Signature SIGNATURE_RNDr-Ing-Jiří-Peterka_20160806-1545 — TOTAL_PASSED

Validation Process for Basic Signatures (Best signature time : 2022-04-26 19:06:29 (UTC)) — INDETERMINATE - OUT_OF_BOUNDS_NOT_REVOKED

- 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? !
  The result of the 'X.509 Certificate Validation' building block is not conclusive!
- Is the signing certificate not revoked at validation time? ✓
- Is the validation time in the validity range of the signing certificate? !
  The validation time is not in the validity range of the signing certificate!
- Is the result of the 'Cryptographic Verification' building block conclusive? ✓
- Is the result of the Basic Validation Process conclusive? ✗
  Basic Signature Validation process failed with INDETERMINATE/OUT_OF_BOUNDS_NOT_REVOKED indication
  The result of the Basic validation process is not conclusive!

Timestamp TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545 — PASSED

Validation Process for Time-stamps (Production time : 2016-08-06 15:45:48 (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 — TSA

- 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
- Is the trusted list acceptable? ✓
  Trusted List : http://tl.nbu.gov.sk/kca/tsl/tsl.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? ✗
  The certificate is not related to a granted status at the timestamp production time!

Timestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052 — PASSED

Validation Process for Time-stamps (Production time : 2022-01-04 10:52:16 (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 : 2016-08-06 15:45:48 (UTC)) — PASSED

- Is the result of the Basic Validation Process acceptable? ✓
- Is an acceptable revocation data present for the certificate? ✓
  Latest acceptable revocation : CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452
- Does the message-imprint match the computed value? ✓
  Signature Timestamp with Id = TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545, production time = 2016-08-06 15:45
- Is the result of basic time-stamp validation process conclusive? ✓
  Signature Timestamp with Id = TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545, production time = 2016-08-06 15:45
- Does the message-imprint match the computed value? ✓
  Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052, production time = 2022-01-04 10:52
- Is the result of basic time-stamp validation process conclusive? ✓
  Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052, production time = 2022-01-04 10:52
- Is the best-signature-time not before the issuance date of the signing certificate? ✓
  Best-signature-time : 2016-08-06 15:45, certificate notBefore : 2016-01-08 06:09
- Is the best-signature-time before the expiration date of the signing certificate? ✓
  Best-signature-time : 2016-08-06 15:45, certificate notAfter : 2017-01-07 06:09

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 = CRL_I-CA-Qualified-Certification-Authority-09-2009_20190831-1952
Is the revocation acceptance check conclusive? !
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20190831-1952, thisUpdate = 2019-08-31 19:52, production time = 2019-08-31 19:52 — The revocation acceptance check is not conclusive!
Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452
Is the revocation acceptance check conclusive? ✓
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452, thisUpdate = 2017-01-07 04:52, production time = 2017-01-07 04:52
Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452

Validation Process for Signatures with Archival Data (Best signature time : 2016-08-06 15:45:48 (UTC)) **PASSED**

Is the result of the LTV validation process acceptable? ✓
Is the result of the Time-stamp Validation Building Block acceptable? ✓
Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052, production time = 2022-01-04 10:52
Is the result of basic time-stamp validation process conclusive? ✓
Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052, production time = 2022-01-04 10:52
Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
Digest algorithm SHA256 at validation time : 2022-04-26 19:06 for time-stamp message imprint with Id : TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052
Does the message-imprint match the computed value? ✓
Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052, production time = 2022-01-04 10:52
Is the result of the Time-stamp Validation Building Block acceptable? ✓
Signature Timestamp with Id = TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545, production time = 2016-08-06 15:45
Is the result of basic time-stamp validation process conclusive? ✓
Signature Timestamp with Id = TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545, production time = 2016-08-06 15:45
Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
Digest algorithm SHA256 at validation time : 2022-01-04 10:52 for time-stamp message imprint with Id : TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545
Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545, production time = 2016-08-06 15:45

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
Is the trusted list acceptable? ✓
Trusted List : http://tl.nbu.gov.sk/kca/tsl/tsl.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 (2016-01-08 06:09:35 (UTC)) **QC for eSig with QSCD**

Is the certificate related to a CA/QC? ✓
Is the trust service consistent? ✓
Trust service name : (16) I.CA - vydávání kvalifikovaných certifikátů
Is the trust service consistent? ✓
Trust service name : (33) I.CA - Qualified Certification Authority, 09/2009
Is a conflict detected between trust services? ✓
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? ✓
Is the certificate qualification conclusive? ✓
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 (2016-08-06 15:45:48 (UTC)) **QC for eSig with QSCD**

Is the certificate related to a CA/QC? ✓
Is the trust service consistent? ✓
Trust service name : (16) I.CA - vydávání kvalifikovaných certifikátů

Is the trust service consistent?
Trust service name : (33) I.CA - Qualified Certification Authority, 09/2009
Is a conflict detected between trust services?
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?
Is the certificate qualification conclusive?
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_20160806-1545

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

Validation Context Initialization : PASSED

Is the signature policy known?

X509 Certificate Validation : INDETERMINATE - OUT_OF_BOUNDS_NOT_REVOKED

Can the certificate chain be built till a trust anchor?
Is the certificate validation conclusive?
The certificate validation is not conclusive!

Certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20160108-0609 : INDETERMINATE - OUT_OF_BOUNDS_NOT_REVOKED

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]
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 : CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452
Is the certificate not revoked?
Is the certificate not on hold?
Is the revocation freshness check conclusive?
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452
Are cryptographic constraints met for the signature's certificate chain?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2022-04-26 19:06
Is the current time in the validity range of the signer's certificate?
Validation time : 2022-04-26 19:06, certificate validity : 2016-01-08 06:09 - 2017-01-07 06:09
The current time is not in the validity range of the signer's certificate!

Certificate Revocation Data Selector : PASSED

Is the revocation acceptance check conclusive?
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20190831-1952, thisUpdate = 2019-08-31 19:52, production time = 2019-08-31 19:52
The revocation acceptance check is not conclusive!
Is the revocation acceptance check conclusive?
Id = CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452, thisUpdate = 2017-01-07 04:52, production time = 2017-01-07 04:52
Is an acceptable revocation data present for the certificate?
Latest acceptable revocation : CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452

Revocation Acceptance Checker : INDETERMINATE - TRY_LATER

Is the revocation status known?
Is the revocation data consistent?
Revocation data is known to contain information about the certificate at 2019-08-31 19:52 which is not in the certificate validity range : 2016-01-08 06:09 - 2017-01-07 06:09
The revocation data is not consistent!
2019-08-31T19:52:02Z

Revocation Acceptance Checker : PASSED

- Is the revocation status known? ✓
- Is the revocation data consistent? ✓
  Revocation thisUpdate 2017-01-07 04:52 is in the certificate validity range : 2016-01-08 06:09 - 2017-01-07 06:09
- Is revocation's signature intact? ✓
- Can the certificate chain be built till a trust anchor? ✓
  2017-01-07T04:52:03Z

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 2048 at validation time : 2022-04-26 19:06

Trust Anchor (CERTIFICATE_I-CA-Qualified-Certification-Authority-09-2009_20090901-0000) (Self Signed) PASSED
Cross certification: CERTIFICATE_I-CA-Qualified-Certification-Authority-09-2009_20091124-1114

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 : 2022-04-26 19:06
- Are cryptographic constraints met for the message digest? ✓
  Digest algorithm SHA256 at validation time : 2022-04-26 19:06 for message digest
- Are cryptographic constraints met for the signing-certificate reference? ✓
  Digest algorithm SHA256 at validation time : 2022-04-26 19:06 for signing-certificate reference with Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20160108-0609

Basic Building Blocks
TIMESTAMP - TIMESTAMP_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20160806-1545

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_I-CA-Time-Stamping-Authority-TSS-TSU-4-12-2015_20151208-1319) 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? ⚠
  The 'Signing Certificate' attribute contains references to other certificates than those present in 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 : 2022-04-26 19:06
- Are cryptographic constraints met for the time-stamp message imprint? ✓
  Digest algorithm SHA256 at validation time : 2022-04-26 19:06 for time-stamp message imprint

Basic Building Blocks
TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-1_20220104-1052

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 : 2022-04-26 19:06
Are cryptographic constraints met for the time-stamp message imprint?
Digest algorithm SHA256 at validation time : 2022-04-26 19:06 for time-stamp message imprint

Basic Building Blocks
REVOCATION - CRL_I-CA-Qualified-Certification-Authority-09-2009_20170107-0452

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_I-CA-Qualified-Certification-Authority-09-2009_20090901-0000) (Self Signed) **PASSED**
Cross certification: CERTIFICATE_I-CA-Qualified-Certification-Authority-09-2009_20091124-1114

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 : 2022-04-26 19:06

Basic Building Blocks
REVOCATION - CRL_I-CA-Qualified-Certification-Authority-09-2009_20190831-1952

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_I-CA-Qualified-Certification-Authority-09-2009_20090901-0000) (Self Signed) **PASSED**
Cross certification: CERTIFICATE_I-CA-Qualified-Certification-Authority-09-2009_20091124-1114

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 : 2022-04-26 19:06

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?

Trusted List SK **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?