1 Einführung

Dieses Dokument soll eine kurze Einführung darüber geben, wie die MaBiS-Erweiterung von ComCT konfiguriert warden kann, um signierte und verschlüsselte E-Mails zu versenden.

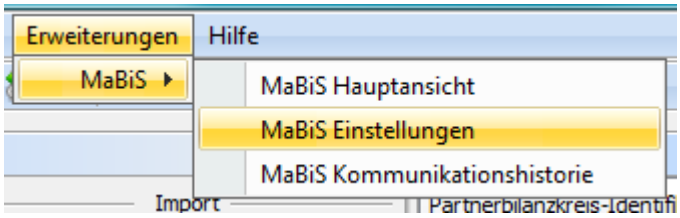
Die Vorgehensweise für die Konfiguration kann in zwei Schritte unterteilt warden.

1. Import der Schlüssel (Zertifikate) in die Schlüsselverwaltung.
2. Zuordnung der importierten Schlüssel zu den BiKos.

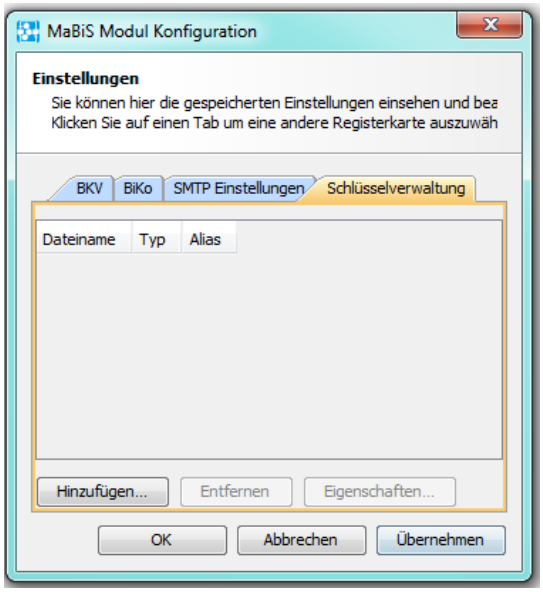
2 How-to

2.1 Import der Schlüssel in die Schlüsselverwaltung

Öffnen Sie die Ansicht *MaBiS Einstellungen*.



Wechsel zum Tab: *Schlüsselverwaltung*

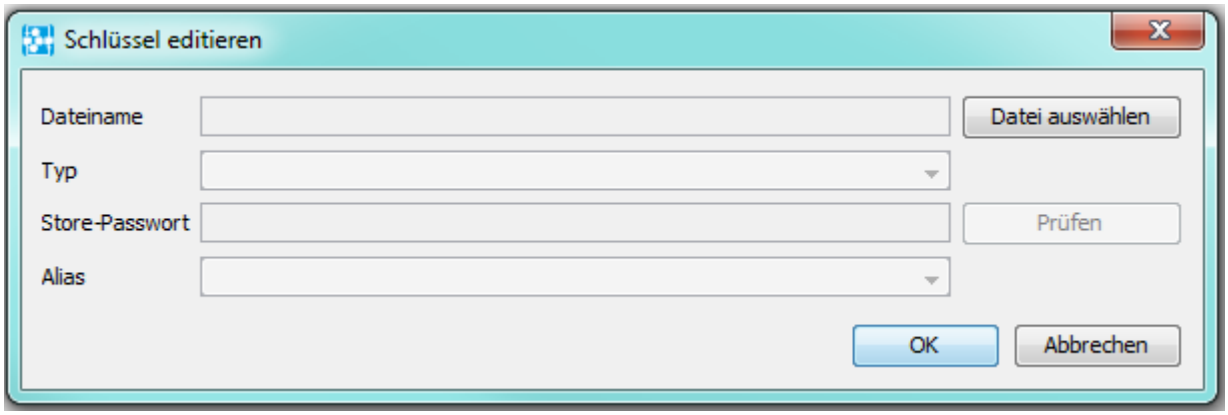


2.1.1 Import des privaten Schlüssels für die E-Mail-Signatur

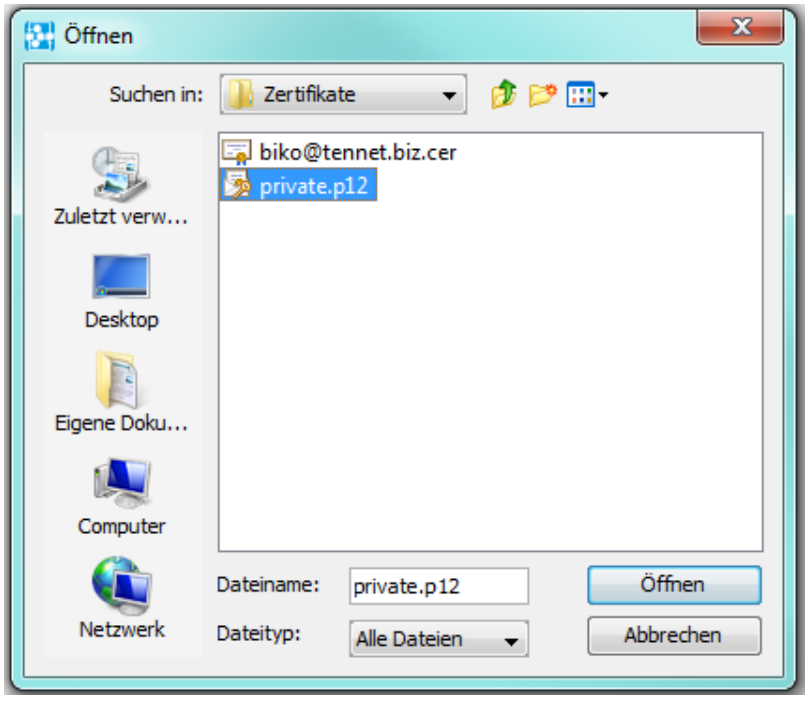
Hierfür muss das eigene Zertifikat importiert warden. Das private Zertifikat ist eine PKCS #12-Datei mit der Dateiendung .p12 oder .pfx.

Klicken Sie hierfür auf *Hinzufügen…*

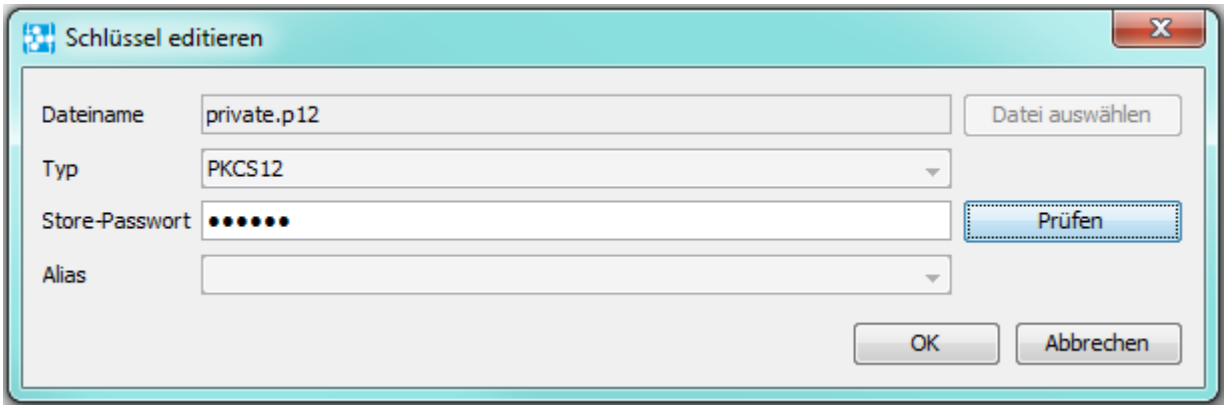
Ein neuer Dialog wird erscheinen.



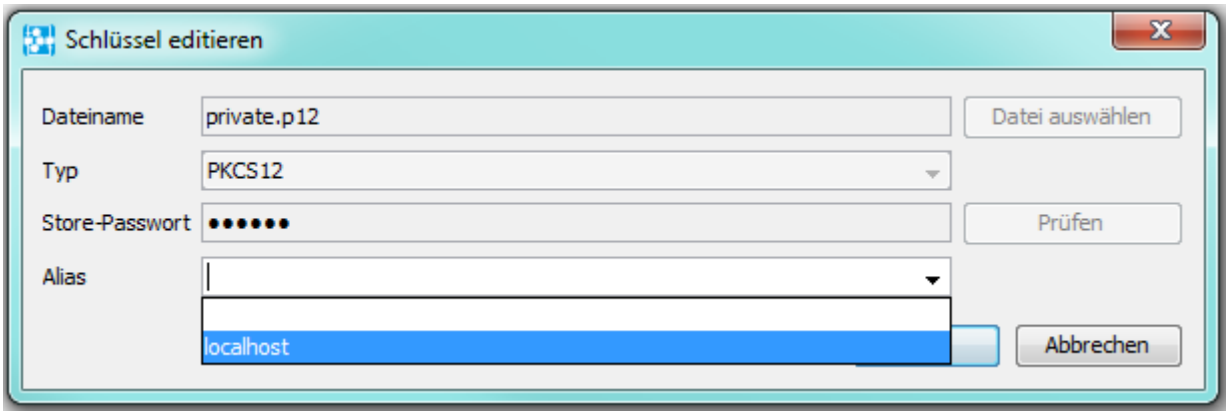
Klicken Sie auf *Datei auswählen*. Wählen Sie die Zertifikatsdatei (.p12 / .pfx) Ihres privaten Schllüssels aus klicken Sie auf *Öffnen*.



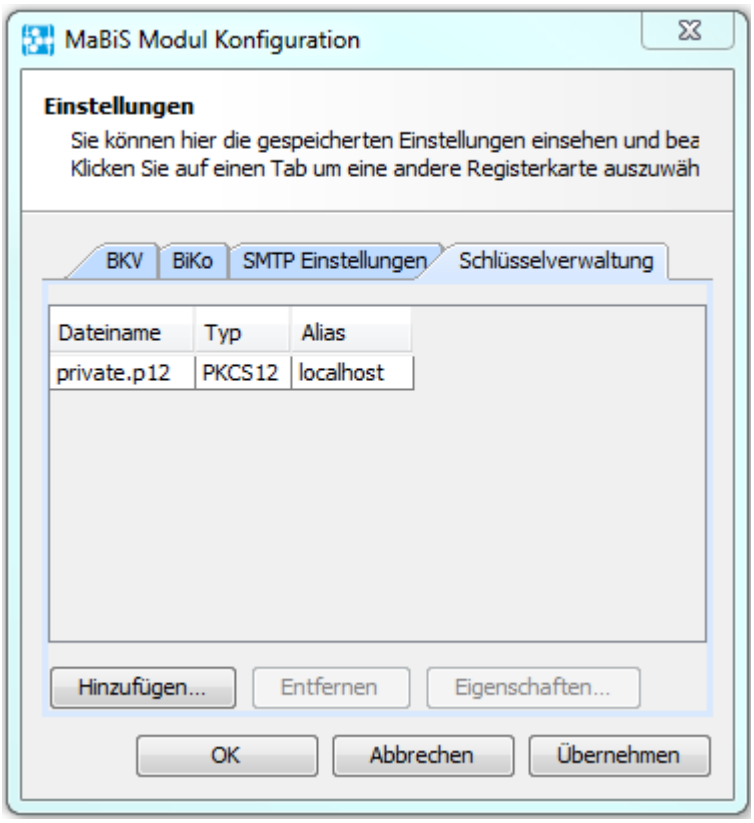
Geben Sie das Passwort ein und klicken Sie auf *Prüfen*.



Wählen Sie den Alias aus und klicken Sie auf *OK*. Gewöhnlicherweise enthält die PKCS #12-Datei nur einen Alias.



Die Datei wird anschließend in der Tabelle sichtbar sein. Klicken Sie auf *Übernehmen*, um den Schlüssel zu speichern.

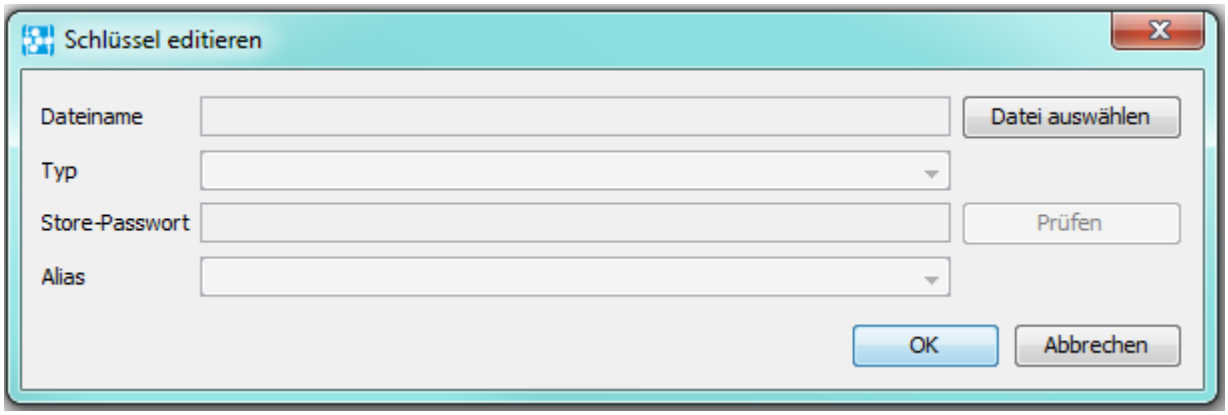


2.1.2 Import des öffentlichen Schlüssels für die E-Mail-Verschlüsselung

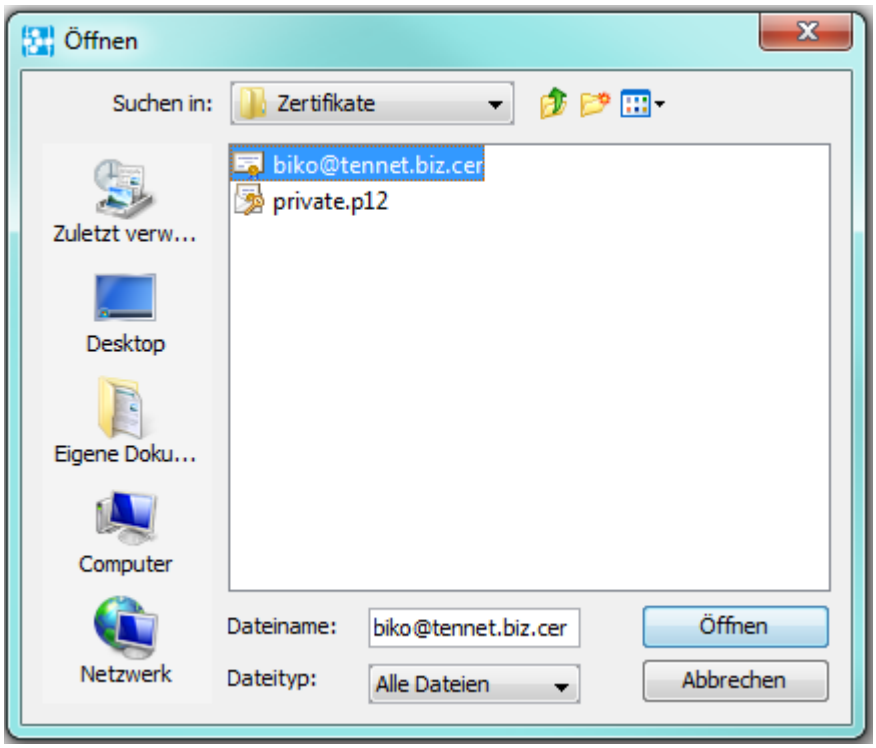
Hierfür ist das Zertifikat des BiKos zu importieren. Dies ist eine X.509-Datei mit der Dateiendung .cer oder .crt. Es kann auch eine PKCS #7-Datei sein. Im folgenden Beispiel wird die X.509-Variante verwendet.

Klicken Sie hierfür auf *Hinzufügen…*

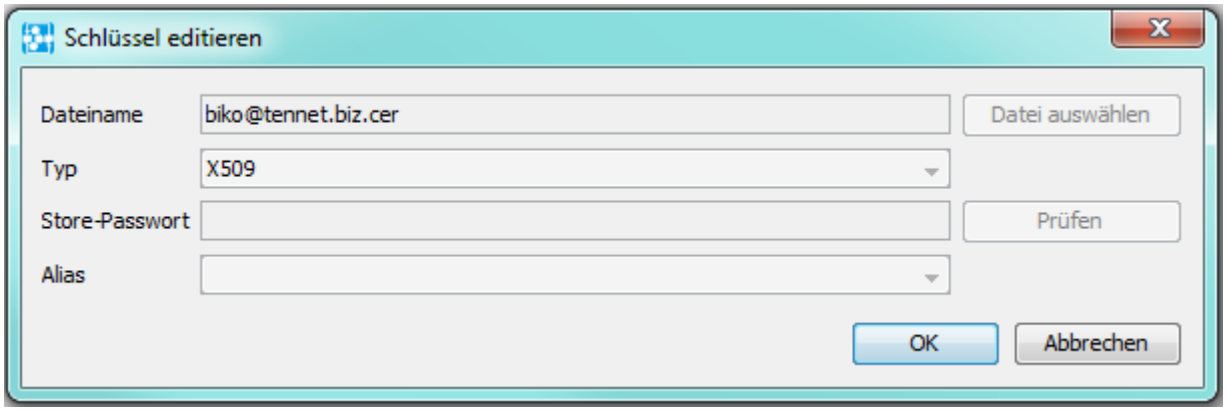
Ein neuer Dialog wird erscheinen.



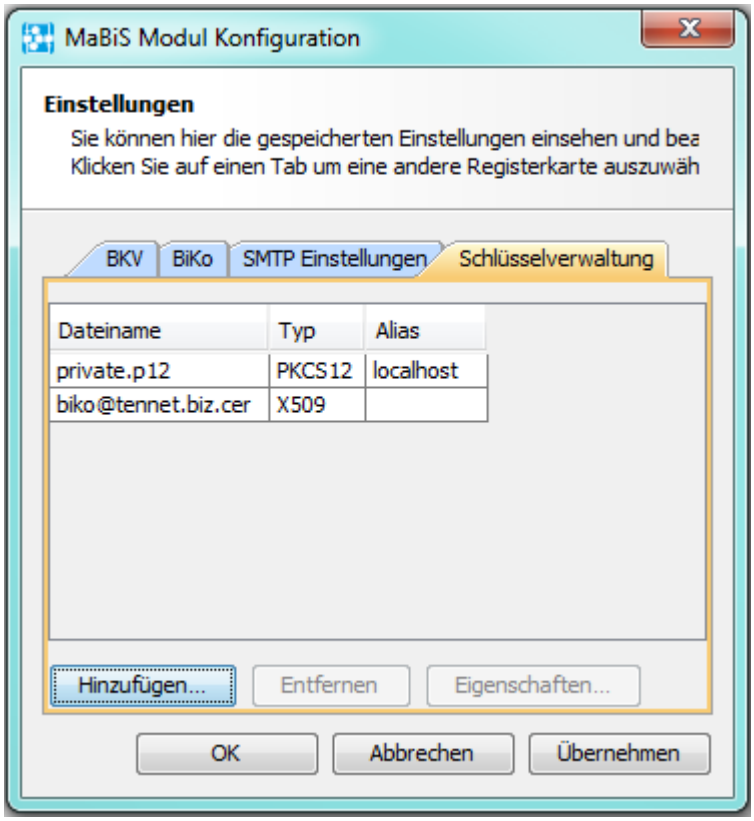
Klicken Sie auf *Datei auswählen*. Wählen Sie die Zertifikatsdatei (.cer / .crt) des öffentlichen Schlüssels aus klicken Sie auf *Öffnen*.



Klicken Sie auf *OK*.

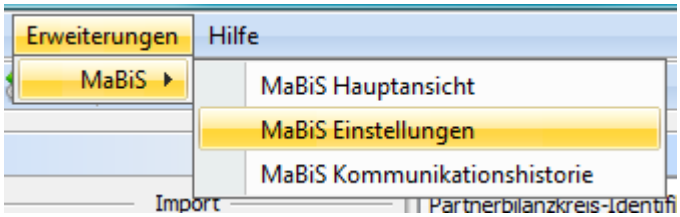


Die Datei wird anschließend in der Tabelle sichtbar sein. Klicken Sie auf *Übernehmen*, um den Schlüssel zu speichern.

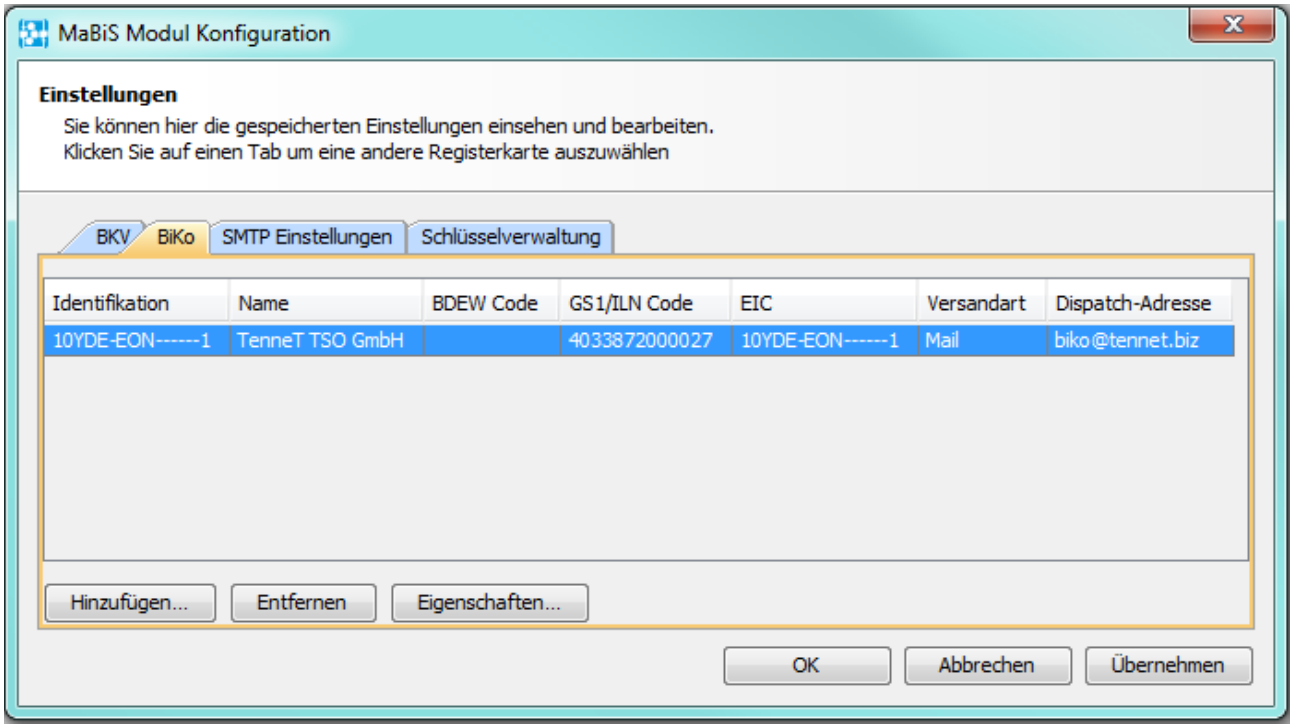


2.2 Zuordnung der Schlüssel

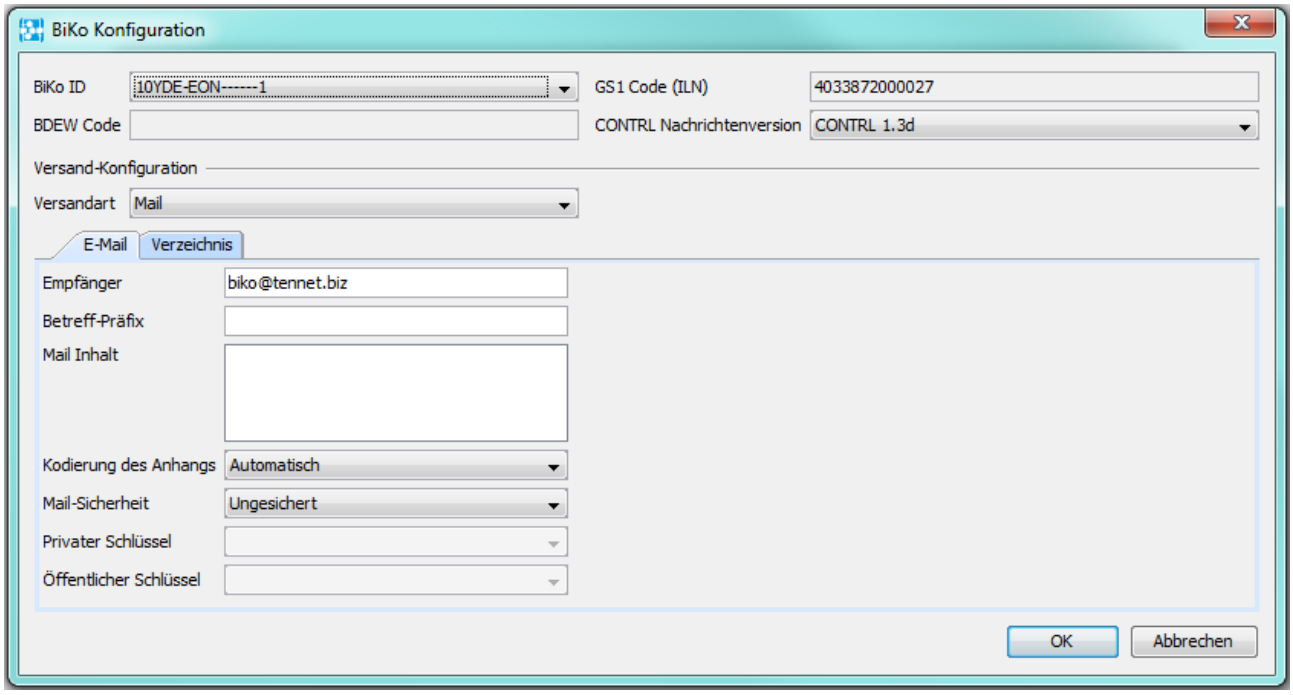
Öffnen Sie die Ansicht *MaBiS Einstellungen*.



Wechseln Sie zum Tab *Biko*. Wählen Sie einen BiKo aus und klicken Sie auf *Eigenschaften…*



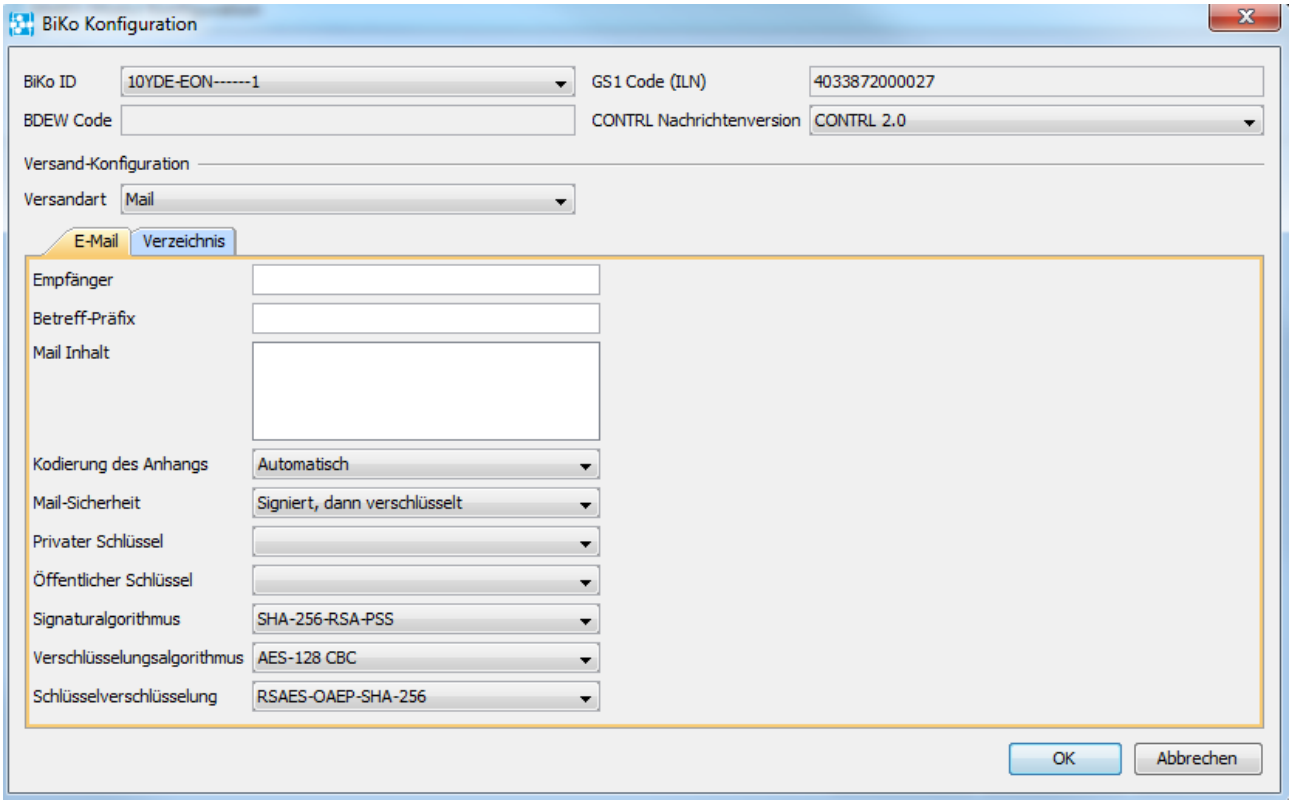
Ein neuer Dialog wird erscheinen.



Ändern Sie die *Mail-Sicherheit* zu *Signiert, dann verschlüsselt*.

Wählen Sie Ihren eigenen privaten Schlüssel über die Combo-Box *Privater Schlüssel* aus.

Wählen Sie dann den öffentlichen Schlüssel des BiKos über die Combo-Box *Öffentlicher Schlüssel aus*.



Als Signaturalgorithmus gem. den aktuellen Regelungen zum Übertragungsweg aus Anlage 5 des Beschlusses BK6-16-200 der Bundesnetzagentur wird folgende Einstellung ab dem 01.01.2018 erwartet:

- Signaturalgorithmus: SHA-256-RSA-PSS oder SHA-512-RSA-PSS
- Verschlüsselungsalgorithmus: AES-128 CBC oder AES-192-CBC
- Schlüsselverschlüsselung: RSAES-OAEP-SHA256 oder RSAES-OAEP-SHA512

Bitte stellen Sie ausserdem sicher, dass die importierten privaten Schlüssel die Schlüsselverschlüsselung nach RSA (RSASSA-PSS empfohlen) mit einer RSA Schlüssellänge von mindestens 2048 Bit aufweist.

Klicken Sie nach der Parametrierung auf *OK*.

Nach Übernehmen der Einstellungen werden die E-Mails an die konfigurierten BiKos signiert/verschlüsselt sein.