

Validation Process for Basic Signatures

INDETERMINATE - TRY_LATER

Is the result of the Basic Validation Process conclusive?

✘

Timestamp T-AA3729353600C17007012EBB42093BA3E56A776A52A8B276D9560C1FD37CCE12**Validation Process for Timestamps**

PASSED

Is the result of the timestamps validation process conclusive?

✔

Timestamp Qualification

QTSA

Has a trusted list been reached for the certificate chain?

✔

Is the list of trusted lists acceptable?

✔

Is the trusted list acceptable?

✔

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?

✔

Timestamp T-A152AFE20F8E2C109FBFB70D0D907C49794F9D2163A139A9AF10B4E59E10ACBF**Validation Process for Timestamps**

PASSED

Is the result of the timestamps validation process conclusive?

✔

Timestamp Qualification

QTSA

Has a trusted list been reached for the certificate chain?

✔

Is the list of trusted lists acceptable?

✔

Is the trusted list acceptable?

✔

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?

✔

Timestamp T-782337BECAB3C2374B4EC073AE3BD43395D1BA8BB6699E164E42240A5D5FFD1E**Validation Process for Timestamps**

PASSED

Is the result of the timestamps validation process conclusive?

✔

Timestamp Qualification

QTSA

Has a trusted list been reached for the certificate chain?

✔

Is the list of trusted lists acceptable?

✔

Is the trusted list acceptable?

✔

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

PASSED

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?

👁

Is the revocation freshness check conclusive?

✔

Is the signature acceptable?

✔

Validation Process for Signatures with Archival Data

PASSED

Is the result of the LTV validation process acceptable?

✔

Signature Qualification

AdESig-QC

Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)?

✔

Has a trusted list been reached for the certificate chain?

✔

Is the list of trusted lists acceptable?

✔

Is the trusted list acceptable?

✔

Has been an acceptable trusted list found?

✔

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

QC for eSig

- Is the certificate related to a CA/QC?
- Is the trust service consistent?
- Is the certificate related to a trust service with a granted status?
- Is the certificate related to a consistent trust service declaration?
- Can the certificate type be issued by a found trust service?
- Does the trusted certificate match the trust service?
- Is the certificate qualified at issuance time?
- Is the certificate for eSig at issuance time?
- Does the private key reside in a QSCD at issuance time?



Certificate Qualification at best signature time

QC for eSig

- Is the certificate related to a CA/QC?
- Is the trust service consistent?
- Is the certificate related to a trust service with a granted status?
- Is the certificate related to a consistent trust service declaration?
- Can the certificate type be issued by a found trust service?
- Does the trusted certificate match the trust service?
- Is the certificate qualified at (best) signing time?
- Is the certificate for eSig at (best) signing time?
- Does the private key reside in a QSCD at (best) signing time?



Signature S-6C462D085C5C1B98B26A4D887632E6582D3E8581573C49B8557EDF08A756E819

Validation Process for Basic Signatures

PASSED

- Is the result of the Basic Validation Process conclusive?



Timestamp T-D1203E4D8064B2F74D8B7F2149E9F733E3AC34E3C34BEDEEE409143108226DA6

Validation Process for Timestamps

PASSED

- Is the result of the timestamps validation process conclusive?



Timestamp Qualification

QTSA

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



Timestamp T-782337BECAB3C2374B4EC073AE3BD43395D1BA8BB6699E164E42240A5D5FFD1E

Validation Process for Timestamps

PASSED

- Is the result of the timestamps validation process conclusive?



Timestamp Qualification

QTSA

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

PASSED

- 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 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?
- Is the signature acceptable?



Validation Process for Signatures with Archival Data

PASSED

- Is the result of the LTV validation process acceptable?



Signature Qualification

AdESig

- 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?	✓
Is the trusted list acceptable?	✓
Has been an acceptable trusted list found?	✓
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	Cert for eSig
Is the certificate related to a CA/QC?	✗
Certificate Qualification at best signature time	Cert for eSig
Is the certificate related to a CA/QC?	✗

Signature S-13A7DA79A1014659AC9666D88C9C54E87BCE9B5AE63D49010F43C3EDABEE740C

Validation Process for Basic Signatures

INDETERMINATE - TRY_LATER

Is the result of the Basic Validation Process conclusive?	✗
---	---

Timestamp T-4727247AEF1A6048931A7808D0BAC4EC1B66EB428AE60DC558E4507C9FD6A7B4

Validation Process for Timestamps

PASSED

Is the result of the timestamps validation process conclusive?	✓
--	---

Timestamp Qualification

QTSA

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

Timestamp T-782337BECAB3C2374B4EC073AE3BD43395D1BA8BB6699E164E42240A5D5FFD1E

Validation Process for Timestamps

PASSED

Is the result of the timestamps validation process conclusive?	✓
--	---

Timestamp Qualification

QTSA

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

PASSED

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?	👁
Is the revocation freshness check conclusive?	✓
Is the signature acceptable?	✓

Validation Process for Signatures with Archival Data

PASSED

Is the result of the LTV validation process acceptable?	✓
---	---

Signature Qualification

AdESig-QC

Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)?	✓
Has a trusted list been reached for the certificate chain?	✓
Is the list of trusted lists acceptable?	✓
Is the trusted list acceptable?	✓
Has been an acceptable trusted list found?	✓
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 trust service consistent?
- Is the certificate related to a trust service with a granted status?
- Is the certificate related to a consistent trust service declaration?
- Can the certificate type be issued by a found trust service?
- Does the trusted certificate match the trust service?
- Is the certificate qualified at issuance time?
- Is the certificate for eSig at issuance time?
- Does the private key reside in a QSCD at issuance time?

QC for eSig

- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- !

Certificate Qualification at best signature time

- Is the certificate related to a CA/QC?
- Is the trust service consistent?
- Is the certificate related to a trust service with a granted status?
- Is the certificate related to a consistent trust service declaration?
- Can the certificate type be issued by a found trust service?
- Does the trusted certificate match the trust service?
- Is the certificate qualified at (best) signing time?
- Is the certificate for eSig at (best) signing time?
- Does the private key reside in a QSCD at (best) signing time?

QC for eSig

- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- !

Basic Building Blocks

SIGNATURE - S-13A7DA79A1014659AC9666D88C9C54E87BCE9B5AE63D49010F43C3EDABEE740C

Format Checking :

- Does the signature format correspond to an expected format?
- Is the signature identification not ambiguous?
- Is only one SignerInfo present?

PASSED

- ✔
- ✔
- ✔

Identification of the Signing Certificate :

- Is there an identified candidate for the signing certificate?
- Is the signed attribute: 'signing-certificate' present?
- Is the signed attribute: 'signing-certificate' present only once?
- 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?

PASSED

- ✔
- ✔
- ✔
- ✔
- ✔
- ✔

Validation Context Initialization :

- Is the signature policy known?

PASSED

- ✔

X509 Certificate Validation :

- Can the certificate chain be built till a trust anchor?
- Is the certificate validation conclusive?

TRY_LATER

- ✔
- ✘

Certificate C-

B395538A2042EB99CEEC06F0AB09B49FF137C173BC98F9EB7228881B28F13399 :

- 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?
- 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?

TRY_LATER

- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✔
- ✘

Revocation Acceptance Validation :

- Is the revocation status known?
- Is the revocation data consistent?
- Is revocation's signature intact?
- Can the certificate chain be built till a trust anchor?

PASSED

- ✔
- ✔
- ✔
- ✔

Revocation Acceptance Validation :

- Is the revocation status known?
- Is the revocation data consistent?
- Is revocation's signature intact?
- Can the certificate chain be built till a trust anchor?

PASSED

- ✔
- ✔
- ✔
- ✔

Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificate's signature intact?	✓
Has the issuer certificate id-pkix-ocsp-nocheck extension?	✓
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?	✗
Are revocation cryptographic constraints met?	✓
Trust Anchor (C-7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE480ECF6F711)	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-6C462D085C5C1B98B26A4D887632E6582D3E8581573C49B8557EDF08A756E819	
Format Checking :	PASSED
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: 'signing-certificate' present only once?	✓
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 C-8E8D691889F528766B5C4C132240A73807B45713FF8CC1E28EBF7F278F98EDAD :	PASSED
Is the certificate unique?	✓
Is a pseudonym used?	✓
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signer's certificate have an expected key-usage?	✓
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 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 signer's certificate?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓

Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
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?	⚡
Are revocation cryptographic constraints met?	✓
Trust Anchor (C-D82F87F93D31D5FC818DD66BD50E7F319AE179FC1C5D00547B658E8EB3F4CE56)	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-870609011E93511FBA26BC6EFB9FC1C6B46D2C89CD7A510104FC6D2EBC0BD2CF	
Format Checking :	PASSED
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: 'signing-certificate' present only once?	✓
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 :	TRY_LATER
Can the certificate chain be built till a trust anchor?	✓
Is the certificate validation conclusive?	✗
Certificate C-B395538A2042EB99CEEC06F0AB09B49FF137C173BC98F9EB7228881B28F13399 :	TRY_LATER
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?	✓
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?	✗
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓

Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificate's signature intact?	✓
Has the issuer certificate id-pkix-ocsp-nocheck extension?	✓
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?	⚠
Are revocation cryptographic constraints met?	✓
Trust Anchor (C-7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711)	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-AA3729353600C17007012EBB42093BA3E56A776A52A8B276D9560C1FD37CCE12	
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: 'signing-certificate' present only once?	✓
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)?	✓
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 C-626D6426702581D2D772A8CF725A3F8D78CAA9468E69728E6FE8E11060986CD3 :	PASSED
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signer's certificate have an expected 'extended key-usage(s)'?	✓
Is the revocation data present for the certificate?	✓
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 signer's certificate?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
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?	⚠
Are revocation cryptographic constraints met?	✓

Trust Anchor PASSED
(C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)

Cryptographic Verification :	PASSED
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestamp's signature intact?	✓

Signature Acceptance Validation :	PASSED
Are timestamp cryptographic constraints met?	✓

Basic Building Blocks
TIMESTAMP - T-A152AFE20F8E2C109FBFB70D0D907C49794F9D2163A139A9AF10B4E59E10ACBF

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: 'signing-certificate' present only once?	✓
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)?	✓

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
C-711C531F7D49F99550A8FCA293399A3A8A5AE98BB2820DACDC48E07CFA1AD268 :

Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signer's certificate have an expected 'extended key-usage(s)'?	✓
Is the revocation data present for the certificate?	✓
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 signer's certificate?	✓

Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓

Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓

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?	⚠
Are revocation cryptographic constraints met?	✓

Trust Anchor PASSED
(C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)

Cryptographic Verification :	PASSED
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestamp's signature intact?	✓

Signature Acceptance Validation :	PASSED
Are timestamp cryptographic constraints met?	✓

Basic Building Blocks
TIMESTAMP - T-D1203E4D8064B2F74D8B7F2149E9F733E3AC34E3C34BEDEEE409143108226DA6

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: 'signing-certificate' present only once?	✓
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)?	✓
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
C-626D6426702581D2D772A8CF725A3F8D78CAA9468E69728E6FE8E11060986CD3 :	
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signer's certificate have an expected 'extended key-usage(s)'?	✓
Is the revocation data present for the certificate?	✓
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 signer's certificate?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
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?	⚠
Are revocation cryptographic constraints met?	✓
Trust Anchor	PASSED
(C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)	
Cryptographic Verification :	PASSED
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestamp's signature intact?	✓
Signature Acceptance Validation :	PASSED
Are timestamp cryptographic constraints met?	✓
Basic Building Blocks	
TIMESTAMP - T-4727247AEF1A6048931A7808D0BAC4EC1B66EB428AE60DC558E4507C9FD6A7B4	
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: 'signing-certificate' present only once?	✓
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)?	✓
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 C-	PASSED
CD12DF942CCD427DD35CA8A6A9C38FF6CEDA7DFB22B76AD8B7FAA40A48F96E4F :	
Is certificate not self-signed?	✓
Is the certificate signature intact?	✓
Does the signer's certificate have an expected 'extended key-usage(s)'?	✓
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 signer's certificate? ✔

Revocation Acceptance Validation : **PASSED**

- Is the revocation status known? ✔
- Is the revocation data consistent? ✔
- Is revocation's signature intact? ✔
- Can the certificate chain be built till a trust anchor? ✔

Revocation Acceptance Validation : **PASSED**

- Is the revocation status known? ✔
- Is the revocation data consistent? ✔
- Is revocation's signature intact? ✔
- Can the certificate chain be built till a trust anchor? ✔
- Is certificate's signature intact? ✔
- Has the issuer certificate id-pkix-ocsp-nocheck extension? ✔

Revocation Acceptance Validation : **PASSED**

- Is the revocation status known? ✔
- Is the revocation data consistent? ✔
- Is revocation's signature intact? ✔
- Can the certificate chain be built till a trust anchor? ✔

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? 🕒
- Are revocation cryptographic constraints met? ✔

Trust Anchor **PASSED**
(C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)

Cryptographic Verification : **PASSED**

- Has the reference data object been found? ✔
- Is the reference data object intact? ✔
- Is timestamp's signature intact? ✔

Signature Acceptance Validation : **PASSED**

- Are timestamp cryptographic constraints met? ✔

Basic Building Blocks
TIMESTAMP - T-782337BECAB3C2374B4EC073AE3BD43395D1BA8BB6699E164E42240A5D5FFD1E

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: 'signing-certificate' present only once? ✔
- 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)? ✔

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 C- **PASSED**
CD12DF942CCD427DD35CA8A6A9C38FF6CEDA7DFB22B76AD8B7FAA40A48F96E4F :

- Is certificate not self-signed? ✔
- Is the certificate signature intact? ✔
- Does the signer's certificate have an expected 'extended key-usage(s)'? ✔
- 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 signer's certificate?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
Is certificate's signature intact?	✓
Has the issuer certificate id-pkix-ocsp-nocheck extension?	✓
Revocation Acceptance Validation :	PASSED
Is the revocation status known?	✓
Is the revocation data consistent?	✓
Is revocation's signature intact?	✓
Can the certificate chain be built till a trust anchor?	✓
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?	✗
Are revocation cryptographic constraints met?	✓
Trust Anchor (C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)	PASSED
Cryptographic Verification :	PASSED
Has the reference data object been found?	✓
Is the reference data object intact?	✓
Is timestamp's signature intact?	✓
Signature Acceptance Validation :	PASSED
Are timestamp cryptographic constraints met?	✓
Basic Building Blocks REVOCATION - R-8639D0EA228C7CD3476125CD6EAE0EDA4E05B94AEAD126AE77EAB0F981E25CE7	
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 (C-7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711)	PASSED
Cryptographic Verification :	PASSED
Is revocation's signature intact?	✓
Signature Acceptance Validation :	PASSED
Are revocation cryptographic constraints met?	✓
Basic Building Blocks REVOCATION - R-54719ABF1CCDC1B04DBA6AB59D1A4986A8BC2D2AD0307428BE42C26D243C75D5	
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 (C- D82F87F93D31D5FC818DD66BD50E7F319AE179FC1C5D00547B658E8EB3F4CE56)	PASSED
Cryptographic Verification :	PASSED
Is revocation's signature intact?	✓
Signature Acceptance Validation :	PASSED
Are revocation cryptographic constraints met?	✓
Basic Building Blocks REVOCATION - R-94C4F5E33BEC167E48FC8D5FD9775594469528ED66BC8F6ED6F07F5FF2E7264E	
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 (C-7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711)	PASSED
Cryptographic Verification :	PASSED
Is revocation's signature intact?	✔
Signature Acceptance Validation :	PASSED
Are revocation cryptographic constraints met?	✔
Basic Building Blocks REVOCATION - R-FB6207D6602E4A7DE29FC73C5E80A3490273E71724BD6670054857B96D37EBE7	
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 (C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)	PASSED
Cryptographic Verification :	PASSED
Is revocation's signature intact?	✔
Signature Acceptance Validation :	PASSED
Are revocation cryptographic constraints met?	✔
Basic Building Blocks REVOCATION - R-95D660C73C71EC0D27B525B96DE8E5E94E265E9D0A773E539245C39B29C1BC75	
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 C- AE5741EDAB35ED5B30FDCEEA2A829CB9C541452F75B497F235DFC6A72D948D4E :	PASSED
Is the certificate signature intact?	✔
Has the issuer certificate id-pkix-ocsp-nocheck extension?	✔
Are certificate cryptographic constraints met?	✔
Is the current time in the validity range of the signer's certificate?	✔
Trust Anchor (C-7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711)	PASSED
Cryptographic Verification :	PASSED
Is revocation's signature intact?	✔
Signature Acceptance Validation :	PASSED
Are revocation cryptographic constraints met?	✔
Basic Building Blocks REVOCATION - R-17C9238F3A420267E33A30F984D3924C5B4DD60EEAE63780B82304B6EBCE4A63	
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 C-9DEAD62CEA25C89975BD6430301F8A29484A29D90592E43F3422B6374C8D6EB4 :	PASSED
Is the certificate signature intact?	✔
Has the issuer certificate id-pkix-ocsp-nocheck extension?	✔
Are certificate cryptographic constraints met?	✔
Is the current time in the validity range of the signer's certificate?	✔
Trust Anchor (C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)	PASSED

Cryptographic Verification : PASSED
Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED
Are revocation cryptographic constraints met? ✓

Basic Building Blocks

REVOCATION - R-C996D822DDDD92D3A569F33D0B196C7E256EFCBCF2A11F9BB118F4DD2108915B

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
(C-6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E)

Cryptographic Verification : PASSED
Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED
Are revocation cryptographic constraints met? ✓

Basic Building Blocks

REVOCATION - R-7021ACC36657DF9BC609411C05C0E9A74B80A68EC40D367AA969AF7936BDCE45

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 (C- PASSED
D82F87F93D31D5FC818DD66BD50E7F319AE179FC1C5D00547B658E8EB3F4CE56)

Cryptographic Verification : PASSED
Is revocation's 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? ✓

Trusted List HU

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? ✓