

<b>Validation Process for Basic Signatures</b> (Best signature time : 2023-11-27 19:17:24 (UTC))	<b>FAILED - SIG_CRYPTO_FAILURE</b>
Is the result of the 'Format Checking' building block conclusive?	✓
Is the result of the 'Identification of Signing Certificate' building block conclusive?	✓
Is the result of the 'Validation Context Initialization' building block conclusive?	✓
Is the result of the 'X.509 Certificate Validation' building block conclusive?	!
	The result of the 'X.509 Certificate Validation' building block is not conclusive!
Is the signing certificate not revoked at validation time?	✓
Is the validation time in the validity range of the signing certificate?	✓
Is the result of the 'Cryptographic Verification' building block conclusive?	✗
	The result of the 'Cryptographic Verification' building block is not conclusive!
<b>Validation Process for Signatures with Time and Signatures with Long-Term Validation Data</b> (Best signature time : 2023-11-27 19:17:24 (UTC))	<b>FAILED - SIG_CRYPTO_FAILURE</b>
Is the result of the Basic Validation Process acceptable?	✗
	The result of the Basic validation process is not acceptable to continue the process!
<b>Validation Process for Signatures with Archival Data</b> (Best signature time : 2023-11-27 19:17:24 (UTC))	<b>FAILED - SIG_CRYPTO_FAILURE</b>
Is the result of the LTV validation process acceptable?	✗
	The result of the LTV validation process is not acceptable to continue the process!
<b>Signature Qualification</b>	<b>N/A</b>
Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)?	!
	The signature/seal is not a valid AdES digital signature!
Has a trusted list been reached for the certificate chain?	✗
	Unable to build a certificate chain up to a trusted list!

**Basic Building Blocks****SIGNATURE - SIGNATURE\_GemBoxRSA4096\_20231127-1743**

<b>Format Checking :</b>	<b>PASSED</b>
Does the signature format correspond to an expected format?	✓
Is the signature identification not ambiguous?	✓
Is the signed references identification not ambiguous?	✓
Is only one SignerInfo present?	✓
Is the /ByteRange dictionary consistent?	✓
Does the /ByteRange not overlap with other signature/timestamp?	✓
Is the signature dictionary consistent?	✓
Do signed and final revisions contain equal amount of pages?	✓
Is no element overlapping detected in the PDF?	✓
Is there no visual difference between signed and final revisions in the PDF?	✓
Does the document contain none of the undefined object modifications?	✓
<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 - NO_CERTIFICATE_CHAIN_FOUND</b>
Can the certificate chain be built till a trust anchor?	✗
	The certificate chain for signature is not trusted, it does not contain a trust anchor.
<b>Cryptographic Verification :</b>	<b>FAILED - SIG_CRYPTO_FAILURE</b>
Has the reference data object been found? Reference : MESSAGE_DIGEST	✓
Is the reference data object intact? Reference : MESSAGE_DIGEST	✓
Is the signature intact?	✗
	The signature is not intact!
<b>Signature Acceptance Validation :</b>	<b>PASSED</b>
Is the structure of the signature valid?	✓
Is the signed attribute: 'signing-certificate' present?	!
	The signed attribute: 'signing-certificate' is absent!
Is the signed qualifying property: 'signing-time' present?	✓
Is the signed qualifying property: 'message-digest' or 'SignedProperties' present?	✓
Are cryptographic constraints met for the signature creation? Signature algorithm RSA with SHA512 with key size 4096 at validation time : 2023-11-27 19:17	✓
Are cryptographic constraints met for the message digest? Digest algorithm SHA512 at validation time : 2023-11-27 19:17 for message digest	✓