27 January 2003 Article · Digital Identity · Privacy & Crypto

SMIME Mail Container

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/smime-mail-container-en/

With this simple Java Tool users can sign and/or encrypt arbitrary content. The signed and/or encrypted content is packaged in a S/MIME container and stored as *.EML file. *.EML files can be opened with Netscape or Outlook Express and enable for verification of their signature and/or encryption certificates.

Details

Before you can create signed and/or encrypted S/MIME container, you have to load the corresponding signature and encryption certificates. As signature certificates the tool accepts PKCS#12 files with the file extensions *.PFD or *.P12. As encryption certificates it accepts PKCS#7 certificates with the file extensions *.P7C, *.P7B or DER encoded certificates with *.DER or *.CER extension.

Important!

Currently no validation regarding validity, revocation status or key usage is performed.

If you choose the options „Detached Signature“ and „Sign Mail“, the tool will create a S/MIME message of type „multipart/signed“. The message consists of the following two parts: the first part provides the content of the message and the second part includes the cryptographic signature.

However if the option „Detached Signature“ is not selected, the content of the message will be included in the signature and the S/MIME messages only consists of one part (type „application/pkcs7-mime“). Detached signatures provide the advantage, that the message content can also be read by mail clients which do not offer S/MIME functionality. Therefor „multipart/signed“ („Detached Signature“) is set as default value.

If the option „Encrypt Mail“ has been selected, then the chosen signature type does not matter, as the message with the signature is included in an encrypted packet. The receiver has to open the encrypted packet, thus the mail client has to support S/MIME anyway.

The fields „Subject“ and „Content“ can be filled manually. By choosing „Automatic Fill“ the fields are set according to the chosen signature and/or encryption options to provide information regarding the cryptographic properties of the S/MIME message (see figure below). In addition users can provide a file, that will be added as attachment (field „Attachment“).

By hitting „Create/Store“ the just created message will be stored as *.EML file and can be opend by most mail clients. In addition the signature of the message can be verified:

This tool is no longer provided for download.