






























Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive? 
Conclusion : **PASSED**

Qualification Signature 1524471517448

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? 
Are trust services consistent ? 
Is the certificate consistent with the trusted list ? 
Is the certificate qualified at signing time? 
Is the certificate for eSig at signing time? 
Is the certificate qualified at issuance time? 
Is the signature/seal created by a QSCD? 
Conclusion : **PASSED**

Basic Building Blocks
SIGNATURE - 1524471517448

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) : **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 unique ? 
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 certificate not revoked?	✔
Is the certificate on hold?	✔
Is the current time in the validity range of the signer's certificate?	✔
Is pseudo used ?	✔
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?	✔
Trust Anchor	PASSED

TL analysis 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

TL analysis EE

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