Signature SIGNATURE_ionut-corbu-mta-ro_20240408-1849 — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

Validation Process for Basic Signatures (Best-signature-time : 2024-04-09 14:37:10 (UTC)) — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- 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? ✓
- Is the result of the Basic Validation Process conclusive? ✗
  Basic Signature Validation process failed with INDETERMINATE/NO_CERTIFICATE_CHAIN_FOUND indication
  The result of the Basic validation process is not conclusive!

Timestamp TIMESTAMP_www-freetsa-org_20240408-1849 — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

Validation Process for Basic Time-stamps (Production time : 2024-04-08 18:49:27 (UTC)) — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- Is the result of the 'Identification of Signing Certificate' 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? ✓
- Is the result of the Basic Validation Process conclusive? ✗
  Basic Signature Validation process failed with INDETERMINATE/NO_CERTIFICATE_CHAIN_FOUND indication
  The result of the Basic validation process is not conclusive!

Validation Process for Time-stamps with Archival Data (Lowest POE : 2024-04-09 14:37:10 (UTC)) — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- Is the result of the Time-stamp Validation Building Block acceptable? ✗
  The result of the Time-stamp Validation Building Block is not acceptable to continue the process!

Time-stamp Qualification — N/A

- Has a trusted list been reached for the certificate chain? ✗
  Unable to build a certificate chain up to a trusted list!

Validation Process for Signatures with Time and Signatures with Long-Term Validation Data (Best-signature-time : 2024-04-09 14:37:10 (UTC)) — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- Is the result of the Basic Validation Process acceptable? ✗
  The result of the Basic validation process is not acceptable to continue the process!

Validation Process for Signatures with Archival Data (Best-signature-time : 2024-04-09 14:37:10 (UTC)) — INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

- Is the result of the LTV validation process acceptable? ✗
  The result of the LTV validation process is not acceptable to continue the process!

Signature Qualification — N/A

- Is the signature/seal an acceptable AdES digital signature (ETSI EN 319 102-1)? !
  The signature/seal is an INDETERMINATE 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_ionut-corbu-mta-ro_20240408-1849

Format Checking : PASSED

- 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? ✓

Identification of the Signing Certificate : PASSED

- Is there an identified candidate for the signing certificate? ✓
- Is the signed attribute: 'cert-digest' of the certificate present? ✓
- Does the certificate digest value match a digest value found in the certificate reference(s)? ✓

Are the issuer distinguished name and the serial number equal?

Validation Context Initialization : PASSED

Is the signature policy known?

X509 Certificate Validation : INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

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.

Cryptographic Verification : PASSED

Has the reference data object been found?
Reference : MESSAGE_DIGEST

Is the reference data object intact?
Reference : MESSAGE_DIGEST

Is the signature intact?

Signature Acceptance Validation : PASSED

Is the structure of the signature valid?

Is the signed attribute: 'signing-certificate' present?

Is the signed attribute: 'signing-certificate' present only once?

Does the 'Signing Certificate' attribute contain references only to the certificate chain?

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 SHA256 with key size 2048 at validation time : 2024-04-09 14:37

Are cryptographic constraints met for the message digest?
Digest algorithm SHA256 at validation time : 2024-04-09 14:37 for message digest

Are cryptographic constraints met for the signing-certificate reference?
Digest algorithm SHA256 at validation time : 2024-04-09 14:37 for signing-certificate reference with Id : CERTIFICATE_ionut-corbu-mta-ro_20240408-1759

Basic Building Blocks
TIMESTAMP - TIMESTAMP_www-freetsa-org_20240408-1849

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

Is the signed attribute: 'cert-digest' of the certificate present?

X509 Certificate Validation : INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

Can the certificate chain be built till a trust anchor?

The certificate chain for time-stamp is not trusted, it does not contain a trust anchor.

Cryptographic Verification : PASSED

Has the message imprint data been found?

Is the message imprint data intact?

Is time-stamp's signature intact?

Signature Acceptance Validation : PASSED

Is the signed attribute: 'signing-certificate' present?

Does the 'Signing Certificate' attribute contain references only to the certificate chain?

Does the TST Info field: 'tsa' match the time-stamp's issuer name?

Are cryptographic constraints met for the time-stamp signature?
Signature algorithm RSA with SHA512 with key size 4096 at validation time : 2024-04-09 14:37

Are cryptographic constraints met for the time-stamp message imprint?
Digest algorithm SHA256 at validation time : 2024-04-09 14:37 for time-stamp message imprint

Basic Building Blocks
REVOCATION - OCSP_www-freetsa-org_20240408-1849

Identification of the Signing Certificate : PASSED

Is there an identified candidate for the signing certificate?

X509 Certificate Validation : INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND

Can the certificate chain be built till a trust anchor?

The certificate chain for revocation data is not trusted, it does not contain a trust anchor.

Cryptographic Verification : PASSED

Is revocation's signature intact?

Signature Acceptance Validation : PASSED

Are cryptographic constraints met for the revocation data signature?
Signature algorithm RSA with SHA256 with key size 2048 at validation time : 2024-04-09 14:37