Signature SIGNATURE_RNDr-Ing-Jiří-Peterka_20220702-2004 — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

Validation Process for Basic Signatures (Best signature time : 2022-07-03 14:51:42 (UTC)) — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

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? ✓

Is the result of the 'Signature Acceptance Validation' building block conclusive? !
The result of the 'Signature Acceptance Validation' building block is not conclusive!

Is the result of the Basic Validation Process conclusive? ✗
Basic Signature Validation process failed with INDETERMINATE/CRYPTO_CONSTRAINTS_FAILURE_NO_POE indication
The result of the Basic validation process is not conclusive!

Timestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005 — PASSED

Validation Process for Time-stamps (Production time : 2022-07-02 20:05:05 (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.gov.cz/publ/TSL_CZ.xtsl

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? ✓

Timestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005 — PASSED

Validation Process for Time-stamps (Production time : 2022-07-02 20:05:05 (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.gov.cz/publ/TSL_CZ.xtsl

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 : 2022-07-02 20:05:05 (UTC)) — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

Is the result of the Basic Validation Process acceptable? ✓

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Are cryptographic constraints met for the signature creation? ✗
The algorithm SHA1 is no longer considered reliable for signature creation! for the token at the validation time : 2022-07-02 20:05
The algorithm SHA1 is no longer considered reliable for signature creation!

Certificate Revocation Data Selector : — PASSED

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, thisUpdate = 2022-07-03 14:51, production time = 2022-07-03 14:51

Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925

Is the revocation acceptance check conclusive? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925, thisUpdate = 2022-07-02 19:25, production time = 2022-07-02 19:25

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005, thisUpdate = 2022-07-02 20:05, production time = 2022-07-02 20:05

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Validation Process for Signatures with Archival Data (Best signature time : 2022-07-02 20:05:05 (UTC)) — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

Is the result of the LTV validation process acceptable? ✓

Is the result of the Time-stamp Validation Building Block acceptable? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
Digest algorithm SHA256 at validation time : 2022-07-03 14:51 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005

Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the result of the Time-stamp Validation Building Block acceptable? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
Digest algorithm SHA256 at validation time : 2022-07-03 14:51 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005

Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005, production time = 2022-07-02 20:05

Is the past signature validation conclusive? ✗
The past signature validation is not conclusive!

Signature Qualification — Indeterminate QESig

Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)? !
The signature/seal is an INDETERMINATE 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.gov.cz/publ/TSL_CZ.xtsl

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 (2022-07-01 06:30:42 (UTC)) — QC for eSig with QSCD

Is the certificate related to a CA/QC? ✓

Is the trust service consistent? ✓
Trust service name : (116) PostSignum - vydávání kvalifikovaných certifikátů

Is the certificate related to a trust service with a granted status? ✓

Is the certificate related to a consistent trust service declaration? ✓

Can the certificate type be issued by a found trust service? ✓

Does the trusted certificate match the trust service? ✓

Is the certificate qualified at issuance time? ✓

Is the certificate type unambiguously identified at issuance time? ✓
Certificate type is for eSig

Does the private key reside in a QSCD at issuance time? ✓

Certificate Qualification at best signature time (2022-07-02 20:05:05 (UTC)) — QC for eSig with QSCD

Is the certificate related to a CA/QC? ✓

Is the trust service consistent? ✓
Trust service name : (116) PostSignum - vydávání kvalifikovaných certifikátů

Is the certificate related to a trust service with a granted status? ✓

Is the certificate related to a consistent trust service declaration? ✓

Can the certificate type be issued by a found trust service? ✓

Does the trusted certificate match the trust service? ✓

Is the certificate qualified at (best) signing time? ✓

Is the certificate type unambiguously identified at (best) signing time? ✓
Certificate type is for eSig

Does the private key reside in a QSCD at (best) signing time? ✓

Basic Building Blocks
SIGNATURE - SIGNATURE_RNDr-Ing-Jiří-Peterka_20220702-2004

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? ✓

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)? ✓
Are the issuer distinguished name and the serial number equal? ✓

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? ✓

Certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630 : PASSED

Is the certificate unique? ✓
Is a pseudonym used? ✓
Is certificate not self-signed? ✓
Is the certificate signature intact? ✓
Does the signer's certificate have an expected key-usage? ✓
Key usage : [NON_REPUDIATION]
Is the authority info access present? ✓
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_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451
Is the certificate not revoked? ✓
Is the certificate not on hold? ✓
Is the revocation freshness check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451
Are cryptographic constraints met for the signature's certificate chain? ✓
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2022-07-03 14:51
Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-03 14:51, certificate validity : 2022-07-01 06:30 - 2025-06-13 22:00
Is the current time in the validity range of the certificate of the issuer of the revocation information? ✓
Issuer certificate CERTIFICATE_PostSignum-QCA-4-OCSP-Responder-1_20211015-1057 of revocation data OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451 with validity range : 2021-10-15 10:57 - 2022-10-15 10:57 and validation time 2022-07-03 14:51

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, thisUpdate = 2022-07-03 14:51, production time = 2022-07-03 14:51
Is the revocation acceptance check conclusive? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925, thisUpdate = 2022-07-02 19:25, production time = 2022-07-02 19:25
Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005, thisUpdate = 2022-07-02 20:05, production time = 2022-07-02 20:05
Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓
Is it not self issued OCSP Response? ✓
Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-03 14:51 is in the certificate validity range : 2022-07-01 06:30 - 2025-06-13 22:00
Is revocation's signature intact? ✓
Can the certificate chain be built till a trust anchor? ✓
Is certificate's signature intact? ✓
Id = CERTIFICATE_PostSignum-QCA-4-OCSP-Responder-1_20211015-1057
Has the issuer certificate id-pkix-ocsp-nocheck extension? ✓
2022-07-03T14:51:42Z

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓
Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-02 19:25 is in the certificate validity range : 2022-07-01 06:30 - 2025-06-13 22:00
Is revocation's signature intact? ✓
Can the certificate chain be built till a trust anchor? ✓
2022-07-02T19:25:07Z

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓

Is it not self issued OCSP Response? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-02 20:05 is in the certificate validity range : 2022-07-01 06:30 - 2025-06-13 22:00

Is revocation's signature intact? ✓

Can the certificate chain be built till a trust anchor? ✓

Is certificate's signature intact? ✓
Id = CERTIFICATE_PostSignum-QCA-4-OCSP-Responder-2_20211015-1128

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

2022-07-02T20:05:05Z

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 SHA512 with key size 2048 at validation time : 2022-07-03 14:51

Trust Anchor (CERTIFICATE_PostSignum-Qualified-CA-4_20180927-0739) PASSED

Cryptographic Verification : PASSED

Has the reference data object been found? ✓
Reference : MESSAGE_DIGEST

Is the reference data object intact? ✓
Reference : MESSAGE_DIGEST

Is the signature intact? ✓

Signature Acceptance Validation : INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

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? ✗
The algorithm SHA1 is no longer considered reliable for signature creation! for the token at the validation time : 2022-07-03 14:51
The algorithm SHA1 is no longer considered reliable for signature creation!

Past Signature Validation : INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

Is an acceptable revocation data present for the certificate? ✓
Acceptable revocation data : [OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, CRL_PostSignum-Qualified-CA-4_20220702-1925, OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005]

Is the past certificate validation conclusive? ✓

Is there a POE of the signature value at (or before) control-time? ✓

Are cryptographic constraints met for the signature creation? ✗
The algorithm SHA1 is no longer considered reliable for signature creation! for the token at the validation time : 2022-07-02 20:05
The algorithm SHA1 is no longer considered reliable for signature creation!

Past Revocation Data Selector : PASSED

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, thisUpdate = 2022-07-03 14:51, production time = 2022-07-03 14:51

Is there a POE for the revocation data issuer within its validity range? ✓
Certificate Id = CERTIFICATE_PostSignum-QCA-4-OCSP-Responder-1_20211015-1057

Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925

Is the revocation acceptance check conclusive? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925, thisUpdate = 2022-07-02 19:25, production time = 2022-07-02 19:25

Is the certificate of revocation data issuer trusted? ✓
Certificate Id = CERTIFICATE_PostSignum-Qualified-CA-4_20180927-0739

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005, thisUpdate = 2022-07-02 20:05, production time = 2022-07-02 20:05

Is there a POE for the revocation data issuer within its validity range? ✓
Certificate Id = CERTIFICATE_PostSignum-QCA-4-OCSP-Responder-2_20211015-1128

Is an acceptable revocation data present for the certificate? ✓
Acceptable revocation data : [OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, CRL_PostSignum-Qualified-CA-4_20220702-1925, OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005]

OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451 CRL_PostSignum-Qualified-CA-4_20220702-1925 OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005

Past Certificate Validation : PASSED

Can the certificate chain be built till a trust anchor? ✓

Is the validation time sliding process conclusive? ✓

Are cryptographic constraints met for the signature's certificate chain? ✓
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2022-07-03 14:51

Validation Time Sliding : PASSED

Is there a satisfying revocation status information? ✓
Revocation data : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451 for certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630 with POE at control time 2022-07-03 14:51

Validation Time Sliding Revocation Data Selector (Certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630) : PASSED

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, thisUpdate = 2022-07-03 14:51, production time = 2022-07-03 14:51

Has the revocation data been issued before the control time? ✓
Revocation data OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451 with thisUpdate time : 2022-07-03 14:51, control time : 2022-07-03 14:51

Is there a POE of the certificate at (or before) control-time? ✓
Token Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630, control time : 2022-07-03 14:51

Is there a POE of the revocation data at (or before) control-time? ✓
Token Id : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451, control time : 2022-07-03 14:51

Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925

Is the revocation acceptance check conclusive? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220702-1925, thisUpdate = 2022-07-02 19:25, production time = 2022-07-02 19:25

Has the revocation data been issued before the control time? ✓
Revocation data CRL_PostSignum-Qualified-CA-4_20220702-1925 with thisUpdate time : 2022-07-02 19:25, control time : 2022-07-03 14:51

Is there a POE of the certificate at (or before) control-time? ✓
Token Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630, control time : 2022-07-03 14:51

Is there a POE of the revocation data at (or before) control-time? ✓
Token Id : CRL_PostSignum-Qualified-CA-4_20220702-1925, control time : 2022-07-03 14:51

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005, thisUpdate = 2022-07-02 20:05, production time = 2022-07-02 20:05

Has the revocation data been issued before the control time? ✓
Revocation data OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005 with thisUpdate time : 2022-07-02 20:05, control time : 2022-07-03 14:51

Is there a POE of the certificate at (or before) control-time? ✓
Token Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630, control time : 2022-07-03 14:51

Is there a POE of the revocation data at (or before) control-time? ✓
Token Id : OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005, control time : 2022-07-03 14:51

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

Basic Building Blocks
TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-1_20220702-2005

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_PostSignum-TSA-TSU-1_20210909-0907) 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 RSA with SHA256 with key size 2048 at validation time : 2022-07-03 14:51
Are cryptographic constraints met for the time-stamp message imprint? ✓
Digest algorithm SHA256 at validation time : 2022-07-03 14:51 for time-stamp message imprint

Basic Building Blocks
REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220703-1451

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_PostSignum-QCA-4-OCSP-Responder-1_20211015-1057 : PASSED

Is the certificate signature intact? ✓

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 : 2022-07-03 14:51

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-03 14:51, certificate validity : 2021-10-15 10:57 - 2022-10-15 10:57

Trust Anchor (CERTIFICATE_PostSignum-Qualified-CA-4_20180927-0739) PASSED

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 SHA512 with key size 2048 at validation time : 2022-07-03 14:51

Basic Building Blocks
REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-2_20220702-2005

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_PostSignum-QCA-4-OCSP-Responder-2_20211015-1128 : PASSED

Is the certificate signature intact? ✓

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 : 2022-07-03 14:51

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-03 14:51, certificate validity : 2021-10-15 11:28 - 2022-10-15 11:28

Trust Anchor (CERTIFICATE_PostSignum-Qualified-CA-4_20180927-0739) PASSED

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 SHA512 with key size 2048 at validation time : 2022-07-03 14:51

Basic Building Blocks
REVOCATION - CRL_PostSignum-Qualified-CA-4_20220702-1925

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_PostSignum-Qualified-CA-4_20180927-0739) PASSED

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 : 2022-07-03 14:51

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 CZ 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? ✓