Signature SIGNATURE_Charlotte-De-Meersman-Signature_20230925-1020 — TOTAL_FAILED - SIG_CRYPTO_FAILURE

Validation Process for Basic Signatures (Best signature time : 2023-10-07 21:30:15 (UTC)) — FAILED - SIG_CRYPTO_FAILURE

- Is the result of the 'Format Checking' building block conclusive? ✓
- Is the result of the 'Identification of Signing Certificate' building block conclusive? ✓
- Is the result of the 'Validation Context Initialization' building block conclusive? ✓
- Is the result of the 'X.509 Certificate Validation' building block conclusive? ✓
- Is the result of the 'Cryptographic Verification' building block conclusive? ✗
  The result of the 'Cryptographic Verification' building block is not conclusive!

Timestamp TIMESTAMP_Timestamp-Unit_20230925-1020 — PASSED

Validation Process for Time-stamps (Production time : 2023-09-25 10:20:50 (UTC)) — PASSED

- Is the result of the 'Identification of Signing Certificate' building block conclusive? ✓
- Is the result of the 'X.509 Certificate Validation' building block conclusive? ✓
- Is the result of the 'Cryptographic Verification' building block conclusive? ✓
- Is the result of the 'Signature Acceptance Validation' building block conclusive? ✓

Time-stamp Qualification — QTSA

- Has a trusted list been reached for the certificate chain? ✓
- Is the list of trusted lists acceptable? ✓
  Trusted List : https://ec.europa.eu/tools/lotl/eu-lotl.xml
- Is the trusted list acceptable? ✓
  Trusted List : https://tsl.belgium.be/tsl-be.xml
- Has been an acceptable trusted list found? ✓
- Is the certificate related to a TSA/QTST? ✓
- Is the certificate related to a trust service with a granted status? ✓
- Is the certificate related to a trust service with a granted status at the production time? ✓

Validation Process for Signatures with Time and Signatures with Long-Term Validation Data (Best signature time : 2023-10-07 21:30:15 (UTC)) — FAILED - SIG_CRYPTO_FAILURE

- Is the result of the Basic Validation Process acceptable? ✗
  The result of the Basic validation process is not acceptable to continue the process!

Validation Process for Signatures with Archival Data (Best signature time : 2023-10-07 21:30:15 (UTC)) — FAILED - SIG_CRYPTO_FAILURE

- Is the result of the LTV validation process acceptable? ✗
  The result of the LTV validation process is not acceptable to continue the process!

Signature Qualification — Not AdES but QC with QSCD

- Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)? !
  The signature/seal is not a valid AdES digital signature!
- Has a trusted list been reached for the certificate chain? ✓
- Is the list of trusted lists acceptable? ✓
  Trusted List : https://ec.europa.eu/tools/lotl/eu-lotl.xml
- Is the trusted list acceptable? ✓
  Trusted List : https://tsl.belgium.be/tsl-be.xml
- Has been an acceptable trusted list found? ✓
- Is the certificate qualified at (best) signing time? ✓
- Is the certificate type unambiguously identified at (best) signing time? ✓
- Is the certificate qualified at issuance time? ✓
- Does the private key reside in a QSCD at (best) signing time? ✓

Certificate Qualification at certificate issuance time (2016-07-26 18:27:52 (UTC)) — QC for eSig with QSCD

- Is the certificate related to a trust service at certificate issuance time? ✓
- Is the certificate related to a CA/QC? ✓
- May a related trust service issue certificates of a suitable type? ✓
- Is the trust service consistent? ✓
  Trust service name : CN=Belgium Root CA4, C=BE
- Is the certificate related to a trust service with a granted status? ✓
- Does the trusted certificate match the trust service? !
  The organization name is missing in the trusted certificate!
- Is the certificate related to a qualified certificate issuing trust service with valid status? ✓
- Is the certificate related to a consistent by QC trust service declaration? ✓
- Is the certificate qualified at issuance time? ✓
- Can the certificate type be issued by a found trust service? ✓
- Is the certificate type unambiguously identified at issuance time? ✓
  Certificate type is for eSig
- Is the certificate related to a consistent by QSCD trust service declaration? ✓
- Does the private key reside in a QSCD at issuance time? ✓

Certificate Qualification at best signature time (2023-10-07 21:30:15 (UTC)) — **QC for eSig with QSCD**

- Is the certificate related to a trust service at best signature time? ✓
- Is the certificate related to a CA/QC? ✓
- May a related trust service issue certificates of a suitable type? ✓
- Is the trust service consistent? ✓
  Trust service name : CN=Belgium Root CA4, C=BE
- Is the certificate related to a trust service with a granted status? ✓
- Does the trusted certificate match the trust service? !
  The organization name is missing in the trusted certificate!
- Is the certificate related to a qualified certificate issuing trust service with valid status? ✓
- Is the certificate related to a consistent by QC trust service declaration? ✓
- Is the certificate qualified at (best) signing time? ✓
- Can the certificate type be issued by a found trust service? ✓
- Is the certificate type unambiguously identified at (best) signing time? ✓
  Certificate type is for eSig
- Is the certificate related to a consistent by QSCD trust service declaration? ✓
- Does the private key reside in a QSCD at (best) signing time? ✓

Basic Building Blocks

SIGNATURE - SIGNATURE_Charlotte-De-Meersman-Signature_20230925-1020

Format Checking : PASSED

- Does the signature format correspond to an expected format? ✓
- Is the signature identification not ambiguous? ✓
- Is the signed references identification not ambiguous? ✓
- Is only one SignerInfo present? ✓
- Is the /ByteRange dictionary consistent? ✓
- Does the /ByteRange not overlap with other signature/timestamp? ✓
- Is the signature dictionary consistent? ✓
- Do signed and final revisions contain equal amount of pages? ✓
- Is no element overlapping detected in the PDF? ✓
- Is there no visual difference between signed and final revisions in the PDF? ✓
- Does the document contain none of the undefined object modifications? ✓

Identification of the Signing Certificate : PASSED

- Is there an identified candidate for the signing certificate? ✓
- Is the signed attribute: 'cert-digest' of the certificate present? ✓
- Does the certificate digest value match a digest value found in the certificate reference(s)? ✓

Validation Context Initialization : PASSED

- Is the signature policy known? ✓

X509 Certificate Validation : PASSED

- Can the certificate chain be built till a trust anchor? ✓
- Is the certificate validation conclusive? ✓
- Is the certificate validation conclusive? ✓
- Is the certificate validation conclusive? ✓

Certificate CERTIFICATE_Charlotte-De-Meersman-Signature_20160726-1827 : PASSED

- Is the certificate unique? ✓
- Is a pseudonym used? ✓
- Is certificate not self-signed? ✓
- Is the certificate signature intact? ✓
- Does the certificate have an expected key-usage? ✓
  Key usage : [NON_REPUDIATION]
- Is the authority info access present? ✓
- Is the certificate's policy tree valid? ✓
- Do certificate's subject names satisfy the imposed name constraints? ✓
- Are all found critical certificate extensions supported? ✓
- Are all found certificate extensions allowed for the certificate? ✓
- Is the revocation info access present? ✓
- Is the revocation data present for the certificate? ✓
- Is an acceptable revocation data present for the certificate? ✓
  Latest acceptable revocation : OCSP_Belgium-OCSP-Responder_20231007-2130
- Is the certificate not revoked? ✓
- Is the certificate not on hold? ✓
- Is the revocation freshness check conclusive? ✓
  Id = OCSP_Belgium-OCSP-Responder_20231007-2130
- Are cryptographic constraints met for the signature's certificate chain? ✓
  Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30
- Is the current time in the validity range of the signer's certificate? ✓
  Validation time : 2023-10-07 21:30, certificate validity : 2016-07-26 18:27 - 2026-07-12 23:59

Is the current time in the validity range of the certificate of the issuer of the revocation information?
Issuer certificate CERTIFICATE_Belgium-OCSP-Responder_20221114-1100 of revocation data OCSP_Belgium-OCSP-Responder_20231007-2130 with validity range : 2022-11-14 11:00 - 2024-01-31 11:00 and validation time 2023-10-07 21:30

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive?
Id = OCSP_Belgium-OCSP-Responder_20231007-2130, thisUpdate = 2023-10-07 21:30, production time = 2023-10-07 21:30

Is the revocation acceptance check conclusive?
Id = OCSP_Belgium-OCSP-Responder_20230925-1020, thisUpdate = 2023-09-25 10:20, production time = 2023-09-25 10:20

Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : OCSP_Belgium-OCSP-Responder_20231007-2130

Revocation Acceptance Checker : PASSED

Is the revocation status known?

Does the ResponderId match the OCSP issuer certificate?

Is it not self issued OCSP Response?

Is the revocation data consistent?
Revocation thisUpdate 2023-10-07 21:30 is in the certificate validity range : 2016-07-26 18:27 - 2026-07-12 23:59

Is revocation's signature intact?

Can the certificate chain be built till a trust anchor?

Is certificate's signature intact?
Id = CERTIFICATE_Belgium-OCSP-Responder_20221114-1100

Has the issuer certificate id-pkix-ocsp-nocheck extension?

Is certificate's signature intact?
Id = CERTIFICATE_Citizen-CA_20151125-1000

Is the revocation data present for the revocation issuer?

Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

2023-10-07T21:30:15Z

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100, thisUpdate = 2023-07-01 11:00, production time = 2023-07-01 11:00

Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

Revocation Acceptance Checker : PASSED

Is the revocation status known?

Is the revocation data consistent?
Revocation thisUpdate 2023-07-01 11:00 is in the certificate validity range : 2015-11-25 10:00 - 2027-07-25 10:00

Is revocation's signature intact?

Can the certificate chain be built till a trust anchor?

2023-07-01T11:00:00Z

Revocation Acceptance Checker : PASSED

Is the revocation status known?

Does the ResponderId match the OCSP issuer certificate?

Is it not self issued OCSP Response?

Is the revocation data consistent?
Revocation thisUpdate 2023-09-25 10:20 is in the certificate validity range : 2016-07-26 18:27 - 2026-07-12 23:59

Is revocation's signature intact?

Can the certificate chain be built till a trust anchor?

2023-09-25T10:20:37Z

Revocation Freshness Checker : PASSED

Is the revocation information fresh for the certificate?

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2023-10-07 21:30

Certificate CERTIFICATE_Citizen-CA_20151125-1000 : PASSED

Is the certificate signature intact?

Is the certificate a CA certificate?

Is the certificate's path depth valid?

Does the certificate have an expected key-usage?
Key usage : [KEY_CERT_SIGN, CRL_SIGN]

Is the certificate's policy tree valid?

Do certificate's subject names satisfy the imposed name constraints?

Are all found critical certificate extensions supported?

Are all found certificate extensions allowed for the certificate?

Is the revocation data present for the certificate?

Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

Is the certificate not revoked?

Is the certificate not on hold?

Is the revocation freshness check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100

Are cryptographic constraints met for the signature's certificate chain?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100, thisUpdate = 2023-07-01 11:00, production time = 2023-07-01 11:00

Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

Revocation Acceptance Checker : PASSED

Is the revocation status known?

Is the revocation data consistent?
Revocation thisUpdate 2023-07-01 11:00 is in the certificate validity range : 2015-11-25 10:00 - 2027-07-25 10:00

Is revocation's signature intact?

Can the certificate chain be built till a trust anchor?
2023-07-01T11:00:00Z

Revocation Freshness Checker : PASSED

Is there a Next Update defined for the revocation data?

Is the revocation information fresh for the certificate?

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Trust Anchor (CERTIFICATE_Belgium-Root-CA4_20130626-1200_2) (Self Signed) PASSED
Equivalent certification: CERTIFICATE_Belgium-Root-CA4_20130626-1200

Cryptographic Verification : FAILED - SIG_CRYPTO_FAILURE

Has the reference data object been found?
Reference : MESSAGE_DIGEST

Is the reference data object intact?
Reference : MESSAGE_DIGEST

Is the signature intact?
The signature is not intact!

Signature Acceptance Validation : PASSED

Is the structure of the signature valid?

Is the signed attribute: 'signing-certificate' present?

Is the signed attribute: 'signing-certificate' present only once?

Does the 'Signing Certificate' attribute contain references only to the certificate chain?

Is the signed qualifying property: 'signing-time' present?

Is the signed qualifying property: 'message-digest' or 'SignedProperties' present?

Are cryptographic constraints met for the signature creation?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2023-10-07 21:30

Are cryptographic constraints met for the message digest?
Digest algorithm SHA256 at validation time : 2023-10-07 21:30 for message digest

Are cryptographic constraints met for the signing-certificate reference?
Digest algorithm SHA256 at validation time : 2023-10-07 21:30 for signing-certificate reference with Id : CERTIFICATE_Charlotte-De-Meersman-Signature_20160726-1827

Basic Building Blocks
TIMESTAMP - TIMESTAMP_Timestamp-Unit_20230925-1020

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

Is the signed attribute: 'cert-digest' of the certificate present?

Are the issuer distinguished name and the serial number equal?

X509 Certificate Validation : PASSED

Can the certificate chain be built till a trust anchor?

Is the certificate validation conclusive?

Trust Anchor (CERTIFICATE_Timestamp-Unit_20210316-0940) PASSED

Cryptographic Verification : PASSED

Has the message imprint data been found?

Is the message imprint data intact?

Is time-stamp's signature intact?

Signature Acceptance Validation : PASSED

Is the signed attribute: 'signing-certificate' present?

Does the 'Signing Certificate' attribute contain references only to the certificate chain?

Does the TST Info field: 'tsa' match the time-stamp's issuer name?

Are cryptographic constraints met for the time-stamp signature?
Signature algorithm ECDSA with SHA256 with key size 256 at validation time : 2023-10-07 21:30

Are cryptographic constraints met for the time-stamp message imprint?
Digest algorithm SHA256 at validation time : 2023-10-07 21:30 for time-stamp message imprint

Basic Building Blocks
REVOCATION - OCSP_BRCA6-OCSP-Responder_20231007-2130

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : PASSED

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?
Is the certificate validation conclusive?

Certificate CERTIFICATE_BRCA6-OCSP-Responder_20221207-1308 : PASSED

Is the certificate signature intact?
Is the certificate's policy tree valid?
Do certificate's subject names satisfy the imposed name constraints?
Are all found critical certificate extensions supported?
Has the issuer certificate id-pkix-ocsp-nocheck extension?
Are cryptographic constraints met for the revocation data's certificate chain?
Signature algorithm ECDSA with SHA384 with key size 384 at validation time : 2023-10-07 21:30
Is the current time in the validity range of the signer's certificate?
Validation time : 2023-10-07 21:30, certificate validity : 2022-12-07 13:08 - 2024-12-06 13:08

Trust Anchor (CERTIFICATE_Belgium-Root-CA6_20200603-1001) (Self Signed) PASSED

Cryptographic Verification : PASSED

Is revocation's signature intact?

Signature Acceptance Validation : PASSED

Are cryptographic constraints met for the revocation data signature?
Signature algorithm ECDSA with SHA256 with key size 256 at validation time : 2023-10-07 21:30

Basic Building Blocks
REVOCATION - CRL_Belgium-Root-CA4_20230701-1100

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : PASSED

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?

Trust Anchor (CERTIFICATE_Belgium-Root-CA4_20130626-1200_2) (Self Signed) PASSED
Equivalent certification: CERTIFICATE_Belgium-Root-CA4_20130626-1200

Cryptographic Verification : PASSED

Is revocation's signature intact?

Signature Acceptance Validation : PASSED

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Basic Building Blocks
REVOCATION - OCSP_Belgium-OCSP-Responder_20231007-2130

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : PASSED

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?
Is the certificate validation conclusive?
Is the certificate validation conclusive?

Certificate CERTIFICATE_Belgium-OCSP-Responder_20221114-1100 : PASSED

Is the certificate signature intact?
Is the certificate's policy tree valid?
Do certificate's subject names satisfy the imposed name constraints?
Are all found critical certificate extensions supported?
Has the issuer certificate id-pkix-ocsp-nocheck extension?
Are cryptographic constraints met for the revocation data's certificate chain?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30
Is the current time in the validity range of the signer's certificate?
Validation time : 2023-10-07 21:30, certificate validity : 2022-11-14 11:00 - 2024-01-31 11:00

Certificate CERTIFICATE_Citizen-CA_20151125-1000 : PASSED

Is the certificate signature intact?
Is the certificate a CA certificate?
Is the certificate's path depth valid?
Does the certificate have an expected key-usage?
Key usage : [KEY_CERT_SIGN, CRL_SIGN]
Is the certificate's policy tree valid?
Do certificate's subject names satisfy the imposed name constraints?
Are all found critical certificate extensions supported?
Are all found certificate extensions allowed for the certificate?

Is the revocation data present for the certificate?
Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100
Is the certificate not revoked?
Is the certificate not on hold?
Is the revocation freshness check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100
Are cryptographic constraints met for the revocation data's certificate chain?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Certificate Revocation Data Selector : **PASSED**

Is the revocation acceptance check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100, thisUpdate = 2023-07-01 11:00, production time = 2023-07-01 11:00
Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

Revocation Acceptance Checker : **PASSED**

Is the revocation status known?
Is the revocation data consistent?
Revocation thisUpdate 2023-07-01 11:00 is in the certificate validity range : 2015-11-25 10:00 - 2027-07-25 10:00
Is revocation's signature intact?
Can the certificate chain be built till a trust anchor?
2023-07-01T11:00:00Z

Revocation Freshness Checker : **PASSED**

Is there a Next Update defined for the revocation data?
Is the revocation information fresh for the certificate?
Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Trust Anchor (CERTIFICATE_Belgium-Root-CA4_20130626-1200) (Self Signed) **PASSED**
Equivalent certification: CERTIFICATE_Belgium-Root-CA4_20130626-1200_2

Cryptographic Verification : **PASSED**

Is revocation's signature intact?

Signature Acceptance Validation : **PASSED**

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2023-10-07 21:30

Basic Building Blocks
REVOCATION - CRL_Belgium-Root-CA6_20221207-1319

Identification of the Signing Certificate : **PASSED**

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : **PASSED**

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?

Trust Anchor (CERTIFICATE_Belgium-Root-CA6_20200603-1001) (Self Signed) **PASSED**

Cryptographic Verification : **PASSED**

Is revocation's signature intact?

Signature Acceptance Validation : **PASSED**

Are cryptographic constraints met for the revocation data signature?
Signature algorithm ECDSA with SHA384 with key size 384 at validation time : 2023-10-07 21:30

Basic Building Blocks
REVOCATION - OCSP_Belgium-OCSP-Responder_20230925-1020

Identification of the Signing Certificate : **PASSED**

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : **PASSED**

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?
Is the certificate validation conclusive?
Is the certificate validation conclusive?

Certificate CERTIFICATE_Belgium-OCSP-Responder_20221114-1100 : **PASSED**

Is the certificate signature intact?
Is the certificate's policy tree valid?
Do certificate's subject names satisfy the imposed name constraints?
Are all found critical certificate extensions supported?
Has the issuer certificate id-pkix-ocsp-nocheck extension?
Are cryptographic constraints met for the revocation data's certificate chain?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Is the current time in the validity range of the signer's certificate?
Validation time : 2023-10-07 21:30, certificate validity : 2022-11-14 11:00 - 2024-01-31 11:00

Certificate CERTIFICATE_Citizen-CA_20151125-1000 : PASSED

Is the certificate signature intact?
Is the certificate a CA certificate?
Is the certificate's path depth valid?
Does the certificate have an expected key-usage?
Key usage : [KEY_CERT_SIGN, CRL_SIGN]
Is the certificate's policy tree valid?
Do certificate's subject names satisfy the imposed name constraints?
Are all found critical certificate extensions supported?
Are all found certificate extensions allowed for the certificate?
Is the revocation data present for the certificate?
Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100
Is the certificate not revoked?
Is the certificate not on hold?
Is the revocation freshness check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100
Are cryptographic constraints met for the revocation data's certificate chain?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive?
Id = CRL_Belgium-Root-CA4_20230701-1100, thisUpdate = 2023-07-01 11:00, production time = 2023-07-01 11:00
Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_Belgium-Root-CA4_20230701-1100

Revocation Acceptance Checker : PASSED

Is the revocation status known?
Is the revocation data consistent?
Revocation thisUpdate 2023-07-01 11:00 is in the certificate validity range : 2015-11-25 10:00 - 2027-07-25 10:00
Is revocation's signature intact?
Can the certificate chain be built till a trust anchor?
2023-07-01T11:00:00Z

Revocation Freshness Checker : PASSED

Is there a Next Update defined for the revocation data?
Is the revocation information fresh for the certificate?
Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-10-07 21:30

Trust Anchor (CERTIFICATE_Belgium-Root-CA4_20130626-1200) (Self Signed) PASSED
Equivalent certification: CERTIFICATE_Belgium-Root-CA4_20130626-1200_2

Cryptographic Verification : PASSED

Is revocation's signature intact?

Signature Acceptance Validation : PASSED

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2023-10-07 21:30

List Of Trusted Lists EU PASSED

Is the trusted list fresh?
Is the trusted list not expired?
Does the trusted list have the expected version?
Is the trusted list well signed?

Trusted List BE PASSED

Is the trusted list fresh?
Is the trusted list not expired?
Does the trusted list have the expected version?
Is the trusted list well signed?