

The Data Security Company.

---

## SafeGuard<sup>®</sup> MailGateway

Controlling the subject field

Gateway Version 5.60

## Introduction

Your organization (company, government body, etc.) uses SafeGuard MailGateway (SGMG) from Utimaco Safeware AG to protect your e-mails.

Outgoing e-mails are automatically encrypted and signed by SGMG. Incoming e-mails are automatically decrypted and their signature is verified.

Your SGMG Administrator defines the rules used to protect your e-mails.

This set of rules is controlled in such a way as to ensure that the majority of your e-mails are processed in the most suitable manner. Despite this it may sometimes be necessary to override the SGMG settings for individual e-mails.

To do this, your SGMG uses Subject line control. This can be configured by a command from your e-mail client.

Status messages will appear in the Subject field to tell you about the progress of the incoming e-mail that is being processed.

This document explains the meaning of the status messages in the Subject field and describes the commands that you can use from your e-mail client to configure how individual e-mails are processed.

You can enter a command in the Subject field to specify whether the public part of your S/MIME certificate and/or your OpenPGP key is to be attached to the outgoing e-mail.

Your SGMG Administrator must give you specific permission for Subject line control. Your SGMG Administrator can change the name of the status messages and commands at any time and define the position of the command (at the start or the end or anywhere) of the Subject line.

SGMG automatically deletes the commands you enter in the Subject field so that they are not sent to your communications partner.

Status messages are displayed in round brackets ( ) at the start or the end of the actual Subject line.

By default, commands are displayed in curly brackets { } at the start, at the end or anywhere in the actual Subject line.

The key combination for curly brackets is Alt Gr + 7 or 0.

## Status messages in the Subject line

Status messages:	Meaning:
(Plain)	This e-mail was not encrypted and not signed (plain (unencrypted) text)
(S/MIME: unsigned and encrypted)	This e-mail was encrypted with S/MIME but not signed.
(S/MIME: signed)	This e-mail was signed with S/MIME, but not encrypted.
(S/MIME: signed and encrypted)	This e-mail was signed with S/MIME, and encrypted.
(WARNING!!! S/MIME with incorrect signature)	This e-mail was signed with S/MIME. The signature is invalid.
(WARNING!!! Encrypted S/MIME with incorrect signature)	This e-mail was encrypted and signed with S/MIME. The signature is invalid.
(S/MIME: cannot decrypt)	This e-mail cannot be decrypted with S/MIME.
(PGP: unsigned and encrypted)	This e-mail was encrypted with OpenPGP but not signed.
(PGP signed)	This e-mail was signed with OpenPGP.
(PGP signed and encrypted)	This e-mail was signed and encrypted with S/MIME.
(WARNING!!! PGP with incorrect signature)	This e-mail was signed with OpenPGP. The signature is invalid.
(WARNING!!! Encrypted PGP with incorrect signature)	This e-mail was encrypted and signed with OpenPGP. The signature is invalid.
(PGP cannot decrypt)	This e-mail cannot be decrypted with OpenPGP.
(Sent by SafeGuard WebMail)	This e-mail was sent by SafeGuard WebMail.
(Secure reply)	This e-mail was sent by SafeGuard PDFMail.
(PrivateCrypto: encrypted)	This e-mail was encrypted with SafeGuard PrivateCrypto.
(PrivateCrypto: Cannot decrypt)	This e-mail cannot be decrypted with SafeGuard PrivateCrypto.
(Mixed security state)	This e-mail was partially signed and/or partially encrypted.

## The commands

You can enter several commands, each separated by a blank space.



*{sign crypt}*

Command:	Meaning:
{plain} or {clear}	The e-mail will be send in plain (unencrypted) text.
{sign}	The e-mail will be signed with S/MIME or OpenPGP. The method your communications partner uses is used for the signature.
{crypt_fb_pc}	The e-mail will be encrypted (S/MIME, OpenPGP, SafeGuard PrivateCrypto). The method your communications partner uses is used for encryption. If the recipient neither have a S/MIME certificate nor an OpenPGP key, the e-mail is encrypted with SafeGuard PrivateCrypto.
{crypt_fb_web}	The e-mail will be encrypted (S/MIME, OpenPGP, SafeGuard WebMail). The method your communications partner uses is used for encryption. If the recipient does neither have a S/MIME certificate nor an OpenPGP key, the e-mail is encrypted with SafeGuard WebMail.
{crypt_fb_pdf}	The e-mail will be encrypted (S/MIME, OpenPGP, SafeGuard PDFMail). The method your communications partner uses is used for encryption. If the recipient does neither have a S/MIME certificate nor an OpenPGP key, the e-mail is encrypted with SafeGuard PDFMail
{crypt} or {crypt_fb_err}	The e-mail will be encrypted (S/MIME, OpenPGP). SafeGuard PrivateCrypto and SafeGuard WebMail is explicitly excluded. The method your communications partner uses is used for encryption. If the recipient does neither have a S/MIME certificate nor an OpenPGP key, the data is not encrypted and your e-mail is returned.
{trust_fb_pc}	The e-mail will be encrypted and signed (S/MIME, OpenPGP, SafeGuard PrivateCrypto). The method your communications partner uses is used for encryption. If the recipient does neither have a S/MIME certificate nor an OpenPGP key, the e-mail is encrypted with SafeGuard PrivateCrypto. S/MIME or OpenPGP is used for the signature.

{trust or {trust_fb_err}}	The e-mail will be encrypted and signed (S/MIME, OpenPGP) SafeGuard PrivateCrypto and SafeGuard WebMail is explicitly excluded for encryption. The method your communications partner uses is used for encryption. If the recipient does neither have a S/MIME certificate nor an OpenPGP key, the data is not encrypted and your e-mail is returned.
{sign_smime}	The e-mail will be signed with S/MIME.
{crypt_smime}	The e-mail will be encrypted with S/MIME. If the recipient does not have an S/MIME certificate the e-mail is returned to you.
{trust_smime}	The e-mail will be encrypted and signed with S/MIME.
{sign_pgp}	The e-mail will be signed with OpenPGP.
{crypt_pgp}	The e-mail will be encrypted with OpenPGP. If the recipient does not have an OpenPGP key the e-mail is returned to you.
{trust_pgp}	The e-mail will be encrypted and signed with OpenPGP. If the e-mail recipient does not have an OpenPGP key the e-mail is returned to you.
{crypt_web}	The e-mail will be encrypted with SafeGuard WebMail.
{crypt_pc} or {private}	<p>The e-mail will be encrypted with SafeGuard PrivateCrypto. If you enter several commands, the {crypt_pc}, or {private} command must always be the final entry. After this, if no fixed password has been assigned, you can enter the SafeGuard PrivateCrypto password. SGMG interprets everything that comes after the {crypt_pc} or {private} command as the SafeGuard PrivateCrypto password.</p> <p>If you do not enter a password in the Subject line for encryption with SafeGuard PrivateCrypto, a password is generated automatically. As the sender of the e-mail, SGMG will inform you by e-mail about the generated password.</p> <p>If you enter a password here, it must not contain a blank space, must include at least 4 characters and be a maximum of 32 characters.</p>



*{sign private flower}*

<p>{crypt_pdf}</p>	<p>The e-mail will be encrypted with SafeGuard PDFMail</p> <p>If you enter several commands, the {crypt_pdf}, command must always be the final entry. After this, if no fixed password has been assigned, you can enter the SafeGuard PDFMail password. SGMG interprets everything that comes after the {crypt_pdf} or command as the SafeGuard PDFMail password.</p> <p>If you do not enter a password in the Subject line for encryption with SafeGuard PDFMail, a password is generated automatically. As the sender of the e-mail, SGMG will inform you by e-mail about the generated password.</p> <p>If you enter a password here, it must not contain a blank space, must include at least 4 characters and be a maximum of 32 characters.</p>
--------------------	---



{sign crypt\_pdf flower}

<p>{send_key} or {add_key}</p>	<p>The public part of your S/MIME certificate and/or the OpenPGP key is added to your e-mail as an attachment so that it is available to your communications partner. <sup>2, 3</sup></p>
<p>{send_key_smime} or {add_key_smime}</p>	<p>The public part of your S/MIME certificate is added to your e-mail as an attachment so that it is available to your communications partner. <sup>2</sup></p>
<p>{send_key_pgp} or {add_key_pgp}</p>	<p>The public part of your OpenPGP key is added to your e-mail as an attachment so that it is available to your communications partner. <sup>3</sup></p>

<sup>2</sup> In the case of S/MIME the corresponding issuing certificate (or CA or sub-CA) is attached along with the user certificate

<sup>3</sup> In the case of OpenPGP, the e-mail postmaster key that signed the OpenPGP users key is also attached.