: 19

Relevant server response headers

Date: May 21, 2018 4:26:01 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 11:45:10 AM

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

OCSP response information
**Source:** OCSP server listed in Certificate  
**Location:** http://ocsp.darkmatter.ae  
**Size:** 1710 bytes (DER)  
**Response time:** 467.286035ms  
**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 11:45:12 AM  
**Next update:** May 24, 2018 11:45:12 AM  
**Produced at:** May 22, 2018 11:45:12 AM  
**Status:** Revoked  

**Relevant server response headers**

- **Date:** May 22, 2018 11:45:12 AM  
- **Last Modified:** May 22, 2018 11:45:12 AM  
- **Expires:** May 24, 2018 11:45:12 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 11:44:51 AM  

http://ocsp.darkmatter.ae (POST)
OCSP response information

Source: OCSP server listed in Certificate  
Location: http://ocsp.darkmatter.ae  
Size: 1710 bytes (DER)  
Response time: 449.883034ms  
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 11:45:12 AM  
Next update: May 24, 2018 11:45:12 AM  
Produced at: May 22, 2018 11:45:12 AM  
Status: Revoked

Relevant server response headers

Date: May 22, 2018 11:45:12 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**: 627a61b10e7f5f27be3beb5e94cf7f448dee1c5
- **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](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)**

This OCSP response was cached at May 22, 2018 11:35:23 AM

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

**OCSP response information**

**Source:** OCSP server listed in Certificate  
**Location:** http://ocsp.quovadisglobal.com  
**Size:** 1825 bytes (DER)  
**Response time:** 230.196687ms  
**Signature algorithm:** SHA256-RSA  
**Signature type:** CA Delegated  
**Signed by:** QuoVadis OCSP Authority Signature  
**Issued by:** QuoVadis Root CA 2 G3  
**Signing certificate validity:** Nov 9, 2016 12:49:39 AM - Nov 9, 2026 12:49:39 AM  
**Signing certificate algorithm:** SHA256-RSA  
**Reported statuses:** 1  
**This update:** May 22, 2018 11:35:44 AM  
**Next update:** May 24, 2018 11:35:44 AM  
**Produced at:** May 22, 2018 11:35:44 AM  
**Status:** Good

**Relevant server response headers**

**Date:** May 22, 2018 11:35:44 AM  
**Last Modified:** May 22, 2018 11:35:44 AM  
**Expires:** May 24, 2018 11:35:44 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 11:35:42 AM

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

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.quovadisglobal.com
Size: 1825 bytes (DER)
Response time: 250.874524ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: QuoVadis OCSP Authority Signature
Issued by: QuoVadis Root CA 2 G3
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: May 22, 2018 11:35:44 AM
Next update: May 24, 2018 11:35:44 AM
Produced at: May 22, 2018 11:35:44 AM
Status: Good

Relevant server response headers

Date: May 22, 2018 11:35:44 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)

**QuoVadis Root CA 2 G3 (CA Certificate)**

Certificate details for QuoVadis Root CA 2 G3 (At position 3 in certificate chain)

- **Serial number:**
  - **hex:** 445734245b81899b35f2ceb82b3b5ba726f07528
  - **int:** 390156079458959257446133169266079962026824725800
- **Issued by:** QuoVadis Root CA 2 G3
- **Public Key Algorithm:** RSA
- **Not valid before:** Jan 12, 2012 10:59:32 PM
- **Not valid after:** Jan 12, 2042 10:59:32 PM
- **Organization:** QuoVadis Limited
- **Country:** BM

- 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 is a self signed certificate

Check certificate compliance for QuoVadis Root CA 2 G3

Check the revocation status for another website
Revoked certificates can't and should not be trusted; these certificates will cause errors like "NET::ERR_CERT_REVOKED" in browsers.