Signature S-F43B7E69EBF2E51E4C534FD86B1DED4FFCAC456EA6418E2C1D69F53104E24B79

Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive?

Conclusion : **PASSED**

Timestamp T-577702815B0B7836B0018ADB3A4C6306CCDA85B62E1B92AC33BAB324FB015EE5

Validation Process for time-stamps
SIGNATURE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?

Is the trusted list acceptable?

Is the trusted list acceptable?

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 T-FB92510FA263A25CC0C1FA41C6C2E0BF7937A9634DFC54719FF3DEEA51BC48DB

Validation Process for time-stamps
ARCHIVE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?

Is the trusted list acceptable?

Is the trusted list acceptable?

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 T-953AEA1CED17DE569C4E132C3C0EC6CC0A43CF75FEBFBFE0D76022A9B46608E4

Validation Process for time-stamps
ARCHIVE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?	✓
Is the trusted list acceptable?	✓
Is the trusted list acceptable?	✓
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

Is the result of the Basic Validation Process acceptable?	✓
Is the result of the revocation data validation process acceptable?	✓
Is the revocation data consistent?	✓
Is an acceptable revocation data present for the certificate?	✓
Are the timestamps in the right order?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signing-time plus the timestamp delay after best-signature-time?	IGNORED
Is the signature acceptable?	✓

Conclusion : **PASSED**

Validation Process for Signatures with Archival Data

Is the result of the LTV validation process acceptable?	✓

Conclusion : **PASSED**

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 trusted list acceptable?	✓
Is the trusted list acceptable?	✓
Is the certificate qualified at (best) signing time?	✓
Is the certificate for eSig 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

Is the certificate related to a CA/QC?	✓
Is the certificate related to a trust service with a granted status?	✓
Is the trust service consistent?	✓
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 for eSig at issuance time?
Does the private key reside in a QSCD at issuance time?

Certificate Qualification at best signature time

Is the certificate related to a CA/QC?
Is the certificate related to a trust service with a granted status?
Is the trust service consistent?
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 for eSig at (best) signing time?
Does the private key reside in a QSCD at (best) signing time?

Signature S-612221361B8CBFBD2B2F3757B3BCA66E9C5C3CF5DD9A53C2A51D916A4847D1D4

Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive?

Conclusion : **PASSED**

Timestamp T-2AC540BA497D2207305C1A5F4A119F676A7447D987A052C7B71A275A990CC1CD

Validation Process for time-stamps
SIGNATURE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?
Is the trusted list acceptable?
Is the trusted list acceptable?
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 T-953AEA1CED17DE569C4E132C3C0EC6CC0A43CF75FEBFBFE0D76022A9B46608E4

Validation Process for time-stamps
ARCHIVE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?	✓
Is the trusted list acceptable?	✓
Is the trusted list acceptable?	✓
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

Is the result of the Basic Validation Process acceptable?	✓
Is the result of the revocation data validation process acceptable?	✓
Is the revocation data consistent?	✓
Is an acceptable revocation data present for the certificate?	✓
Are the timestamps in the right order?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signing-time plus the timestamp delay after best-signature-time?	IGNORED
Is the signature acceptable?	✓

Conclusion : **PASSED**

Validation Process for Signatures with Archival Data

Is the result of the LTV validation process acceptable?	✓

Conclusion : **PASSED**

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 trusted list acceptable?	✓
Is the trusted list acceptable?	✓
Is the certificate qualified at (best) signing time?	✓
Is the certificate for eSig 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

Is the certificate related to a CA/QC?	✓
Is the certificate related to a trust service with a granted status?	✓
Is the trust service consistent?	✓
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 for eSig at issuance time?
Does the private key reside in a QSCD at issuance time?

Certificate Qualification at best signature time

Is the certificate related to a CA/QC?
Is the certificate related to a trust service with a granted status?
Is the trust service consistent?
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 for eSig at (best) signing time?
Does the private key reside in a QSCD at (best) signing time?

Signature S-80C2DD2BBAAE076E85A43BA76F21D39AC65DAF3DB81C5E55EA33F25C6177D4DC

Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive?

Conclusion : **PASSED**

Timestamp T-55B2AD737475E7802F3A4BC5F906B574119261728FFB95D989B869528C32DEDE

Validation Process for time-stamps

SIGNATURE_TIMESTAMP -

Is the result of the timestamps validation process conclusive?

Conclusion : **PASSED**

Timestamp Qualification : QTSA

Has a trusted list been reached for the certificate chain?
Is the trusted list acceptable?
Is the trusted list acceptable?
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

Is the result of the Basic Validation Process acceptable?
Is the result of the revocation data validation process acceptable?
Is the revocation data consistent?
Is the result of the revocation data validation process acceptable?
Is the revocation data consistent?
Is the result of the revocation data validation process acceptable?

Is the revocation data consistent?	✓
Is an acceptable revocation data present for the certificate?	✓
Are the timestamps in the right order?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signing-time plus the timestamp delay after best-signature-time?	IGNORED
Is the signature acceptable?	✓

Conclusion : **PASSED**

Validation Process for Signatures with Archival Data

Is the result of the LTV validation process acceptable?	✓

Conclusion : **PASSED**

Signature Qualification : AdESeal-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 trusted list acceptable?	✓
Is the trusted list acceptable?	✓
Is the certificate qualified at (best) signing time?	✓
Is the certificate for eSig 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

Is the certificate related to a CA/QC?	✓
Is the certificate related to a trust service with a granted status?	✓
Is the trust service consistent?	✓
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 for eSig at issuance time?	!
Does the private key reside in a QSCD at issuance time?	!

Certificate Qualification at best signature time

Is the certificate related to a CA/QC?	✓
Is the certificate related to a trust service with a granted status?	✓
Is the trust service consistent?	✓
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 for eSig at (best) signing time?	!

Does the private key reside in a QSCD at (best) signing time?	⚠

Basic Building Blocks
SIGNATURE - S-612221361B8CBFBD2B2F3757B3BCA66E9C5C3CF5DD9A53C2A51D916A4847D1D4

Does the signature format correspond to an expected format?	✓
Is the signature identification not ambiguous?	✓
Is only one SignerInfo present?	✓
Identification of the Signing Certificate :	**PASSED**
Is there an identified candidate for the signing certificate?	✓
Is the signed attribute: signing-certificate present?	✓
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 :	**PASSED**
Is the certificate unique?	✓
Is a pseudonym used?	✓
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signers certificate have an expected key-usage?	✓
Is the authority info access present?	✓
Is the revocation info access present?	✓
Is the revocation data present for the certificate?	✓
Is the revocation acceptance check conclusive?	✓
Is there a satisfying revocation status information?	✓
Is the revocation freshness check conclusive?	✓
Is the certificate not revoked?	✓
Is the certificate on hold?	✓
Are certificate cryptographic constraints met?	✓
Is the current time in the validity range of the signers certificate?	✓
Revocation Acceptance Validation :	**PASSED**
Is the revocation data consistent?	✓
Is revocations signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificates signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Revocation Freshness Checker :	**PASSED**
Is an acceptable revocation data present for the certificate?	✓
Is there a Next Update defined for the revocation data?	✓
Is the revocation information fresh for the certificate?	IGNORED

Are revocation cryptographic constraints met?	✓
Trust Anchor	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is the signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Is the structure of the signature valid?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signed qualifying property: message-digest or SignedProperties present?	✓
Are signature cryptographic constraints met?	✓

Basic Building Blocks
SIGNATURE - S-F43B7E69EBF2E51E4C534FD86B1DED4FFCAC456EA6418E2C1D69F53104E24B79

Does the signature format correspond to an expected format?	✓
Is the signature identification not ambiguous?	✓
Is only one SignerInfo present?	✓
Identification of the Signing Certificate :	**PASSED**
Is there an identified candidate for the signing certificate?	✓
Is the signed attribute: signing-certificate present?	✓
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 :	**PASSED**
Is the certificate unique?	✓
Is a pseudonym used?	✓
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signers certificate have an expected key-usage?	✓
Is the authority info access present?	✓
Is the revocation info access present?	✓
Is the revocation data present for the certificate?	✓
Is the revocation acceptance check conclusive?	✓
Is there a satisfying revocation status information?	✓
Is the revocation freshness check conclusive?	✓
Is the certificate not revoked?	✓
Is the certificate on hold?	✓
Are certificate cryptographic constraints met?	✓
Is the current time in the validity range of the signers certificate?	✓
Revocation Acceptance Validation :	**PASSED**

Is the revocation data consistent?	✓
Is revocations signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificates signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Revocation Freshness Checker :	**PASSED**
Is an acceptable revocation data present for the certificate?	✓
Is there a Next Update defined for the revocation data?	✓
Is the revocation information fresh for the certificate?	IGNORED
Are revocation cryptographic constraints met?	✓
Trust Anchor	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is the signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Is the structure of the signature valid?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signed qualifying property: message-digest or SignedProperties present?	✓
Are signature cryptographic constraints met?	✓

Basic Building Blocks
SIGNATURE - S-80C2DD2BBAAE076E85A43BA76F21D39AC65DAF3DB81C5E55EA33F25C6177D4DC

Does the signature format correspond to an expected format?	✓
Is the signature identification not ambiguous?	✓
Is only one SignerInfo present?	✓
Identification of the Signing Certificate :	**PASSED**
Is there an identified candidate for the signing certificate?	✓
Is the signed attribute: signing-certificate present?	✓
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 :	**PASSED**
Is the certificate unique?	✓
Is a pseudonym used?	✓
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signers certificate have an expected key-usage?	✓
Is the authority info access present?	✓
Is the revocation info access present?	✓

Is the revocation data present for the certificate?	✓
Is the revocation acceptance check conclusive?	✓
Is the revocation acceptance check conclusive?	✓
Is the revocation acceptance check conclusive?	✓
Is there a satisfying revocation status information?	✓
Is the revocation freshness check conclusive?	✓
Is the certificate not revoked?	✓
Is the certificate on hold?	✓
Are certificate cryptographic constraints met?	✓
Is the current time in the validity range of the signers certificate?	✓
Revocation Acceptance Validation :	**PASSED**
Is the revocation data consistent?	✓
Is revocations signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificates signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Revocation Acceptance Validation :	**PASSED**
Is the revocation data consistent?	✓
Is revocations signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	**PASSED**
Is the revocation data consistent?	✓
Is revocations signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificates signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Revocation Freshness Checker :	**PASSED**
Is an acceptable revocation data present for the certificate?	✓
Is there a Next Update defined for the revocation data?	✓
Is the revocation information fresh for the certificate?	IGNORED
Are revocation cryptographic constraints met?	✓
Trust Anchor	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is the signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Is the structure of the signature valid?	✓
Is the signed qualifying property: signing-time present?	✓
Is the signed qualifying property: message-digest or SignedProperties present?	✓
Are signature cryptographic constraints met?	✓

Basic Building Blocks

TIMESTAMP - T-2AC540BA497D2207305C1A5F4A119F676A7447D987A052C7B71A275A990CC1CD

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	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✔
Is the reference data object intact?	✔
Is timestampss signature intact?	✔
Signature Acceptance Validation :	**PASSED**
Are timestamp cryptographic constraints met?	✔

Basic Building Blocks
TIMESTAMP - T-55B2AD737475E7802F3A4BC5F906B574119261728FFB95D989B869528C32DEDE

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	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✔
Is the reference data object intact?	✔
Is timestampss signature intact?	✔
Signature Acceptance Validation :	**PASSED**
Are timestamp cryptographic constraints met?	✔

Basic Building Blocks
TIMESTAMP - T-577702815B0B7836B0018ADB3A4C6306CCDA85B62E1B92AC33BAB324FB015EE5

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	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✔
Is the reference data object intact?	✔
Is timestampss signature intact?	✔
Signature Acceptance Validation :	**PASSED**
Are timestamp cryptographic constraints met?	✔

Basic Building Blocks
TIMESTAMP - T-953AEA1CED17DE569C4E132C3C0EC6CC0A43CF75FEBFBFE0D76022A9B46608E4

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	**PASSED**

Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestampss signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are timestamp cryptographic constraints met?	✓

Basic Building Blocks
TIMESTAMP - T-FB92510FA263A25CC0C1FA41C6C2E0BF7937A9634DFC54719FF3DEEA51BC48DB

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	**PASSED**
Cryptographic Verification :	**PASSED**
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestampss signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are timestamp cryptographic constraints met?	✓

Basic Building Blocks
REVOCATION - R-1B37A79155000ADF27D927E6186F2650DAAE74177FB9B33A7F9E8906347A62B8

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	**PASSED**
Cryptographic Verification :	**PASSED**
Is revocations signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are revocation cryptographic constraints met?	✓

Basic Building Blocks
REVOCATION - R-DE2AFD387853FABE2A0BEDF2A148572A1582FE560FC684F11E5DB9F29B361314

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 :	**PASSED**
Is the certificate signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Are certificate cryptographic constraints met?	✓
Is the current time in the validity range of the signers certificate?	✓

Trust Anchor	**PASSED**
Cryptographic Verification :	**PASSED**
Is revocations signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are revocation cryptographic constraints met?	✓

Basic Building Blocks
REVOCATION - R-0AAD93660A26BF1ECC5DD64985976906B0C7DB26C0030FF95338068C62357908

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?	!
Cryptographic Verification :	**PASSED**
Is revocations signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are revocation cryptographic constraints met?	✓

Basic Building Blocks
REVOCATION - R-B9A13D5E818A9B65668EBF85A01FEBE30CE55306ADAE635CA88EE2C0BB086A26

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 :	**PASSED**
Is the certificate signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Are certificate cryptographic constraints met?	✓
Is the current time in the validity range of the signers certificate?	✓
Trust Anchor	**PASSED**
Cryptographic Verification :	**PASSED**
Is revocations signature intact?	✓
Signature Acceptance Validation :	**PASSED**
Are revocation cryptographic constraints met?	✓

Basic Building Blocks
REVOCATION - R-B4C98AE539E915CFA7B13E01863D213186A95B6D8F2B2286D2C3381B1A67D16E

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 :	**PASSED**
Is the certificate signature intact?	✓
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)	✓
Are certificate cryptographic constraints met?	✓

Is the current time in the validity range of the signers certificate?

Trust Anchor **PASSED**

Cryptographic Verification : **PASSED**

Is revocations signature intact?

Signature Acceptance Validation : **PASSED**

Are revocation cryptographic constraints met?

Basic Building Blocks
REVOCATION - R-C4DDB0B3C27C39D9F3EB5265D60C9AEE325E3565205304F4BF173CA5245BB05E

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 : **PASSED**

Is the certificate signature intact?

The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)

Are certificate cryptographic constraints met?

Is the current time in the validity range of the signers certificate?

Trust Anchor **PASSED**

Cryptographic Verification : **PASSED**

Is revocations signature intact?

Signature Acceptance Validation : **PASSED**

Are revocation cryptographic constraints met?

List Of Trusted Lists EU

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?

Conclusion : **PASSED**

Trusted List CZ

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?

Conclusion : **PASSED**

Trusted List BE

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?

Conclusion : **PASSED**

Trusted List NL

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?

Conclusion : **PASSED**