Signature SIGNATURE_RNDr-Ing-Jiří-Peterka_20160802-1045 — INDETERMINATE - OUT_OF_BOUNDS_NOT_REVOKED

Validation Process for Basic Signatures (Best signature time : 2023-04-22 18:05:11 (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_PostSignum-TSA-TSU-2_20160802-1045 — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

Validation Process for Time-stamps (Production time : 2016-08-02 10:45:20 (UTC)) — INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

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? !
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!

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

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-4_20210929-1323 — PASSED

Validation Process for Time-stamps (Production time : 2021-09-29 13:23:31 (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 : 2021-09-29 13:23:31 (UTC)) — INDETERMINATE - OUT_OF_BOUNDS_NOT_REVOKED

Is the result of the Basic Validation Process acceptable? ✓

Is the revocation data present for the certificate? ✓

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

Does the message-imprint match the computed value? ✓
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20160802-1045, production time = 2016-08-02 10:45

Is the result of basic time-stamp validation process conclusive? !
Signature Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-2_20160802-1045, production time = 2016-08-02 10:45
The result of basic time-stamp validation process is not conclusive! Past time-stamp validation is required.

Does the message-imprint match the computed value? ✓
Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-4_20210929-1323, production time = 2021-09-29 13:23

Is the result of basic time-stamp validation process conclusive? ✓
Document Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-4_20210929-1323, production time = 2021-09-29 13:23

Is the best-signature-time not before the issuance date of the signing certificate? ✓
Best-signature-time : 2021-09-29 13:23, certificate notBefore : 2016-08-02 07:47

Is the best-signature-time before the expiration date of the signing certificate? ✗
Best-signature-time : 2021-09-29 13:23, certificate notAfter : 2017-08-02 07:47
The best-signature-time is not before the expiration date of the signing certificate!

Certificate Revocation Data Selector : PASSED

Is the result of the revocation data basic validation process acceptable? ✓
Id = CRL_I-CA-Qualified-2-CA-RSA-02-2016_20170802-0732

Is the revocation acceptance check conclusive? ✓
Id = CRL_I-CA-Qualified-2-CA-RSA-02-2016_20170802-0732, thisUpdate = 2017-08-02 07:32, production time = 2017-08-02 07:32

Is the result of the revocation data basic validation process acceptable? ✓
Id = OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

Is the revocation acceptance check conclusive? ✓
Id = OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759, thisUpdate = 2023-04-22 17:59, production time = 2023-04-22 17:59

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

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 (2016-08-02 07:47:15 (UTC)) QC for eSig with QSCD

Is the certificate related to a CA/QC? ✓

Is the trust service consistent? ✓
Trust service name : (78) I.CA - vydávání kvalifikovaných certifikátů

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

Does the trusted certificate match the trust service? ✓

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 (2021-09-29 13:23:31 (UTC)) QC for eSig with QSCD

Is the certificate related to a CA/QC? ✓

Is the trust service consistent? ✓
Trust service name : (78) I.CA - vydávání kvalifikovaných certifikátů

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

Does the trusted certificate match the trust service? ✓

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_RNDr-Ing-Jiří-Peterka_20160802-1045

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 : **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_20160802-0747 : **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 : OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

Is the certificate not revoked? ✓

Is the certificate not on hold? ✓

Is the revocation freshness check conclusive? ✓
Id = OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

Are cryptographic constraints met for the signature's certificate chain? ✓
Signature algorithm RSA with SHA256 with key size 4096 at validation time : 2023-04-22 18:05

Is the current time in the validity range of the signer's certificate? ✗
Validation time : 2023-04-22 18:05, certificate validity : 2016-08-02 07:47 - 2017-08-02 07:47
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-2-CA-RSA-02-2016_20170802-0732, thisUpdate = 2017-08-02 07:32, production time = 2017-08-02 07:32

Is the revocation acceptance check conclusive? ✓
Id = OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759, thisUpdate = 2023-04-22 17:59, production time = 2023-04-22 17:59

Is an acceptable revocation data present for the certificate? ✓
Latest acceptable revocation : OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

Revocation Acceptance Checker : **PASSED**

Is the revocation status known? ✓

Is the revocation data consistent? ✓
Revocation thisUpdate 2017-08-02 07:32 is in the certificate validity range : 2016-08-02 07:47 - 2017-08-02 07:47

Is revocation's signature intact? ✓

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

2017-08-02T07:32:34Z

Revocation Acceptance Checker : **PASSED**

Is the revocation status known? ✓

Is it not self issued OCSP Response? ✓

Is the revocation data consistent? ✓
CertHash value of revocation data matches with the certificate digest

Is revocation's signature intact? ✓

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

Is certificate's signature intact? ✓
Id = CERTIFICATE_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230125-1208

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

2023-04-22T17:59:14Z

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 : 2023-04-22 18:05

Trust Anchor (CERTIFICATE_I-CA-Qualified-2-CA-RSA-02-2016_20160211-1217) **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 : 2023-04-22 18:05
Are cryptographic constraints met for the message digest? ✓
Digest algorithm SHA256 at validation time : 2023-04-22 18:05 for message digest
Are cryptographic constraints met for the signing-certificate reference? ✓
Digest algorithm SHA256 at validation time : 2023-04-22 18:05 for signing-certificate reference with Id : CERTIFICATE_RNDr-Ing-Jiří-Peterka_20160802-0747

Basic Building Blocks

TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-2_20160802-1045

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_20150826-0841) 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 : INDETERMINATE - CRYPTO_CONSTRAINTS_FAILURE_NO_POE

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? ✗
The algorithm SHA1 is no longer considered reliable for time-stamp signature! for the token at the validation time : 2023-04-22 18:05
The algorithm SHA1 is no longer considered reliable for time-stamp signature!

Basic Building Blocks

TIMESTAMP - TIMESTAMP_PostSignum-TSA-TSU-4_20210929-1323

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-4_20200914-1053) 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 : 2023-04-22 18:05
Are cryptographic constraints met for the time-stamp message imprint? ✓
Digest algorithm SHA256 at validation time : 2023-04-22 18:05 for time-stamp message imprint

Basic Building Blocks

REVOCATION - CRL_I-CA-Qualified-2-CA-RSA-02-2016_20170802-0732

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-2-CA-RSA-02-2016_20160211-1217) 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 : 2023-04-22 18:05

Basic Building Blocks
REVOCATION - OCSP_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230422-1759

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_I-CA-Qualified-2-CA-RSA-02-2016-OCSP-responder_20230125-1208 : 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 : 2023-04-22 18:05

Is the current time in the validity range of the signer's certificate? ✓
Validation time : 2023-04-22 18:05, certificate validity : 2023-01-25 12:08 - 2023-05-15 12:08

Trust Anchor (CERTIFICATE_I-CA-Qualified-2-CA-RSA-02-2016_20160211-1217) 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 2048 at validation time : 2023-04-22 18:05

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? ✓