Signature S-8DFF69F8DE2D7BE8F2C08CA8665CB605B2850E9612C26368FDEEB6CA4C60DA5F

Validation Process for Basic Signatures — PASSED

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

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 an acceptable revocation data present for the certificate? ✓
- 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 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-87DB05254A112291F739FABED34606B8EFF606516FFF921849DF645A6A29ABED

Validation Process for Basic Signatures — PASSED

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

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 an acceptable revocation data present for the certificate? ✓
- 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 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-6ABFD18DEE8DF723363160C28056D60F9A268775B0F37612C54E07E2340E82D6

Validation Process for Basic Signatures — **PASSED**

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

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 an acceptable revocation data present for the certificate? ✓
- 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 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-4E45B8A7FB025C608E4A422D9F450598D5A585F29D1EFB9EA92AF29F9FEE3B56

Validation Process for Basic Signatures — **PASSED**

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

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 an acceptable revocation data present for the certificate? ✓
- 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 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? !

Basic Building Blocks

SIGNATURE - S-8DFF69F8DE2D7BE8F2C08CA8665CB605B2850E9612C26368FDEEB6CA4C60DA5F

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-7FC96DE843D794971F3D2BFBB02541C1B0D802DC7A7A5050DB61A9689083021D : 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 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?
Is certificate's signature intact?
Is the revocation data present for the revocation issuer?
Is the revocation acceptance check conclusive?
Is an acceptable revocation data present for the certificate?
Is there a satisfying revocation status information?

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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) 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-6ABFD18DEE8DF723363160C28056D60F9A268775B0F37612C54E07E2340E82D6

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-7FC96DE843D794971F3D2BFBB02541C1B0D802DC7A7A5050DB61A9689083021D : 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 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?
Is certificate's signature intact?
Is the revocation data present for the revocation issuer?
Is the revocation acceptance check conclusive?
Is an acceptable revocation data present for the certificate?
Is there a satisfying revocation status information?

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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) 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-87DB05254A112291F739FABED34606B8EFF606516FFF921849DF645A6A29ABED

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-7FC96DE843D794971F3D2BFBB02541C1B0D802DC7A7A5050DB61A9689083021D : 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 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? ✓
Is certificate's signature intact? ✓
Is the revocation data present for the revocation issuer? ✓
Is the revocation acceptance check conclusive? ✓
Is an acceptable revocation data present for the certificate? ✓
Is there a satisfying revocation status information? ✓

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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) 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-4E45B8A7FB025C608E4A422D9F450598D5A585F29D1EFB9EA92AF29F9FEE3B56

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-7FC96DE843D794971F3D2BFBB02541C1B0D802DC7A7A5050DB61A9689083021D : 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 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? ✓
- Is certificate's signature intact? ✓
- Is the revocation data present for the revocation issuer? ✓
- Is the revocation acceptance check conclusive? ✓
- Is an acceptable revocation data present for the certificate? ✓
- Is there a satisfying revocation status information? ✓

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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) 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

REVOCATION - R-8472C536ED9A72FD3572CC7E3712C2D5A21D363B07CA0560C2310B0A7F087690

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-DD6D5EBBF946BB9E8D470C05FBA2A5459A93D873E4CC38AB58CF04DBEC14DB43 : PASSED

- Is the certificate signature intact? ✓
- 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 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 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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) PASSED

Cryptographic Verification : PASSED

- Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED

- Are revocation cryptographic constraints met? ✓

Basic Building Blocks

REVOCATION - R-ADFFA84DE98A6185479A249437CE6CACC1544BEA75694CA542288E6E99AF8EE2

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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) PASSED

Cryptographic Verification : PASSED

- Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED

- Are revocation cryptographic constraints met? ✓

Basic Building Blocks

REVOCATION - R-9F5BC49ADE669A22A2465DBB803123238917221069344559 18FF3F2DBEC35363

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-DD6D5EBBF946BB9E8D470C05FBA2A5459A93D873E4CC38AB58CF04DBEC14DB43 : PASSED

- Is the certificate signature intact? ✓
- 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 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 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-73B2E40CFEA79BD5CF9F6B100EC8262DE4B31499C80BD7DF12BC686C3B6F0B6B) PASSED

Cryptographic Verification : PASSED

- Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED

- Are revocation cryptographic constraints met? ✓

Basic Building Blocks

REVOCATION - R-178E053D7F462290FAD9BCF6D800A29989235FC14F79C5B75DCA3D22A3E68F15

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-944F1E01408F0FD0A20820BCB92044971E5F15AC5DC69871149BFCD0BBF3016D) (Self Signed) PASSED

Cryptographic Verification : PASSED

- Is revocation's signature intact? ✓

Signature Acceptance Validation : PASSED

- Are revocation cryptographic constraints met? ✓

Trusted List UA

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?	✓