|  |  |
| --- | --- |
| Logo of the European Commission, 12 yellow stars on a blue background arranged in a circle and framed by two light grey graphic elements representing the Berlaymont building, which is the headquarter of the European Commission. | EUROPEAN COMMISSION  DIRECTORATE-GENERAL FOR INFORMATICS  Directorate D – Digital Services  **DIGIT.D.3 – Trans-European Services** |

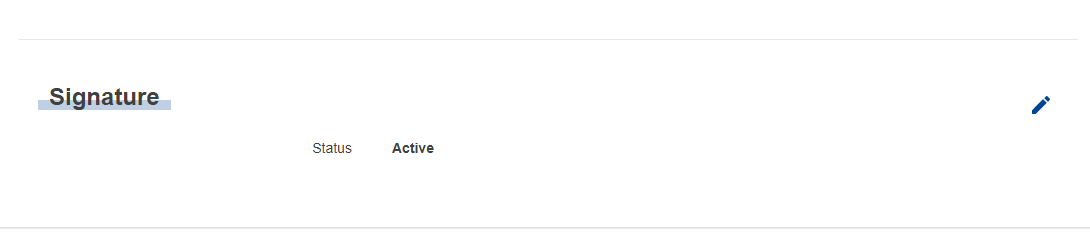
eTrustex Web digital signing.

# Digital signatures in eTrustex Web

eTrustex Web allows to digitally sign the transmitted messages.

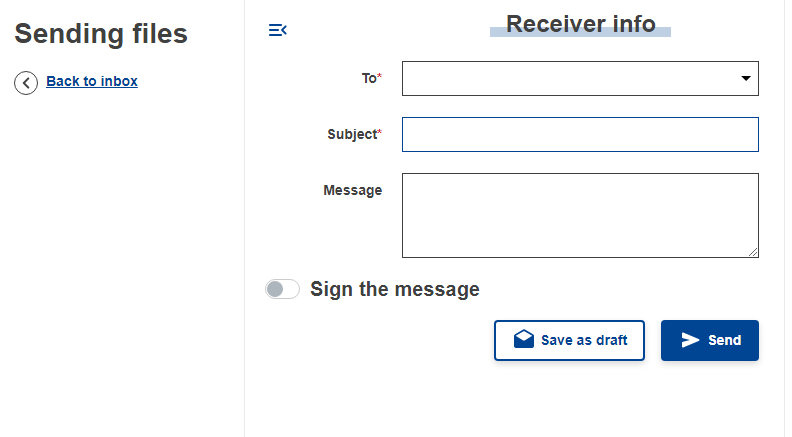
This feature needs to be enabled from the administration section for the Business Domain before being used.

Figure : : the business configuration with enabled signature.



If the feature is enabled, users composing new messages are provided with the option of including a digital signature.

Figure : the option to sing the message.



In order to do so, a certificate needs be provided to retrieve the key pair needed for signing.

Figure : input a certificate in order to sign.



# Applied standards

The standard applied for digitally sing the messages is the JSON Web Signature (JWS). In particular we use the Detached Content, as described in the Appendix-F of (Jones, Bradley, & Sakimura, JSON Web Signature (JWS), 2015). We also use the JSON serialization in favour of the compact one to improve readability.

We use PS512 (RSASSA-PSS with SHA-512) as the signing algorithm. This is one of the implementations listed as optional for JWS headers. See (Jones, JSON Web Algorithms (JWA), 2015).

# Information being signed

The information included in the signed JSON object are the following:

* The subject of the message.
* The content of the message body.
* The confidentiality (PUBLIC for messages sent in clear text, LIMITED-HIGH when using end-to-end encryption) and integrity (for now always set to MODERATE) of the message.
* The information about the AES key used for end-to-end-encryption
* The total number and collective size of the attachments
* The template variables
* For each attachment:
  + Its id
  + The original file name and relative path
  + The content type
  + The initialization vector used for end-to-end encryption
  + The byte length (of the clear text file if end-to-end encryption is not used, of the encrypted file otherwise, notice these sizes are slightly different due to padding)
  + The file checksum (of the clear text file if end-to-end encryption is not used, of the encrypted file otherwise)

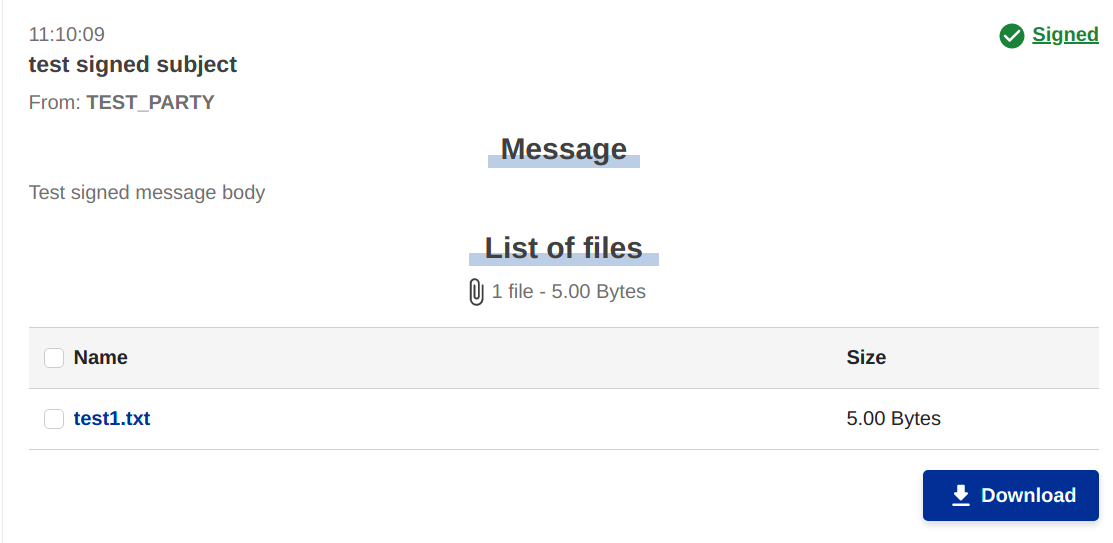
Notice that all files are uploaded with end-to-end encryption, but the AES key used for encryption is either encrypted using the public key of the recipient (when end-to-end encryption is required) or sent in clear text.

# Signature verification

Each time a user opens the details of a received message, if the message is digitally signed, the client application performs a signature validation.

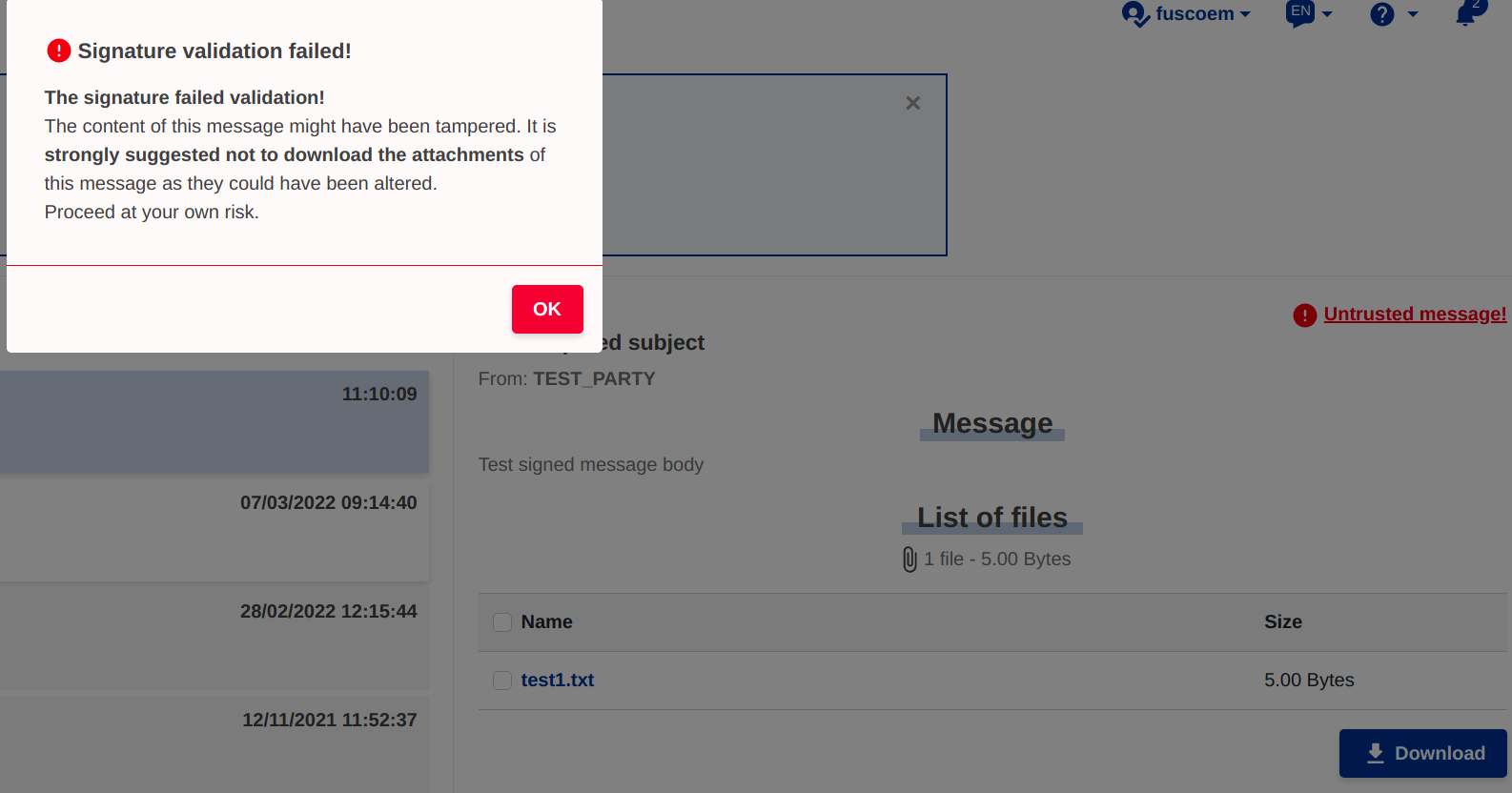
If the signature passes validation, a green ``Signed’’ link is displayed on the top-right corner of the message details.

Figure : a signed message that passes signature validation.



In case of failed validation, a popup is displayed to the user to warn her the data in the message might have been tampered, and a red ``Untrusted message!’’ link is displayed on the top right corner of the message details.

Figure : a signature fails validation.



Source: Type your source here.

The ``signed’’ or ``Untrusted message!’’ links allow the user to download the signed JSON data, which can be used to verify the certificate used for signing and perform signature validation with any compatible external tool.

At the moment, we do not verify that the certificate used for signing is trusted.

# Bibliography

Jones, M. (2015). *JSON Web Algorithms (JWA).* Internet Engineering Task Force (IETF). Retrieved from https://datatracker.ietf.org/doc/html/rfc7518

Jones, M., Bradley, J., & Sakimura, N. (2015). *JSON Web Signature (JWS).* Internet Engineering Task Force (IETF). Retrieved from https://datatracker.ietf.org/doc/html/rfc7515