alidation Dragog for Pagig Cignotures in	TOTAL_PASS
alidation Process for Basic Signatures (Best signature time : 2022-07-01 19:59:42	PASS
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?	
mestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136	PASS
Validation Process for Time-stamps (Production time : 2022-07-01 11:36:15 (UTC))	PASS
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	QT
Has a trusted list been reached for the certificate chain?	<b>x</b> -
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?	
mestamp TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136	PASS
Validation Process for Time-stamps (Production time : 2022-07-01 11:36:15 (UTC))	PASS
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	QT
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?	
alidation Process for Signatures with Time and Signatures with Long- erm Validation Data (Best signature time : 2022-07-01 11:36:15 (UTC))	PASS
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	
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 :	PASS
Is the result of the revocation data basic validation process acceptable?	r ASS
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	

mat Ch	necking :	PASS
	ding Blocks - SIGNATURE_RNDr-Ing-Jiří-Peterka_20220701-1136	
· · · ·	es the private key reside in a QSCD at (best) signing time?	
	he certificate type unambiguously identified at (best) signing time? tificate type is for eSig	
ls t	he certificate qualified at (best) signing time?	
	n the certificate type be issued by a found trust service? es the trusted certificate match the trust service?	
1	the certificate related to a consistent trust service declaration?	
	ist service name : (116) PostSignum - vydávání kvalifikovaných certifikátů he certificate related to a trust service with a granted status?	
ls t	he trust service consistent?	
	he certificate related to a CA/QC?	
Certi (UTC))	ficate Qualification at best signature time (2022-07-01 11:36:15	QC for eSig with QS
· · · ·	es the private key reside in a QSCD at issuance time?	
	he certificate type unambiguously identified at issuance time? tificate type is for eSig	
	the certificate qualified at issuance time?	
	es the trusted certificate match the trust service?	
	he certificate related to a consistent trust service declaration? n the certificate type be issued by a found trust service?	
ls t	he certificate related to a trust service with a granted status?	
	<b>he trust service consistent?</b> ist service name : (116) PostSignum - vydávání kvalifikovaných certifikátů	
	he certificate related to a CA/QC?	
	ficate Qualification at certificate issuance time (2022-07-01 42 (UTC))	QC for eSig with QS
	the private key reside in a QSCD at (best) signing time?	
	certificate qualified at issuance time?	
	certificate type unambiguously identified at (best) signing time?	
	een an acceptable trusted list found? certificate qualified at (best) signing time?	
Trustec	d List : https://tsl.gov.cz/publ/TSL_CZ.xtsl	
	d List : https://ec.europa.eu/tools/lotl/eu-lotl.xml trusted list acceptable?	
Is the	list of trusted lists acceptable?	
	signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)? trusted list been reached for the certificate chain?	
-	ire Qualification	QE
= 2022-	-07-01 11:36	
	the message-imprint match the computed value? ure Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time	
Id : TIM	IESTAMP_PostSignum-TSA-TSU-1_20220701-1136	
	digest algorithm reliable at lowest POE time for the time-stamp token? algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint with	
	ure Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time -07-01 11:36	
ls the	-07-01 11:36 result of basic time-stamp validation process conclusive?	
Signatu	result of the Time-stamp Validation Building Block acceptable? re Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time 07.0111-56	
= 2022-	-07-01 11:36	
Does t	the message-imprint match the computed value? Ire Timestamp with Id = TIMESTAMP PostSignum-TSA-TSU-1 20220701-1136, production time	
Digest a	algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint with IESTAMP_PostSignum-TSA-TSU-1_20220701-1136	
	-07-01 11:36 digest algorithm reliable at lowest POE time for the time-stamp token?	
Signatu	result of basic time-stamp validation process conclusive? ure Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time	
= 2022-	-07-01 11:36	
	result of the Time-stamp Validation Building Block acceptable? Jre Timestamp with Id = TIMESTAMP_PostSignum-TSA-TSU-1_20220701-1136, production time	
	result of the LTV validation process acceptable?	
	1 11:36:15 (UTC))	
·	est acceptable revocation : OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959 ion Process for Signatures with Archival Data (Best signature time :	PASS
ls a	an acceptable revocation data present for the certificate?	
Id =	OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959, thisUpdate = 2022-07-01 19:59, duction time = 2022-07-01 19:59	
	= OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959 the revocation acceptance check conclusive?	
Id =		
ls t	e = 2022-07-01 11:30 the result of the revocation data basic validation process acceptable?	

Is the signature identification not ambiguous? Is the signed references identification not ambiguous?	0
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?	0
	-
X509 Certificate Validation :	PASSED
Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive?	©
Is the certificate validation conclusive?	õ
Certificate CERTIFICATE_RNDr-Ing-Jiří-Peterka_20220701-0630 :	PASSED
Is the certificate unique?	
Is a pseudonym used?	õ
Is certificate not self-signed?	0
Is the certificate signature intact?	0
Does the signer's certificate have an expected key-usage? Key usage : [NON_REPUDIATION]	0
Is the authority info access present?	•
Is the revocation info access present?	0
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?	0 0
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?	0
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?	0
Is the revocation data consistent?	0
Revocation thisUpdate 2022-07-01 11:30 is in the certificate validity range : 2022-07-01 06:30 - 2025-06-13 22:00	
ls 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?	0
Is it not self issued OCSP Response?	0

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	0
Is revocation's signature intact?	•
Can the certificate chain be built till a trust anchor? Is certificate's signature intact?	0
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?	Ø
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?	0
Reference : MESSAGE_DIGEST Is the signature intact?	•
Signature Acceptance Validation :	PASSED
Is the structure of the signature valid?	<ul> <li>Image: A start of the start of</li></ul>
Is the signed attribute: 'signing-certificate' present?	•
Is the signed attribute: 'signing-certificate' present only once?	0
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	Ŭ
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 there an identified candidate for the signing certificate? Is the signed attribute: 'cert-digest' of the certificate present?	0
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?	0
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? <b>X509 Certificate Validation :</b>	O O 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?	0
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor?	O O PASSED O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive?	O PASSED O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b>	O PASSED O 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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact?	O PASSED O PASSED PASSED O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact?	O PASSED O PASSED PASSED O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b>	<ul> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> </ul>
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> Is the signed attribute: 'signing-certificate' present?	O PASSED PASSED PASSED O O PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b>	<ul> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> <li>PASSED</li> </ul>
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> 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?	O PASSED PASSED PASSED O O PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> 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?	O PASSED PASSED PASSED O O PASSED O O PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> 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 Agorithm 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?	O PASSED O PASSED PASSED O O PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is the message imprint data intact? 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 'sisuer name? Are cryptographic constraints met for the time-stamp signature? Signature algorithm SA 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? <b>Basic Building Blocks</b>	O PASSED O PASSED PASSED O O PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> Is the signed attribute: 'signing-certificate' present? Does the 'Signing Certificate' attribute contain references only to the certificate chain? Does the TSI 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 <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b>	<ul> <li>O</li> <li>O</li> <li>PASSED</li> <li>O</li> <li>PASSED</li> <li>O</li> <li>O</li> <li>O</li> <li>PASSED</li> <li>O</li> <l< td=""></l<></ul>
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? Signature Acceptance Validation : 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 RSA with SHA256 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 <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b>	PASSED PASSED PASSED PASSED PASSED PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? Signature Acceptance Validation : Is the signed attribute: 'signing-certificate' present? Does the 'Signing Certificate' attribute contain references only to the certificate chain? Does the 'Signing Certificate' attribute contain references only to the certificate chain? Does the 'Signing Certificate' 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 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 <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b> <b>Identification of the Signing Certificate :</b> Is there an identified candidate for the signing certificate? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor?	PASSED PASSED PASSED PASSED PASSED PASSED O PASSED O PASSED O 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? <b>X509 Certificate Validation :</b> Can the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is the message imprint data intact? Is the signed attribute: 'signing-certificate' present? Does the 'Signing Certificate' attribute contain references only to the certificate chain? 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 algorthm fSA-265 at validation time : 2022-07-01 19:59 Are cryptographic constraints met for the time-stamp signature? Digest algorithm SHA256 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 Are cryptographic constraints met for the time-stamp message imprint? <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b> <b>Identification of the Signing Certificate :</b> Is there an identified candidate for the signing certificate? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive?	PASSED PASSED PASSED PASSED PASSED PASSED PASSED O O O O O O O O O O O O O O O O O O O
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? <b>X509 Certificate Validation :</b> Can the certificate Validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data been found? Is the message imprint data been found? Is the message imprint data intact? Is time-stamp's signature intact? <b>Signature Acceptance Validation :</b> 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 signature? Signature algorithm SKA 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 SKA 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? Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint? Digest algorithm SHA256 at validation time : 2022-07-01 19:59 for time-stamp message imprint <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b> <b>Identification of the Signing Certificate :</b> Is there an identified candidate for the signing certificate? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive? Is the certificate validation conclusive? Is the certificate validation conclusive?	PASSED PASSED PASSED PASSED PASSED PASSED PASSED O PASSED O PASSED O O
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? <b>X509 Certificate Validation :</b> Can the certificate validation conclusive? <b>Trust Anchor (CERTIFICATE_PostSignum-TSA-TSU-1_20210909-0907)</b> <b>Cryptographic Verification :</b> Has the message imprint data been found? Is the message imprint data intact? Is the message imprint data intact? Is the signed attribute: 'signing-certificate' present? Does the 'Signing Certificate' attribute contain references only to the certificate chain? 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 algorthm fSA-265 at validation time : 2022-07-01 19:59 Are cryptographic constraints met for the time-stamp signature? Digest algorithm SHA256 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 Are cryptographic constraints met for the time-stamp message imprint? <b>Basic Building Blocks</b> <b>REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-7_20220701-1136</b> <b>Identification of the Signing Certificate :</b> Is there an identified candidate for the signing certificate? <b>X509 Certificate Validation :</b> Can the certificate chain be built till a trust anchor? Is the certificate validation conclusive?	PASSED PASSED PASSED PASSED PASSED PASSED PASSED O O O O O O O O O O O O O O O O O O O

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?	0
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)	PASSE
Cryptographic Verification :	PASSE
Is revocation's signature intact?	C
ignature Acceptance Validation :	PASSEE
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	C
Basic Building Blocks REVOCATION - OCSP_PostSignum-QCA-4-OCSP-Responder-5_20220701-1959	
dentification of the Signing Certificate :	PASSED
Is there an identified candidate for the signing certificate?	C
509 Certificate Validation :	PASSED
Can the certificate chain be built till a trust anchor?	C
Is the certificate validation conclusive?	C
Is the certificate validation conclusive?	C
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	Č.
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	C
Trust Anchor (CERTIFICATE_PostSignum-Qualified- CA-4_20180927-0739)	PASSEE
ryptographic Verification :	PASSED
Is revocation's signature intact?	٢
ignature 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	e
Basic Building Blocks REVOCATION - CRL_PostSignum-Qualified-CA-4_20220701-1130	
dentification of the Signing Certificate :	PASSED
Is there an identified candidate for the signing certificate?	C
509 Certificate Validation :	PASSED
Can the certificate chain be built till a trust anchor?	•
Is the certificate validation conclusive?	C
Trust Anchor (CERTIFICATE_PostSignum-Qualified- CA-4_20180927-0739)	PASSED
ryptographic Verification :	PASSED
Is revocation's signature intact?	C
ignature 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	C
ist Of Trusted Lists EU	PASSED
Is the trusted list fresh?	٢
Is the trusted list not expired?	C
Does the trusted list have the expected version?	C
Is the trusted list well signed?	C
rusted List CZ	PASSED
Is the trusted list fresh?	0
Is the trusted list not expired?	S
Does the trusted list have the expected version?	<b>~</b>