ECB-PUBLIC

€STR

EURO-SHORT-TERM-RATE

Signature validation

# Release digital signature verification

The ECB system that calculates the €STR rate digitally signs each EURO-SHORT-TERM-RATE publication release using the following procedure:

Only the body XML sections of the release message under the element *<CALCULATION\_RESULTS>* is used for generating the signature. The corresponding value of this signature will appear under the element *<SIGNATURE\_VALUE>.*

The publication message is signed using Entrust Certificate and an implicit signature is generated containing the signature and the signing certificate, detached from the data. This is base 64 encoded representation [PEM format] of the signed object as specified in CMS standard.

To make sure of the quality of the data use for the verification, accessing to the XML via internet browser can modify certain characters and/or break lines of the document in order to provide a better visualization. Using the data provide by the browser format will cause a validation failure. Please save the XML file in your computer and open it with a text editor.

To verify the validity of the digital signature the next procedure can be followed:[[1]](#footnote-1)

1. Place the content under the element *<CALCULATION\_RESULTS>* including the *<CALCULATION\_RESULTS>* tag of the publication to validate in a separate file[[2]](#footnote-2) and save it e.g. *unsigned\_body.txt* with the next content:

**<CALCULATION\_RESULTS>**

**<REF\_DATE>**2019-08-05**</REF\_DATE>**

**<PUB\_DATE>**2019-08-06**</PUB\_DATE>**

**<RATE>**-0.457**</RATE>**

**<INITIAL\_VOLUME>**65246**</INITIAL\_VOLUME>**

**<NUMBER\_BANKS>**41**</NUMBER\_BANKS>**

**<NUMBER\_TRNX>**926**</NUMBER\_TRNX>**

**<SH\_VOL\_TOP\_BANKS>**60**</SH\_VOL\_TOP\_BANKS>**

**<PUB\_MODE>**Normal**</PUB\_MODE>**

**<VOL\_DIST\_25>**-0.49**</VOL\_DIST\_25>**

**<VOL\_DIST\_75>**-0.42**</VOL\_DIST\_75>**

**<PUB\_TYPE>**Standard**</PUB\_TYPE>**

**</CALCULATION\_RESULTS>**

1. Place the content under the element *<SIGNATURE\_VALUE>* including the *-----BEGIN CMS----* and *-----END CMS-----* delimiters of the publication to validate in a separate file[[3]](#footnote-3) and save it e.g. signed\_body.pem with the next content:

**-----BEGIN CMS-----**

Signed content

**-----END CMS-----**

1. Place the Entrust certificate used for the validation including the *-----BEGIN CCERTIFICATE ----* and *-----END CERTIFICATE-----* delimiters of the publication to validate in a separate file and save it e.g. certificate.pem[[4]](#footnote-4) with the next content:

**-----BEGIN CERTIFICATE-----**

Signed content

**-----END CERTIFICATE-----**

1. Run the next OpenSSL command:

openssl cms -verify -noverify -content *unsigned\_body.txt* -in *signed\_body.pem* -signed -nointern -certfile certificate.pem -inform pem

1. If the unsigned content is shown with the message “*Verification successful*” the content has been successfully verified.

# Certificates and dates

Periodically it is needed to renew the certificates used for the publication of the euro-short-term-rate.

In the following table you will be able to find the corresponding certificate for each publication message:

|  |  |  |  |
| --- | --- | --- | --- |
| **Certificate Serial Number** | **Location** | **Valid from** | **Valid until** |
| 63b744c6549e6f6fe8402357a326862e | /data sets/euro-short-term-rate/certificates/01\_signature.euro-short-term-rate.ecb.europa.eu.crt | 07/11/2023 | 28/10/2024 |
| 00c62b4b9fd7295b83d3f8903f1fc00395 | /data sets/euro-short-term-rate/certificates/02\_signature.euro-short-term-rate.ecb.europa.eu.crt | 29/10/2024 | 07/11/2025 |

# Troubleshooting

Verification failure.

Trace:

52964:error:2E09A09E:CMS routines:CMS\_SignerInfo\_verify\_content:verification

failure:cms\_sd.c:853:

52964:error:2E09D06D:CMS routines:CMS\_verify:content verify error:cms\_smime.c:393:

Solution: Check in the unsigned\_body.txt file end-of-line character and make sure there is not whitespaces or break line at the end.

## Error reading S/MIME message

Trace:

74672:error:0D07207B:asn1 encoding routines:ASN1\_get\_object:header too long:asn1\_lib.c:157:

74672:error:0D068066:asn1 encoding routines:ASN1\_CHECK\_TLEN:bad object header:tasn\_dec.c:1187:

74672:error:0D07803A:asn1 encoding routines:ASN1\_ITEM\_EX\_D2I:nested asn1 error:tasn\_dec.c:374:Type=CMS\_ContentInfo

74672:error:0906700D:PEM routines:PEM\_ASN1\_read\_bio:ASN1 lib:pem\_oth.c:83:

Solution: the signed\_body,pem file is not correct. There is missing data or the encoding it is incorrect.

## Unable to load certificates

Trace:

62564:error:0D0680A8:asn1 encoding routines:ASN1\_CHECK\_TLEN:wrong tag:tasn\_dec.c:1199:

62564:error:0D07803A:asn1 encoding routines:ASN1\_ITEM\_EX\_D2I:nested asn1 error:tasn\_dec.c:374:Type=X509

62564:error:0907400D:PEM routines:PEM\_X509\_INFO\_read\_bio:ASN1 lib:pem\_info.c:249:

Solution: The certificate is wrong, there is not a format error. Find the right certificate.

## Unable to load certificates

Trace: -

Solution: The format of the certificate is wrong. Adjust the end-of-line characters and line breaks.

## Error reading S/MIME message

Trace: -

Solution: The format of the signed\_body.pem file is not correct. Adjust the end-of-line characters and line breaks.

1. Example performed using Openssl 1.0.2k [↑](#footnote-ref-1)
2. The files should be in UNIX format with using LF as end of line. [↑](#footnote-ref-2)
3. The files should be in UNIX format with using LF as end of line. [↑](#footnote-ref-3)
4. The certificate used for the signature example can be found in the folder /data sets/euro-short-term-rate/certificates/01\_signature.euro-short-term-rate.ecb.europa.eu.crt and should match with the one appended in the signature message. [↑](#footnote-ref-4)