



Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive? 
Conclusion : **INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND**



Validation Process for Signatures with Time and Signatures with Long-Term Validation Data

Is the result of the Basic Validation Process acceptable? 
Conclusion : **INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND**

Validation Process for Signatures with Archival Data


















Is the result of the LTV validation process acceptable? 
Conclusion : **INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND**

Qualification Signature : N/A

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

Basic Building Blocks

SIGNATURE - id-e872c44e92b668e124b8fb2f54032acef02e3b250d06a84a14944f9c2e03f588

Is the expected format found? 
Identification of the signing certificate (ISC) : **PASSED**
Is there an identified candidate for the signing certificate? 
Is the signing certificate signed? 
Is the signed attribute: 'signing-certificate' present? 
Is the signed attribute: 'cert-digest' of the certificate present? 
Is the certificate's digest value valid? 
Are the issuer distinguished name and the serial number equal? 
Validation Context Initialization (VCI) : **PASSED**
Is the signature policy known? 
Cryptographic Verification (CV) : **PASSED**
Is the reference data object(s) found? 
Is the reference data object(s) intact? 
Is the signature intact? 
Signature Acceptance Validation (SAV) : **PASSED**
Is signed qualifying property: 'signing-time' present? 
Are signature cryptographic constraints met? 
X509 Certificate Validation (XCV) : **INDETERMINATE**
Can the certificate chain be built till the trust anchor? 
Certificate : **PASSED**
Is the certificate unique ? 
Is pseudo used ? 
Is not self-signed certificate? 
Is the certificate's signature intact? 

Are signature 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 ?	✔
Revocation Freshness Checker (RFC) :	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?	✔
Are signature cryptographic constraints met?	✔
Certificate :	PASSED
Is the certificate's signature intact?	✔
Are signature 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 (RFC) :	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?	✔
Are signature cryptographic constraints met?	✔
Certificate :	PASSED
Is the certificate's signature intact?	✔
Are signature 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 (RFC) :	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?	✔
Are signature cryptographic constraints met?	✔
Certificate :	INDETERMINATE
Is the certificate's signature intact?	✔
Are signature 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 (RFC) :	INDETERMINATE
Is the revocation data present for the certificate?	✖

Basic Building Blocks

REVOCATION -

700f1ffc3b2fb90f0790a21035fea0c11b215155d9738a67d0f5c7cf2499cc6001c3c5c99301a045f16f801f2680b40b3b84832e4789199699675c9755

Identification of the signing certificate (ISC) :

Is there an identified candidate for the signing certificate?

PASSED



Cryptographic Verification (CV) :

Is the reference data object(s) found?

PASSED



Is the reference data object(s) intact?



Is the signature intact?



Signature Acceptance Validation (SAV) :

Are signature cryptographic constraints met?

PASSED



X509 Certificate Validation (XCV) :

Can the certificate chain be built till the trust anchor?

PASSED



Is the certificate validation concluant ?



Is the certificate validation concluant ?



Is the certificate validation concluant ?



Is the certificate validation concluant ?



Certificate :

Is the certificate's signature intact?

PASSED



Are signature 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?



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



Certificate :

Is the certificate's signature intact?

PASSED



Are signature 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 (RFC) :

Is the revocation data present for the certificate?

PASSED



Is there a Next Update defined for the revocation data?



Is the revocation information fresh for the certificate?



Are signature cryptographic constraints met?



Certificate :

Is the certificate's signature intact?

PASSED



Are signature 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 (RFC) :

Is the revocation data present for the certificate?

PASSED



Is there a Next Update defined for the revocation data?



Is the revocation information fresh for the certificate?	✔
Are signature cryptographic constraints met?	✔
Certificate :	PASSED
Is the certificate's signature intact?	✔
Are signature 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 (RFC) :	PASSED
Is the revocation data present for the certificate?	!

Basic Building Blocks

REVOCATION -

5db47c4a066f17c3c8ac5505b7cc88f4cd8bf35252ca102ba43cf1521aaa1287443bf50aa2d84038edc0244f8aae80c5e4004d8f7767978d3beac56

Identification of the signing certificate (ISC) :	PASSED
Is there an identified candidate for the signing certificate?	✔
Cryptographic Verification (CV) :	PASSED
Is the reference data object(s) found?	✔
Is the reference data object(s) intact?	✔
Is the signature intact?	✔
Signature Acceptance Validation (SAV) :	PASSED
Are signature cryptographic constraints met?	✔
X509 Certificate Validation (XCV) :	PASSED
Can the certificate chain be built till the trust anchor?	!
Is the certificate validation concluant ?	✔
Is the certificate validation concluant ?	✔
Is the certificate validation concluant ?	✔
Certificate :	PASSED
Is the certificate's signature intact?	✔
Are signature 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?	✔
The certificate has the id-pkix-ocsp-nocheck extension (RFC is skipped)	✔
Certificate :	PASSED
Is the certificate's signature intact?	✔
Are signature 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 (RFC) :	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?	✔
Are signature cryptographic constraints met?	✔

Certificate :

- Is the certificate's signature intact?
- Are signature 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 ?

PASSED

- ✔
- ✔
- ✔
- ✔
- ✔
- ✔

Revocation Freshness Checker (RFC) :

- Is the revocation data present for the certificate?

PASSED

- !

Basic Building Blocks

REVOCATION -

5ce1598524766f50aad1873964b8a661d755c94363f2833d140226666580afc731f9efbeb1a89b527c03cc5a3ccb946675aa34e9b51607250ce1c1f

Identification of the signing certificate (ISC) :

- Is there an identified candidate for the signing certificate?

PASSED

- ✔

Cryptographic Verification (CV) :

- Is the reference data object(s) found?
- Is the reference data object(s) intact?
- Is the signature intact?

PASSED

- ✔
- ✔
- ✔

Signature Acceptance Validation (SAV) :

- Are signature cryptographic constraints met?

PASSED

- ✔

X509 Certificate Validation (XCV) :

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

INDETERMINATE

- !
- ✘

Certificate :

- Is the certificate's signature intact?
- Are signature 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 ?

INDETERMINATE

- ✔
- ✔
- ✔
- ✔
- ✔
- ✘

Revocation Freshness Checker (RFC) :

- Is the revocation data present for the certificate?

INDETERMINATE

- ✘