1 Introduction

The main aim of this document is to give a brief introduction on how to configure the MaBiS extension of ComCT for sending signed and encrypted e-mails.

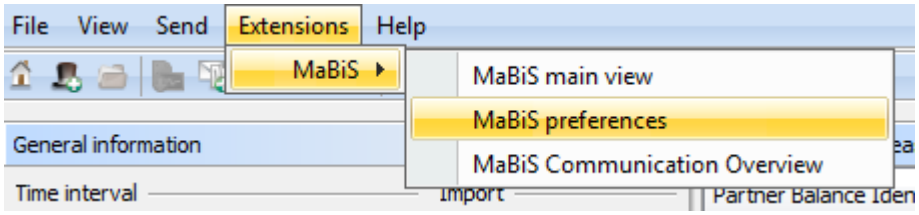
The main workflow of the configuration can be separated into two steps:

1. Import the key files into the key management
2. Assign the imported keys to the BiKos

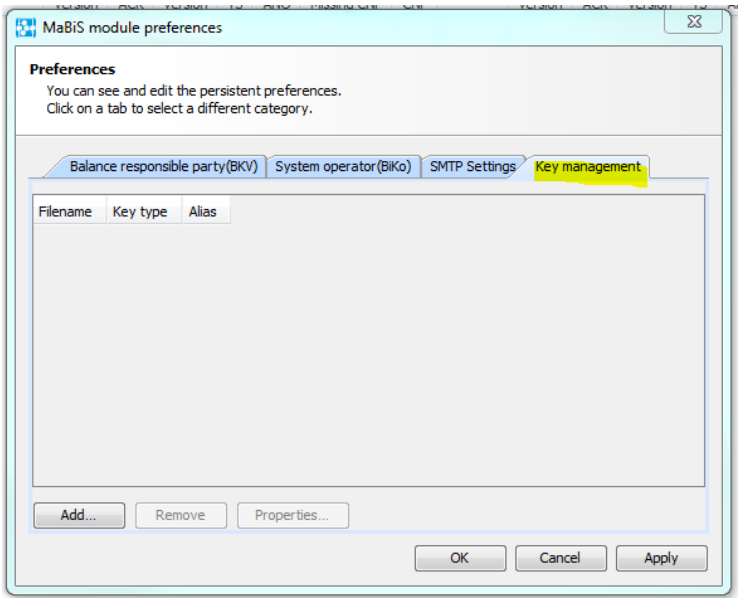
2 How-to

2.1 Import the key files into the key management

Open the *MaBiS preferences* view.



Go to the tab: *Key management*

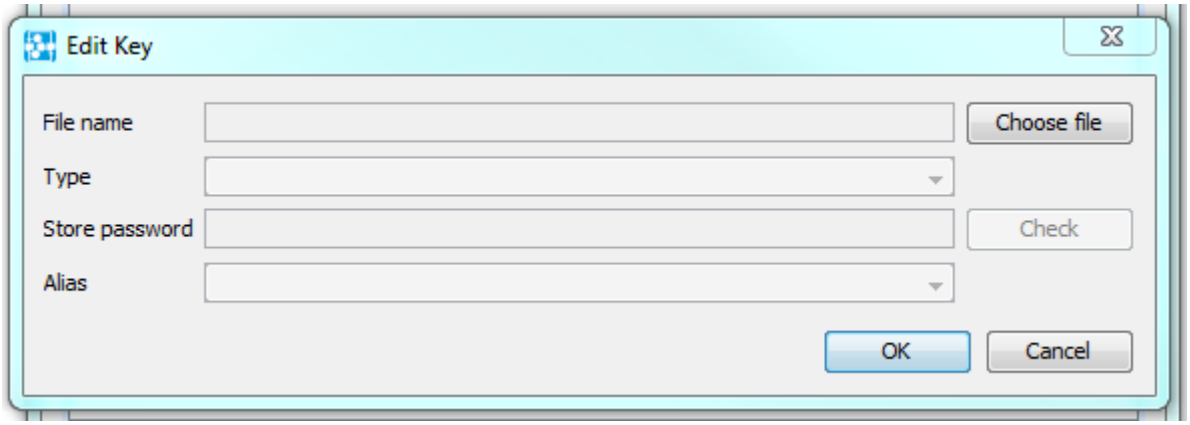


2.1.1 Importing the private key for signing the mail

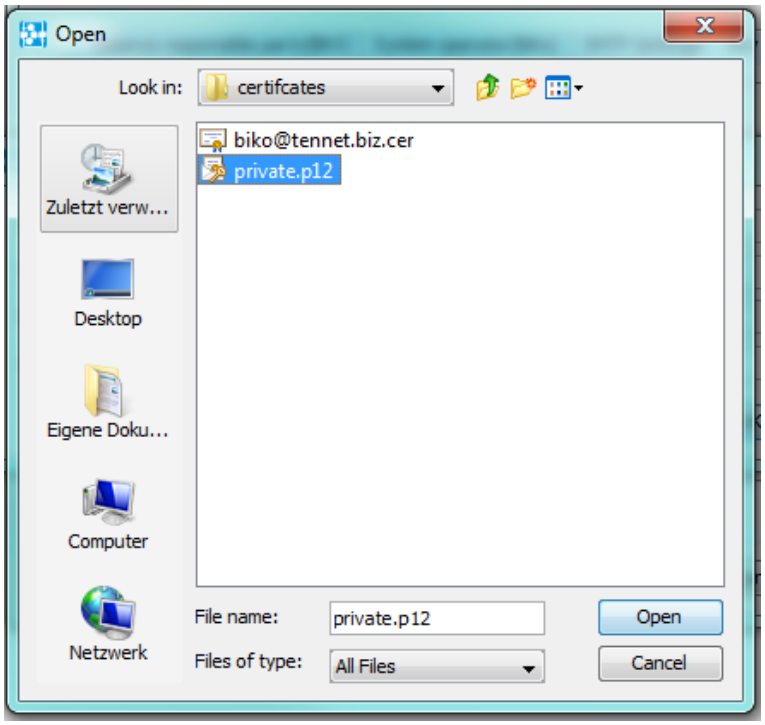
Now you need to import your (own) certificate for signing your mails. This is a PKCS #12 file with the file ending .p12 or .pfx.

For this click on *Add…*

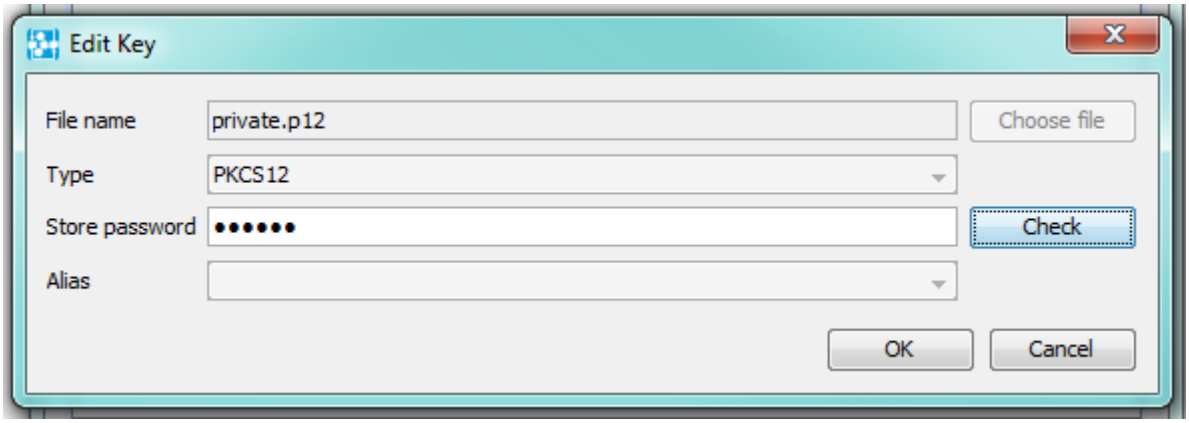
A new dialog will appear.



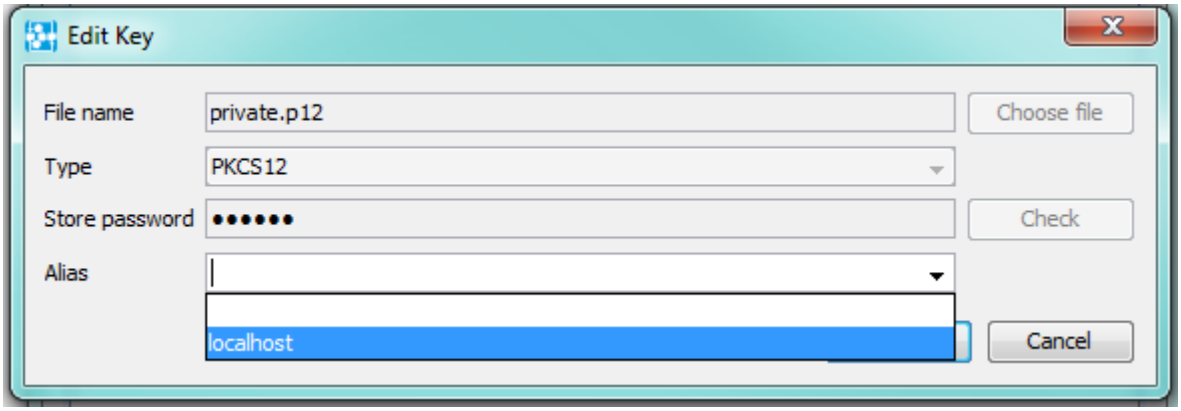
Click on *Choose file*. Select your private key certificate file (.p12 / .pfx) and click *Open*.



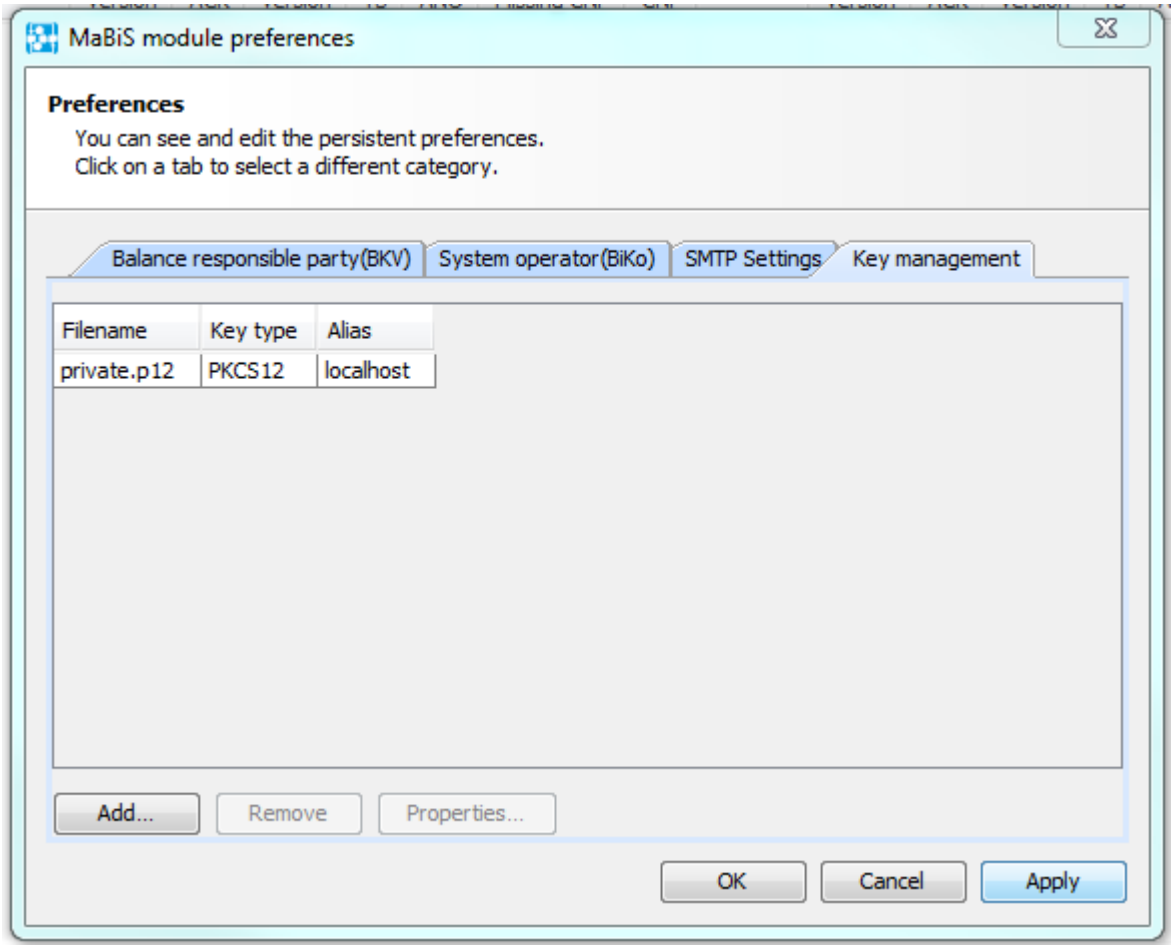
Enter the password and click on *Check*.



Select the alias and click on *OK*. The common case is, that the PKCS #12 file contains only one alias.



The file is visible in the table now. Click on *Apply* to persist the key.

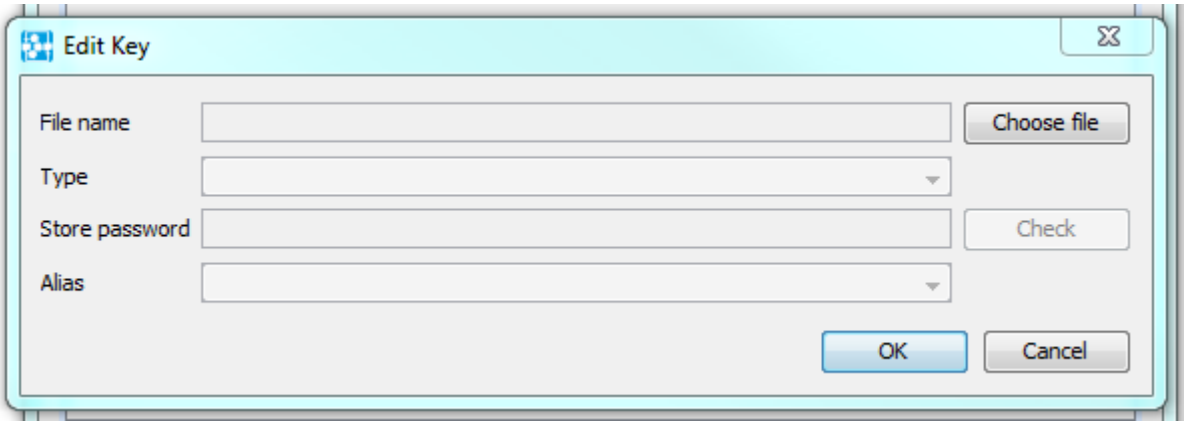


2.1.2 Importing the public key for encrypting the mail

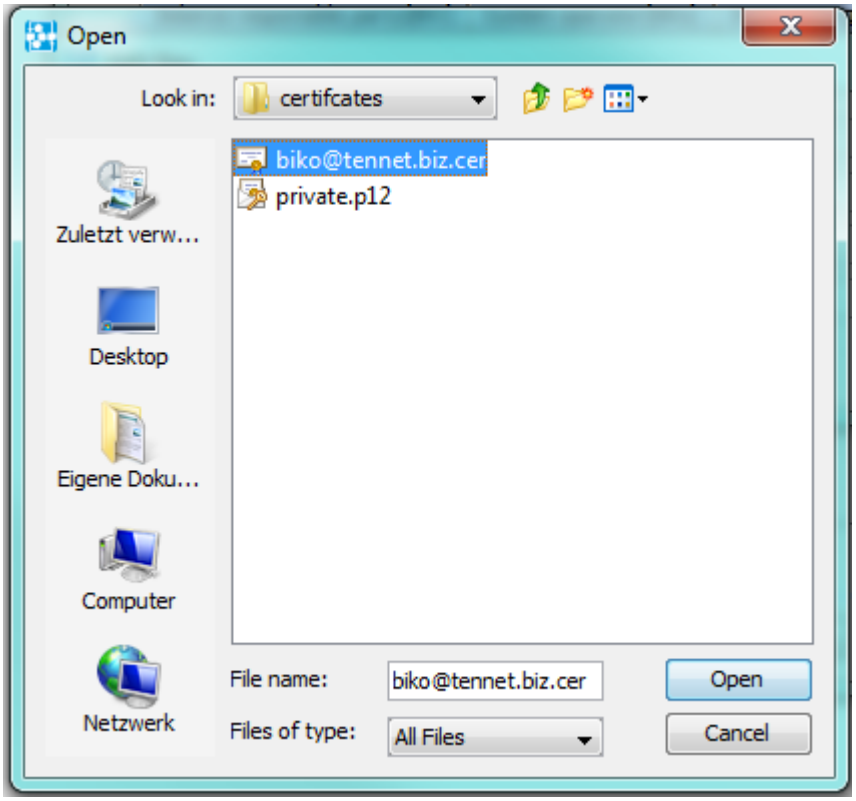
Now you need to import the certificate for encrypting your mail for the BiKo. This is a X.509 file with the file ending .cer or .crt. It can also be a PKCS #7 file. The example considers the X.509 variant.

For this click on *Add…*

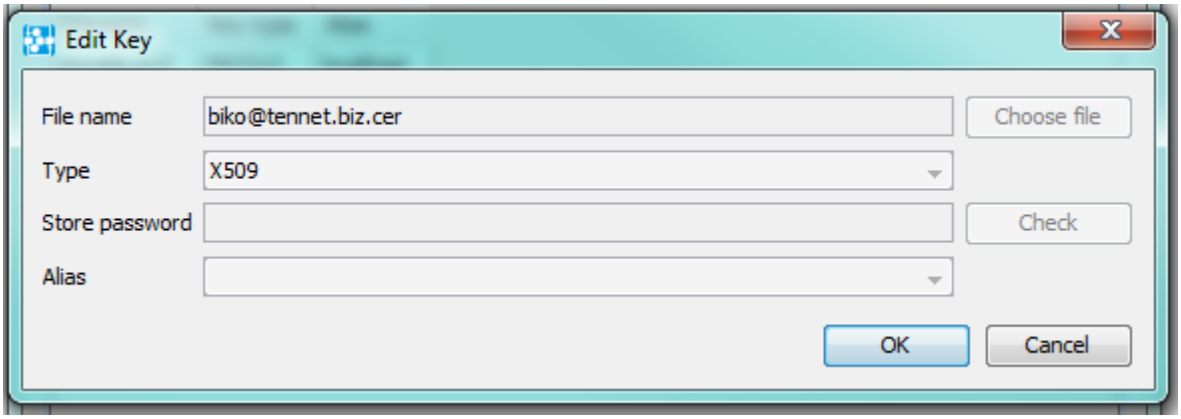
A new dialog will appear.



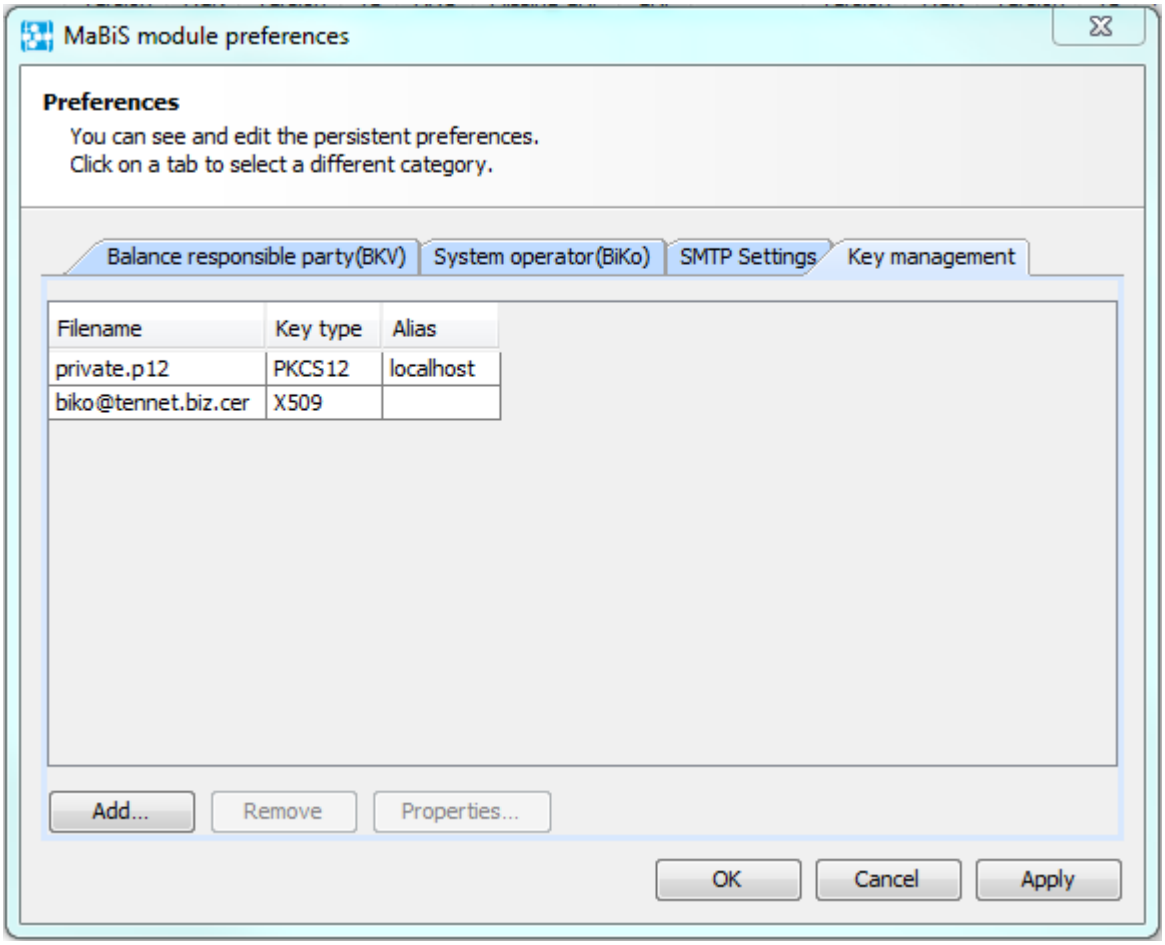
Click on *Choose file*. Select the public key certificate file (.cer / .crt) and click *Open*.



Click on *OK*.

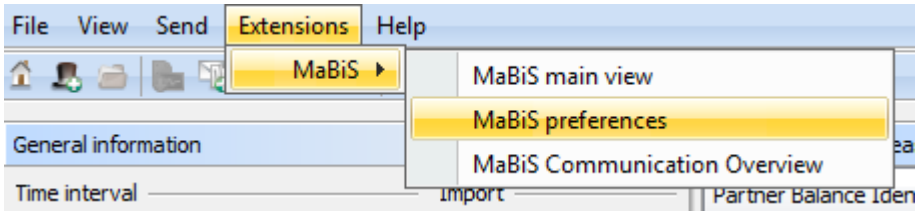


The file is visible in the table now. Click on *Apply* to persist the key.

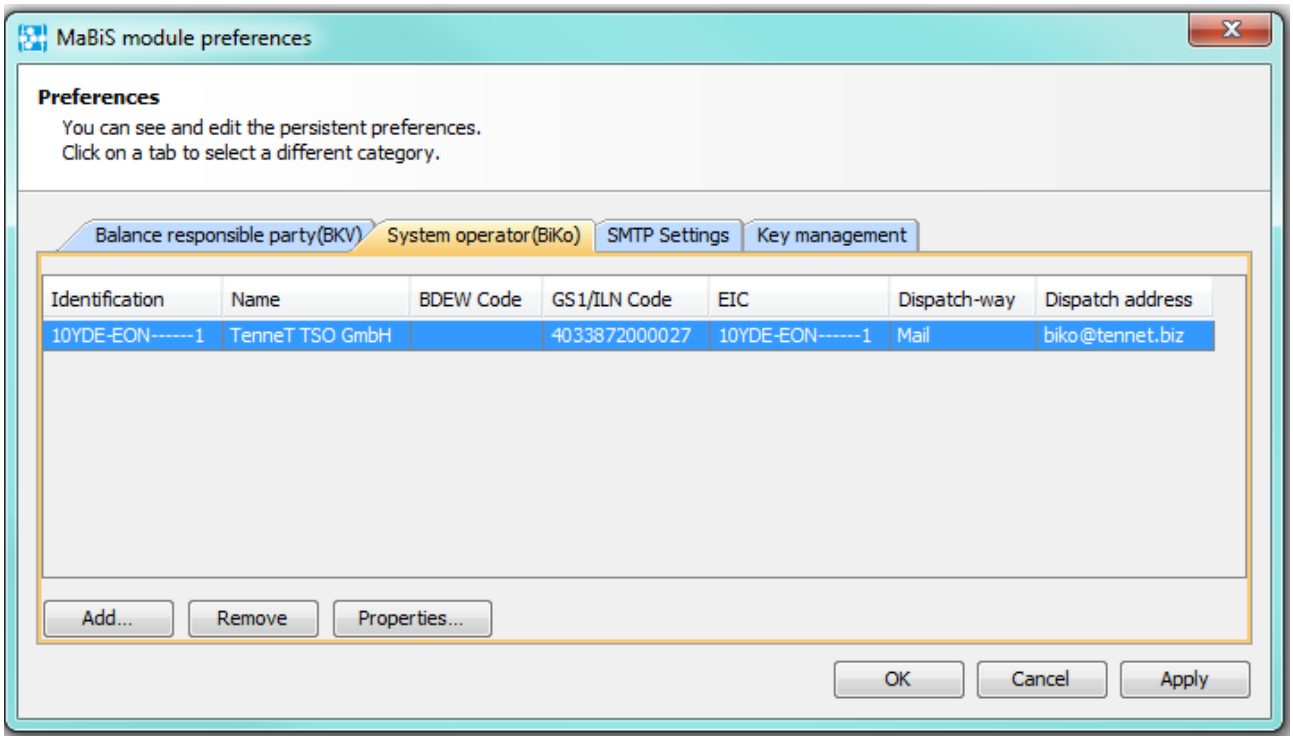


2.2 Assgin the keys

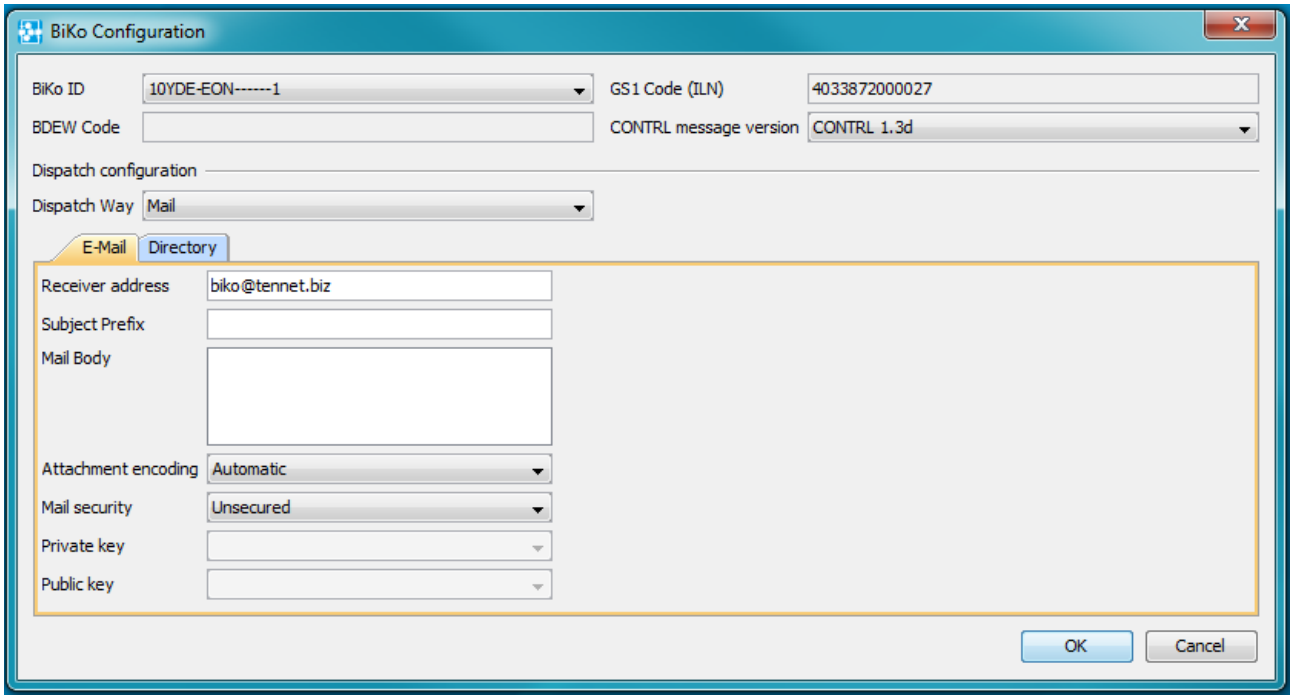
Open the *MaBiS preferences* view.



Go to the tab *System operator (Biko)*. Select a BiKo and click on *Properties…*



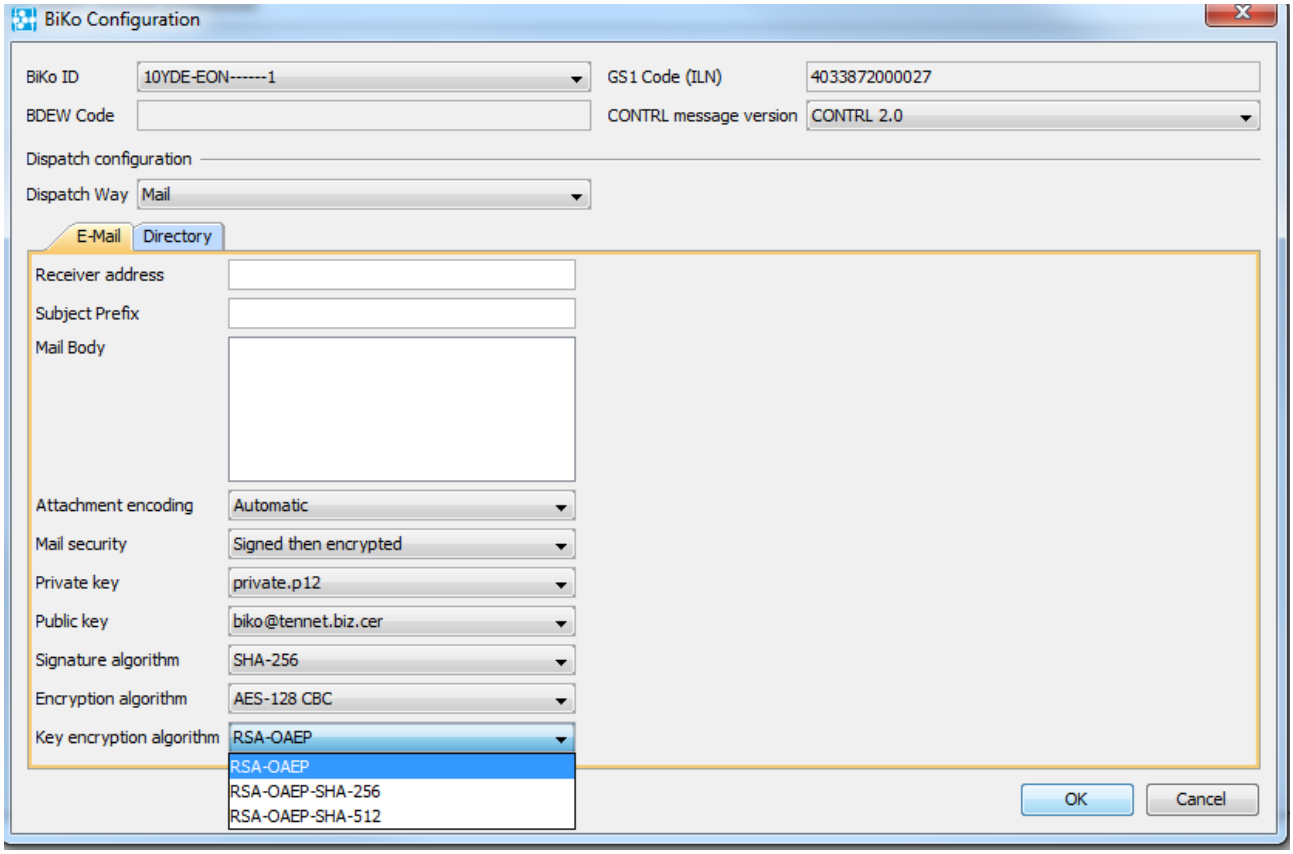
A new dialog will appear.



Change the *Mail security* to *Signed then encrypted*.

Select your own private key from the combo box *Private key*.

Then select the public key oft he BiKo from the combo box *Public key*.



After 1st January 2018, when decision BK6-16-200 of Germanys Federal Network Agencies ruling chamber 6 takes effect, at least the following settings need to be set:

- Signature algorithm: at least SHA-256-RSA-PSS or SHA-512-RSA-PSS
- Content encryption: at least AES-128 CBC or AES-192-CBC
- Key encryption: at least RSAES-OAEP-SHA-256 or RSAES-OAEP-SHA-512

Please ensure also, that the provided private key has RSA key encryption(RSASSA-PSS recommended) with a key length of 2048 bit.

Click after the configuration on *OK*.

After applying the changes the mails to the configured BiKos will be signed/encrypted.