Signature SIGNATURE_RNDr-Ing-Jiří-Peterka_20220222-1923 — TOTAL_PASSED

Validation Process for Basic Signatures (Best signature time : 2022-04-24 14:30:45 (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-2_20220222-1923 — PASSED

Validation Process for Time-stamps (Production time : 2022-02-22 19:23:20 (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 : 2022-02-22 19:23:20 (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-1_20220424-1313
- Does the message-imprint match the computed value? ✓
  Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923, production time = 2022-02-22 19:23
- Is the result of basic time-stamp validation process conclusive? ✓
  Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923, production time = 2022-02-22 19:23
- Is the best-signature-time not before the issuance date of the signing certificate? ✓
  Best-signature-time : 2022-02-22 19:23, certificate notBefore : 2020-03-18 10:20
- 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-1_20220424-1313
- Is the revocation acceptance check conclusive? ✓
  Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220424-1313, thisUpdate = 2022-04-24 13:13, production time = 2022-04-24 13:13
- Is an acceptable revocation data present for the certificate? ✓
  Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220424-1313

Validation Process for Signatures with Archival Data (Best signature time : 2022-02-22 19:23:20 (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-2_20220222-1923, production time = 2022-02-22 19:23
- Is the result of basic time-stamp validation process conclusive? ✓
  Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923, production time = 2022-02-22 19:23
- Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
  Digest algorithm SHA256 at validation time : 2022-04-24 14:30 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923
- Does the message-imprint match the computed value? ✓
  Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923, production time = 2022-02-22 19:23

Signature Qualification — AdESig-QC

- 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? !
The private key does not reside in a QSCD at (best) signing time!

Certificate Qualification at certificate issuance time (2020-03-18 10:20:20 (UTC)) — QC for eSig

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? !
The private key does not reside in a QSCD at issuance time!

Certificate Qualification at best signature time (2022-02-22 19:23:20 (UTC)) — QC for eSig

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? !
The private key does not reside in a QSCD at (best) signing time!

Basic Building Blocks
SIGNATURE - SIGNATURE_RNDr-Ing-Jiří-Peterka_20220222-1923

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? ✓

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? ✓

Certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20200318-1020 : 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 : [DIGITAL_SIGNATURE, NON_REPUDIATION, KEY_ENCIPHERMENT]

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_20220424-1313

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_20220424-1313

Are cryptographic constraints met for the signature's certificate chain? ✓
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2022-04-24 14:30

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-04-24 14:30, certificate validity : 2020-03-18 10:20 - 2023-04-07 10:20

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_20220424-1313 with validity range : 2021-10-15 10:57 - 2022-10-15 10:57 and validation time 2022-04-24 14:30

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive? ✓
Id = OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220424-1313, thisUpdate = 2022-04-24 13:13, production time = 2022-04-24 13:13

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220424-1313

Revocation Acceptance Checker : PASSED

Is the revocation status known? ✓

Is it not self issued OCSP Response? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2022-04-24 13:13 is in the certificate validity range : 2020-03-18 10:20 - 2023-04-07 10:20

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? ✓

2022-04-24T13:13:17Z

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 : 2022-04-24 14:30

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 : 2022-04-24 14:30

Are cryptographic constraints met for the message digest? ✓
Digest algorithm SHA256 at validation time : 2022-04-24 14:30 for message digest

Are cryptographic constraints met for the signing-certificate reference? ✓
Digest algorithm SHA256 at validation time : 2022-04-24 14:30 for signing-certificate reference with Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20200318-1020

Basic Building Blocks
TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-2_20220222-1923

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-2_20210909-0909) 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 : 2022-04-24 14:30

Are cryptographic constraints met for the time-stamp message imprint? ✓
Digest algorithm SHA256 at validation time : 2022-04-24 14:30 for time-stamp message imprint

Basic Building Blocks

REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-1_20220424-1313

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 : 2022-04-24 14:30
Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2022-04-24 14:30, 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 : 2022-04-24 14:30

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 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? ✓