

### Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive?



Conclusion : **INDETERMINATE - CRYPTO\_CONSTRAINTS\_FAILURE\_NO\_POE**

### 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 result of the revocation data validation process acceptable?



Are signature cryptographic constraints met?



Are certificate cryptographic constraints met?



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 (ETSI EN 319 102-1) ?



Is the certificate path trusted?



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?



Is the private key on a QSCD at (best) signing time?



### Certificate Qualification @ 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?



Is the certificate type can be issued by a found trust service(s)?



Is the trusted certificate match the trust service ?



Is the certificate qualified at issuance time?



Is the certificate for eSig at issuance time?



Is the private key on a QSCD at issuance time?



## Certificate Qualification @ 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?	✔
Is the certificate type can be issued by a found trust service(s)?	✔
Is the trusted certificate match the trust service ?	✔
Is the certificate qualified at (best) signing time?	✔
Is the certificate for eSig at (best) signing time?	✔
Is the private key on a QSCD at (best) signing time?	✔

## Basic Building Blocks

SIGNATURE - S-B34CF3F278A76F342D3998267AFC698BC2B44985C9EE07EC1A177E7CAC03D813

Is the expected format found?	✔
<b>Identification of the Signing Certificate :</b>	<b>PASSED</b>
Is there an identified candidate for the signing certificate?	✔
<b>Validation Context Initialization :</b>	<b>PASSED</b>
Is the signature policy known?	✔
<b>X509 Certificate Validation :</b>	<b>INDETERMINATE</b>
Can the certificate chain be built till the trust anchor?	✔
Is the certificate validation concluant ?	✘
<b>Certificate :</b>	<b>INDETERMINATE</b>
Is the certificate unique ?	✔
Is pseudo used ?	✔
Is not self-signed certificate?	✔
Is the certificate's signature intact?	✔
Are certificate cryptographic constraints met?	✔
Has the signer's certificate given key-usage?	✔
Is authority info access present?	!
Is revocation info access present?	✔
Is the current time in the validity range of the signer's certificate?	✔
Is the certificate not revoked?	✔
Is the certificate on hold?	✔
Is the revocation freshness check concluant ?	✘
<b>Revocation Freshness Checker :</b>	<b>INDETERMINATE</b>
Is the 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?	✘
<b>Trust Anchor</b>	<b>PASSED</b>
<b>Cryptographic Verification :</b>	<b>PASSED</b>
Is the reference data object found?	✔
Is the reference data object intact?	✔
Is the signature intact?	✔
<b>Signature Acceptance Validation :</b>	<b>PASSED</b>

- Is signed qualifying property: 'signing-time' present? ✔
- Is signed qualifying property: 'message-digest' or 'SignedProperties' present? ✔
- Are signature cryptographic constraints met? ✔

**Basic Building Blocks**  
 REVOCATION - R-7886BA663125576BC299FCB9FD69236BDB2E9B3990DE6D45002B8B733D642DA

- 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 the trust anchor? ✔
- Is the certificate validation concluant ? ✔
- Is the certificate validation concluant ? ✔
- Certificate :** **PASSED**
- Is the certificate's signature intact? ✔
- Are certificate cryptographic constraints met? ✔
- Is the current time in the validity range of the signer's certificate? ✔
- Is the certificate not revoked? ✔
- Is the certificate on hold? ✔
- Is the revocation freshness check concluant ? ✔
- Revocation Freshness Checker :** **PASSED**
- Is the 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**
- Is the signature intact? ✔
- Signature Acceptance Validation :** **INDETERMINATE**
- Are revocation cryptographic constraints met? ✘

**Basic Building Blocks**  
 REVOCATION - R-E32B58149D77868D9AA8F77DF388627E7404A4D250F5591B6D228C2699536EA

- 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 the trust anchor? ✔
- Is the certificate validation concluant ? ✔
- Trust Anchor** **PASSED**
- Cryptographic Verification :** **PASSED**
- Is the signature intact? ✔
- Signature Acceptance Validation :** **PASSED**
- Are revocation cryptographic constraints met? ✔

**Trusted List EU**

- Is the trusted list fresh ? ❗
- Is the trusted list not expired ? ✔
- Is the trusted list has the expected version ? ✔

Is the trusted list well signed ?



Conclusion : **PASSED**

### Trusted List PT

Is the trusted list fresh ?



Is the trusted list not expired ?



Is the trusted list has the expected version ?



Is the trusted list well signed ?



Conclusion : **PASSED**