

# Validation report

## Document details

**Document name:** CITATIE - ICCJ.pdf

**Selected validation policy:** Only Qualified Electronic Signatures and Seals

Validation of Qualified Electronic Signatures and Seals that comply with the highest requirements and therefore have indisputable legal force according to the EU Regulation No 910/2014 (eIDAS).

## Signature #1

### Inalta Curte De Casatie Si Justitie

**Sealing time:** 2024-05-17 16:26:32 (GMT+3)  
**Qualified timestamp:** Not included  
**Seal format:** PKCS7-B  
**Certificate issuer:** certSIGN Qualified CA, CERTSIGN SA, RO  
 CERTSIGN SA, RO  
**Seal scope:** Full PDF  
 Full document



**Qualified Electronic Seal**

### Insufficient information to ascertain validity

**Seal indication:**  
INDETERMINATE

**Sub-indication:**  
CRYPTO\_CONSTRAINTS\_FAILURE\_NO\_POE

#### Validation Process for Basic Signatures

**Conclusion:** **INDETERMINATE**  
(CRYPTO\_CONSTRAINTS\_FAILURE\_NO\_POE)

Is the result of the Basic Validation Process conclusive?

NOT OK

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

**Conclusion:** **INDETERMINATE**  
(CRYPTO\_CONSTRAINTS\_FAILURE\_NO\_POE)

Is the result of the Basic Validation Process acceptable?

OK

Is the result of the revocation data validation process acceptable?

OK

Is the revocation data consistent?

OK

Is an acceptable revocation data present for the certificate?

OK

Are signature cryptographic constraints met?

NOT OK

#### Validation Process for Signatures with Archival Data

**Conclusion:** **INDETERMINATE**  
(CRYPTO\_CONSTRAINTS\_FAILURE\_NO\_POE)

Is the result of the LTV validation process acceptable?

OK

Is the past signature validation conclusive?

NOT OK

#### Signature Qualification: Indeterminate QESeal

**Conclusion:** **INDETERMINATE**

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

WARNING

Has a trusted list been reached for the certificate chain?

OK

Is the trusted list acceptable?

OK

Is the trusted list acceptable?

OK

Is the certificate qualified at (best) signing time?	OK
Is the certificate for eSig at (best) signing time?	WARNING
Is the certificate qualified at issuance time?	OK
Does the private key reside in a QSCD at (best) signing time?	OK

<b>REVOCACTION</b> R-7EB51B716539906C163FAD30667F9D15ACA1098C5451166003422564270AFED9	<b>Conclusion:</b>	<b>PASSED</b>
<b>Identification of the Signing Certificate</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is there an identified candidate for the signing certificate?		OK
<b>Certificate</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is the certificate signature intact?		OK
The certificate has the id-pkix-ocsp-nocheck extension (Revocation Check is skipped)		OK
Are certificate cryptographic constraints met?		OK
Is the current time in the validity range of the signer's certificate?		OK
<b>X509 Certificate Validation</b>	<b>Conclusion:</b>	<b>PASSED</b>
Can the certificate chain be built till a trust anchor?		OK
Is the certificate validation conclusive?		OK
Is the certificate validation conclusive?		OK
<b>Cryptographic Verification</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is revocation's signature intact?		OK
<b>Signature Acceptance Validation</b>	<b>Conclusion:</b>	<b>PASSED</b>
Are revocation cryptographic constraints met?		OK

<b>SIGNATURE</b> S-B7B6A5D2442E9F1A9EBCED1132E14355086EB1FA34D64D125E60C17E8EF1809B	<b>Conclusion:</b>	<b>INDETERMINATE</b> (CRYPTO_CONSTRAINTS_FAILURE_NO_POE)
<b>Identification of the Signing Certificate</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is there an identified candidate for the signing certificate?		OK
<b>Validation Context Initialization</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is the signature policy known?		OK
<b>Certificate</b>	<b>Conclusion:</b>	<b>PASSED</b>
Is the certificate unique?		OK
Is a pseudonym used?		OK
Is certificate not self-signed?		OK
Certificate meta-data constraints: Is the signer's certificate qualified?		OK
Certificate meta-data constraints: Is it supported by a QSCD?		OK

Is the certificate signature intact?	OK
Does the signer's certificate have an expected key-usage?	OK
Is the authority info access present?	OK
Is the revocation info access present?	OK
Is the revocation data present for the certificate?	OK
Is the revocation acceptance check conclusive?	OK
Is there a satisfying revocation status information?	OK
Is the revocation freshness check conclusive?	OK
Is the certificate not revoked?	OK
Is the certificate on hold?	OK
Are certificate cryptographic constraints met?	OK
Is the current time in the validity range of the signer's certificate?	OK
<b>X509 Certificate Validation</b>	<b>Conclusion: PASSED</b>
Can the certificate chain be built till a trust anchor?	OK
Has a trust service with an expected status been found?	OK
Is the certificate validation conclusive?	OK
Is the certificate validation conclusive?	OK
<b>Format Checking</b>	<b>Conclusion: PASSED</b>
Does the signature format correspond to an expected format?	OK
Is there any elements that might change visual content dynamically?	OK
<b>Cryptographic Verification</b>	<b>Conclusion: PASSED</b>
Has the reference data object been found?	OK
Is the reference data object intact?	OK
Is the signature intact?	OK
<b>Signature Acceptance Validation</b>	<b>Conclusion: INDETERMINATE (CRYPTO_CONSTRAINTS_FAILURE_NO_POE)</b>
Is the signed qualifying property: 'signing-time' present?	OK
Is the signed qualifying property: 'message-digest' or 'SignedProperties' present?	OK
Are signature cryptographic constraints met?	NOT OK
<b>List Of Trusted Lists</b>	<b>Conclusion: PASSED</b>
Is the trusted list fresh?	OK
Is the trusted list not expired?	OK
Does the trusted list have the expected version?	OK
Is the trusted list well signed?	OK
<b>Trusted List</b>	<b>Conclusion: PASSED</b>
Is the trusted list fresh?	OK
Is the trusted list not expired?	OK
Does the trusted list have the expected version?	OK
Is the trusted list well signed?	OK

---

This validation report is prepared by a Qualified Trust Service Provider Dokobit, UAB, in accordance with [Dokobit Qualified Signature Validation Service Practice Statement and Policy](#) with an OID 1.3.6.1.4.1.54720.1.1 using selected signature validation policy with an OID 1.3.6.1.4.1.54720.1.2

**Validation liability:** Document has been validated using the Advanced liability level. Dokobit assumes the liability for up to 10 000 Eur for this validation report.

**Validation time:** 2024-05-17 16:26:32 (GMT+3)

**Validation report ID:** cbf26f0bf0fcf3d455afe0c56cbafa58e22e378c

**Validated document hash:** 7640071b9418d48481928d6d9b3aa1eb036cb4927e9ede744cfb9b7dbdce7919

This validation report is only correct at the actual validation time.

