Signature SIGNATURE_RNDr-Ing-Jiří-Peterka_20220701-1136 TOTAL_PASSED

Validation Process for Basic Signatures (Best signature time : 2022-07-01 19:59:42 (UTC)) PASSED

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? ✓

Timestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136 PASSED

Validation Process for Time-stamps (Production time : 2022-07-01 11:36:15 (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_20220701-1136 PASSED

Validation Process for Time-stamps (Production time : 2022-07-01 11:36:15 (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 : 2022-07-01 11:36:15 (UTC)) PASSED

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-5_20220701-1959
Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36
Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36
Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36
Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36
Is the best-signature-time not before the issuance date of the signing certificate? ✓
Best-signature-time : 2022-07-01 11:36, certificate notBefore : 2022-07-01 06:30
Are the time-stamps in the right order? ✓
Is the signed qualifying property: 'signing-time' present? ✓
Is the signing-time plus the time-stamp delay after best-signature-time? ⊘
Is the signature acceptable? ✓

Certificate Revocation Data Selector : PASSED

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136
Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136, thisUpdate = 2022-07-01 11:36, production time = 2022-07-01 11:36
Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220701-1130

Is the revocation acceptance check conclusive? ✓

Id = CRL_PostSignum-Qualified-CA-4_20220701-1130, thisUpdate = 2022-07-01 11:30, production time = 2022-07-01 11:30

Is the result of the revocation data basic validation process acceptable? ✓

Id = OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959

Is the revocation acceptance check conclusive? ✓

Id = OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959, thisUpdate = 2022-07-01 19:59, production time = 2022-07-01 19:59

Is an acceptable revocation data present for the certificate? ✓

Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959

Validation Process for Signatures with Archival Data (Best signature time : 2022-07-01 11:36:15 (UTC)) — PASSED

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_20220701-1136, production time = 2022-07-01 11:36

Is the result of basic time-stamp validation process conclusive? ✓

Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36

Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓

Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136

Does the message-imprint match the computed value? ✓

Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36

Is the result of the Time-stamp Validation Building Block acceptable? ✓

Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36

Is the result of basic time-stamp validation process conclusive? ✓

Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36

Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓

Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136

Does the message-imprint match the computed value? ✓

Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time = 2022-07-01 11:36

Signature Qualification — QESig

Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)? ✓

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 (2022-07-01 11:36:15 (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_20220701-1136

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-5_20220701-1959

Is the certificate not revoked? ✓

Is the certificate not on hold? ✓

Is the revocation freshness check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959

Are cryptographic constraints met for the signature's certificate chain? ✓
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2022-07-01 19:59

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-01 19:59, 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-5_20211015-1209 of revocation data OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959 with validity range : 2021-10-15 12:09 - 2022-10-15 12:09 and validation time 2022-07-01 19:59

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136, thisUpdate = 2022-07-01 11:36, production time = 2022-07-01 11:36

Is the revocation acceptance check conclusive? ✓
Id = CRL_PostSignum-Qualified-CA-4_20220701-1130, thisUpdate = 2022-07-01 11:30, production time = 2022-07-01 11:30

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959, thisUpdate = 2022-07-01 19:59, production time = 2022-07-01 19:59

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓

Is it not self issued OCSP Response? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-01 11:36 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-7_20211015-1216

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

2022-07-01T11:36:15Z

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-01 11:30 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? ✓

2022-07-01T11:30:37Z

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓

Is it not self issued OCSP Response? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2022-07-01 19:59 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-5_20211015-1209
Has the issuer certificate id-pkix-ocsp-nocheck extension? ✓
2022-07-01T19:59:42Z

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 : 2022-07-01 19:59

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 : 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 : 2022-07-01 19:59
Are cryptographic constraints met for the message digest? ✓
Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for message digest
Are cryptographic constraints met for the signing-certificate reference? ✓
Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for signing-certificate reference with Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630

Basic Building Blocks
TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136

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 : 2022-07-01 19:59
Are cryptographic constraints met for the time-stamp message imprint? ✓
Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint

Basic Building Blocks
REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136

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-7_20211015-1216 : 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 : 2022-07-01 19:59

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-01 19:59, certificate validity : 2021-10-15 12:16 - 2022-10-15 12:16

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 : 2022-07-01 19:59

Basic Building Blocks
REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959

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-5_20211015-1209 : 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 : 2022-07-01 19:59
Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-07-01 19:59, certificate validity : 2021-10-15 12:09 - 2022-10-15 12:09

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 : 2022-07-01 19:59

Basic Building Blocks
REVOCATION - CRL_PostSignum-Qualified-CA-4_20220701-1130

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 : 2022-07-01 19:59

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? ✓