

# **A User Perspective: What should be improved in Thunderbird – considering especially the use of S/MIME and PGP/Enigmail**

(Document structured by using three different scenarios:  
S/MIME only, S/MIME and Enigmail, Enigmail only).

## Goal of this document:

To report, what we think could / should be improved in Thunderbird.

Notation: TB Thunderbird  
FF Firefox

Remark: The reported bad wording is NOT a matter of translation.  
According wrong or misleading strings are also in the English version.

Last change: January 28<sup>th</sup>, 2016

Author: Bernhard Esslinger  
(Head of an open-source project producing e-learning tools about  
cryptography, and member of a German academic group helping  
to improve handling of secure email)

## Content

1. Thunderbird solely.....	4
1.1. Text too long for the status line in TB – How to handle this?.....	4
1.2. Attachments too big. Warning but no advice.....	4
1.3. S/MIME Certificate Manger is missing a search field to look through all information within one tab or all tabs.....	5
1.4. Formal and stupid messages instead of a helpful analysis (besides all information is known).....	6
1.4.1 Signature invalid.....	6
1.4.2 Certificate information wrong.....	9
1.4.3 Certificate was revoked: No recommendation what the user should do.....	10
1.5. TB installation doesn't suggest to protect the keystore with a “master password” (wrong default).....	11
1.6. Can an S/MIME certificate contain more than one email address?.....	11
1.7. TB needs an equivalent to the Encrypt-if-Possible plugin as build-in functionality.....	12
1.8. Bad usability, if an email cannot be S/MIME encrypted for some of the recipients, but for others.....	13
1.8.1 First error dialog is ok, second is incomplete.....	13
1.8.2 Dialog "Message Security" has wrong wording ("not found" instead of "expired").....	14
1.8.3 Bug in the spreadsheet control in the dialog "Message Security".....	14
1.9. Creation and prolongation of certificates from within TB.....	15
1.10. Handling of partner certificates: Show icon as flag for user trust.....	17
1.11. Search also through encrypted mails.....	18
1.12. Importing of CA certificates into the TB keystore.....	19
1.13. Handling of own expiring certificates.....	20
1.13.1 Notification BEFORE a certificate expires.....	20
1.13.2 Support with certificate renewal.....	20
2. TB used to mail with both S/MIME and Enigmail communication partners.....	21
2.1. Message from Enigmail besides only using S/MIME for this mail.....	21
2.2. Different ways to activate/deactivate enc/sign properties and to see their status.....	22
2.2.1 The way of S/MIME.....	22
2.2.2 The way of Enigmail.....	23
2.3. Conflicting parameters – PGP is overruled, lower security might be used.....	24
2.4. Sending an email to recipients with different key types – from the user's perspective.....	25
2.4.1 Coexistence and both-support – Request 1.....	25
2.4.2 Coexistence and both-support – Request 2.....	25
3. Some Enigmail-only issues.....	26
3.1. Scenario where the trust level isn't shown correctly, and the attached key isn't handled accordingly.....	26
3.2. Scenario where the trust level isn't shown correctly, and the attached key isn't handled accordingly.....	31

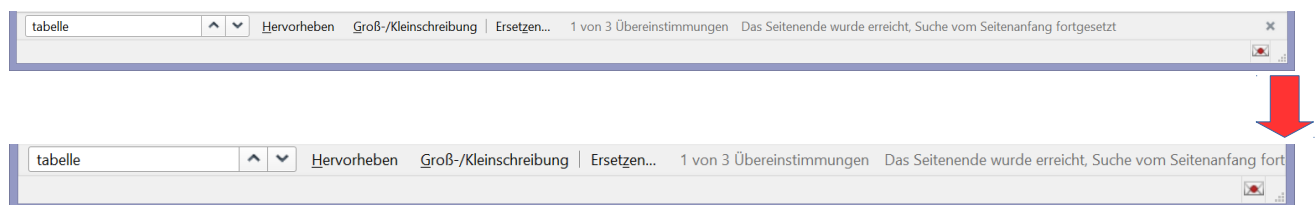
3.2.1 Wrong messages after getting an encrypted email with the sender's pubkey attached....	32
3.2.2 Case where Enigmail menu entry "Import key" doesn't work correctly.....	33
3.2.3 Case where Enigmail menu entry "Decrypt / Verify" doesn't work correctly.....	33
3.2.4 Double click on the attached pubkey works fine, but some texts are misleading.....	34
3.3. Getting the pubkey of a user as string within the email body (not as an attached email) leaves user alone how to import it.....	36
3.4. Offer comment to each PGP key added in the keystore.....	39
3.5. Offer as default: Send PGP-signed emails (like in S/MIME).....	39
3.6. Sometimes signatures and keys are UNVERTRAUT besides I spent user trust (maybe my fault).....	40
3.7. Received S/MIME message contains a PGP key as attachment.....	42
3.8. After receiving a PGP-encrypted email you did not enter the key at once.....	42
3.9. Umlaut problems in some Enigmail triggered dialogs.....	43
4. Appendix.....	44
4.1. GnuPG: User feedback in case of decryption.....	44

# 1. Thunderbird solely

Here issues are listed which have nothing to do with security (chapter 1.1 and 1.2), and issues which are related to the currently built-in S/MIME implementation.

## 1.1. Text too long for the status line in TB – How to handle this?

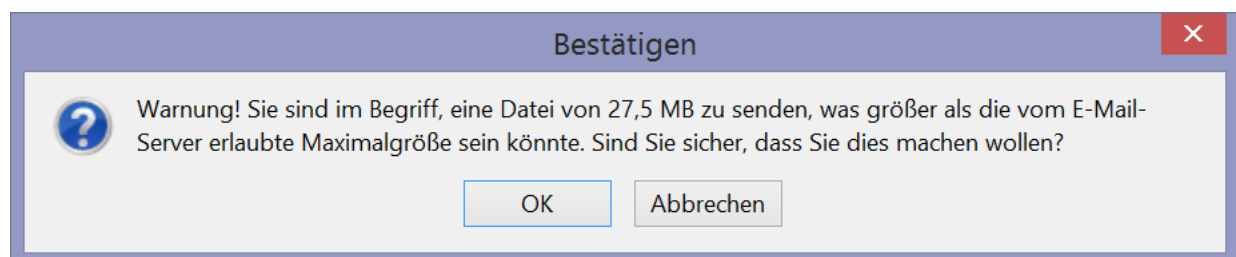
(This is no important issue, and independent of S/MIME.)



## 1.2. Attachments too big. Warning but no advice

(This is no important issue, and independent of S/MIME.)

A normal user would expect in addition an advice what he should do and where he can get more hints how to do this.



### 1.3. S/MIME Certificate Manger is missing a search field to look through all information within one tab or all tabs



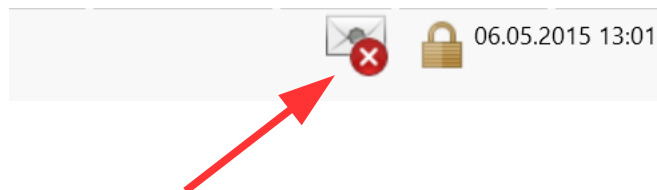
A search field is necessary e.g. if you want to know the reason why there is no valid certificate: Did the time of its validity period end, or do you have no certificate for this email address in your keystore?

## 1.4. Formal and stupid messages instead of a helpful analysis (besides all information is known)

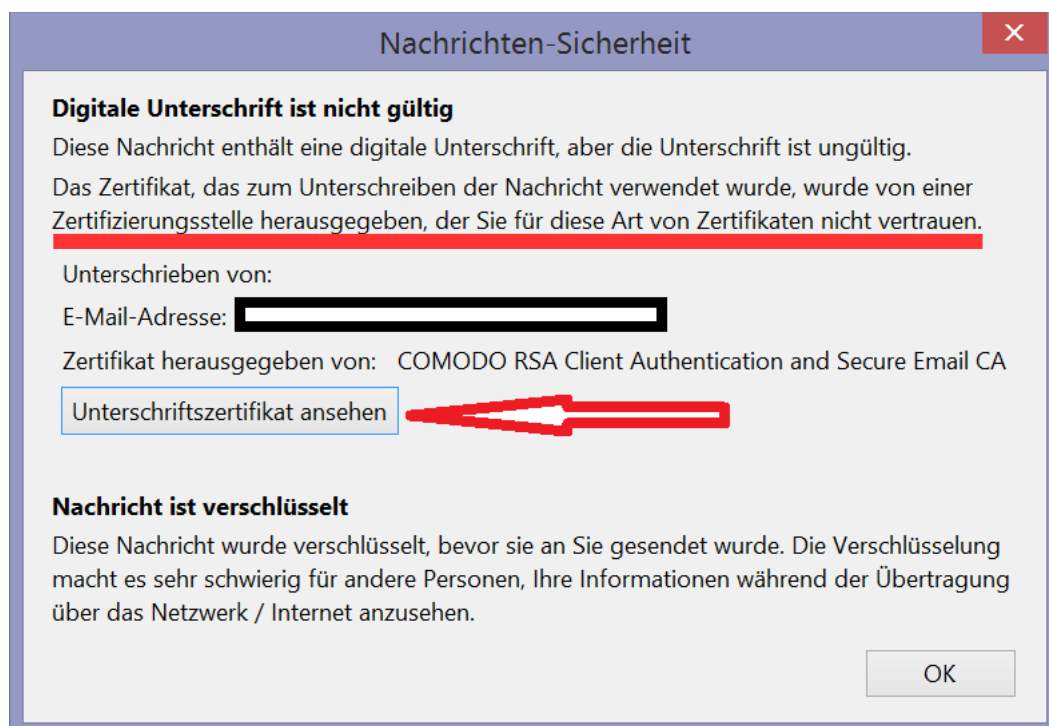
(This is an important issue from the user perspective when he wants to secure his emails.)

### 1.4.1 Signature invalid

Scenario: You received an S/MIME encrypted message which had a valid signature a while ago (maybe just shown yesterday). Then you look at it again later:



Clicking on the invalid signature icon brings up the following message box with a formally correct but stupid and unhelpful message which gives security aware users unnecessarily a bad feeling.

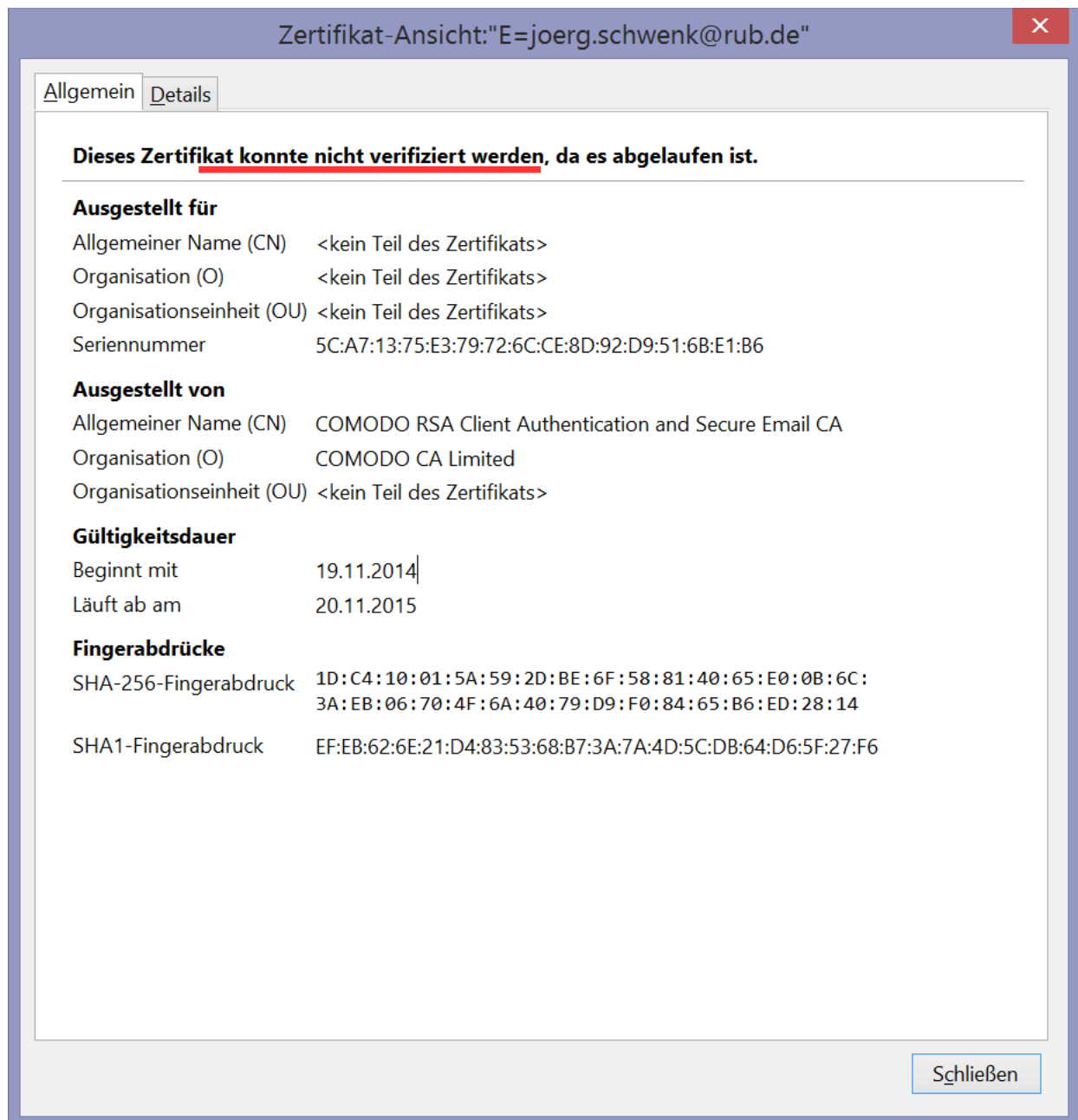


The sentence, that I don't trust the according certification authority (here Comodo) for this kind of signatures, is just wrong!!!

Then, clicking on "Unterschriftszertifikat ansehen" reveals the correct reason but still has a wrong part stating, that the signature could not be verified.

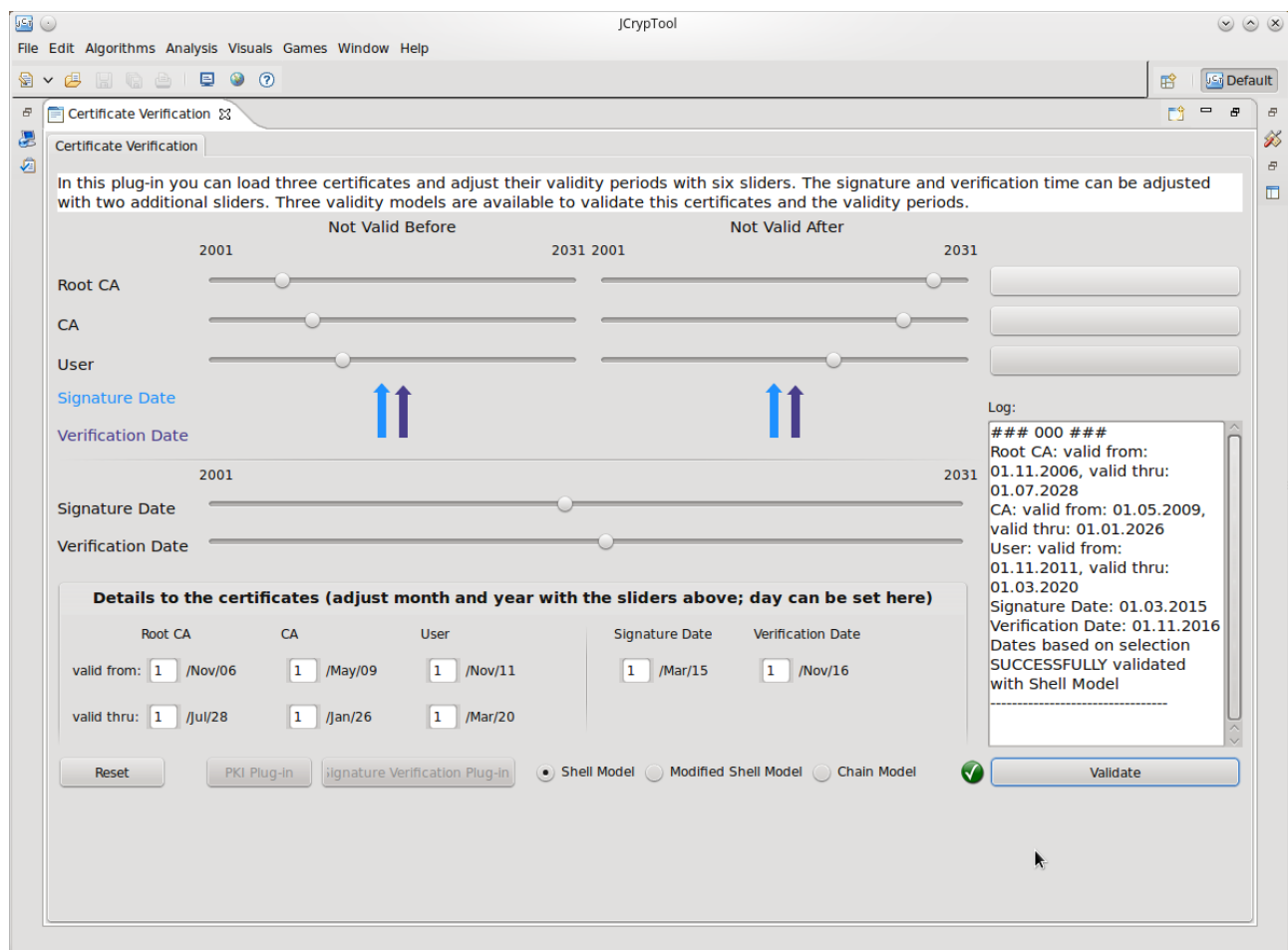
What I'd consider as helpful is a set of statements like this:

- The message is digitally signed and the signature hash fits to the message.
- As the certificate of the user isn't valid any more (it ended 2015-11-20) the signature has to be rated as "invalid" [according to the used verification model (layer model)].
- So if you would have looked at this message before 2015-11-20 the verification result would have been "valid".



Just for information:

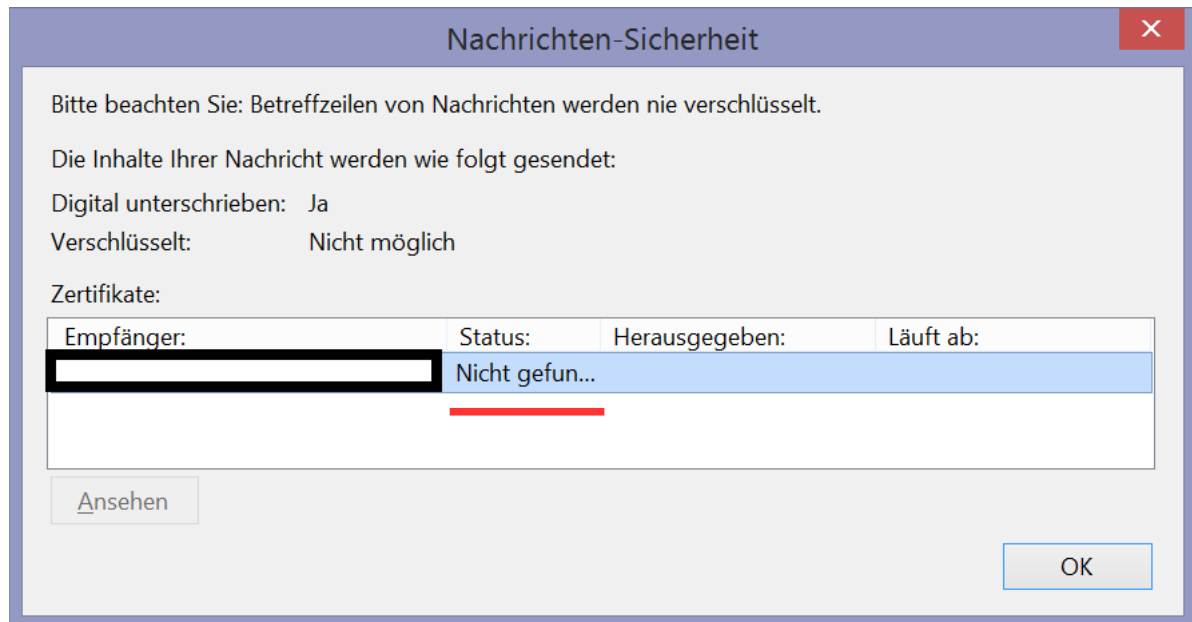
The e-learning program JavaCrypTool (JCT) from [www.cryptool.org](http://www.cryptool.org) contains a visualization where you can see what the result depends on in the different verification models (shell, modified shell and chain model – in German: Schalenmodell, erweitertes Schalenmodell und Kettenmodell), and how you interactively can learn this playfully. S/MIME uses Schalenmodell = PKIX-Model = layer model.





## 1.4.2 Certificate information wrong

This dialog is from the scenario described below in chapter "2.2 Different ways to activate/deactivate enc/sign properties and to see their status" [within part "a) The way of S/MIME"]:

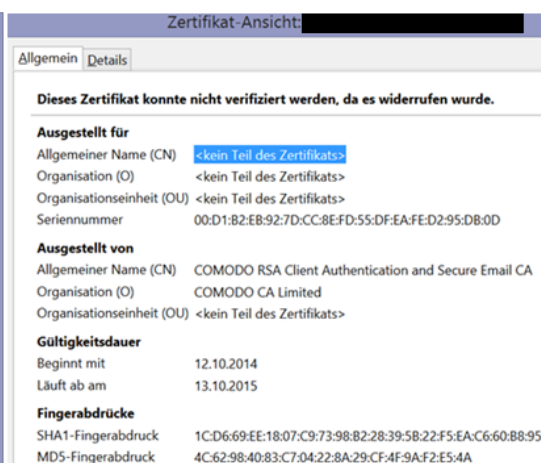
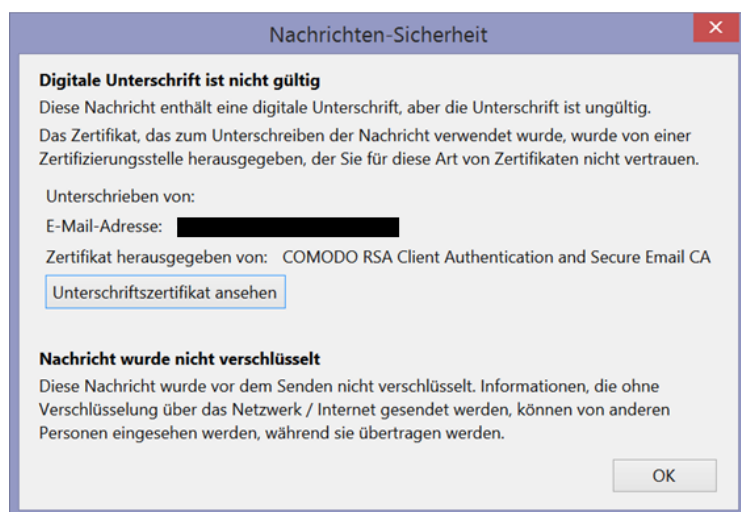
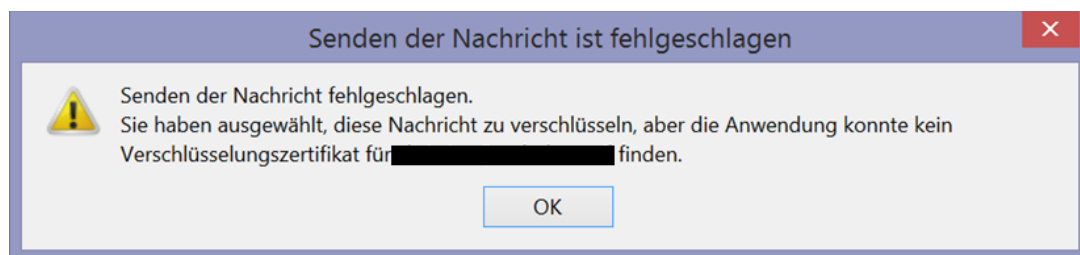


There is indeed a certificate fitting to the according receiver's address. So it should not state "Not found", but "No more valid", and then still allow to mark it and to click on the "View" button.

However, there also should be another column like "Usable", and then there should be a red cross instead of a green check.

### 1.4.3 Certificate was revoked: No recommendation what the user should do

There should always be a good *explanation* what happened (both if success or if no success); and there should always be a meaningful *recommendation* what to do using all the given information.



## **1.5. TB installation doesn't suggest to protect the keystore with a “master password” (wrong default)**

This seems to be a symbol that the developers haven't been aware enough for security in the past.

At least when generating an S/MIME key pair TB should ask to protect its keystore too.

## **1.6. Can an S/MIME certificate contain more than one email address?**

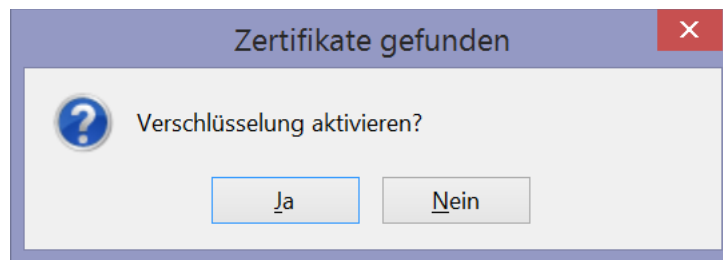
If not this is a request, as a PGP certificate can contain for a user several email addresses.

## 1.7. TB needs an equivalent to the Encrypt-if-Possible plugin as build-in functionality

The TB plugin "Encrypt-if-possible" is helpful to ensure that TB always encrypts your mails if you have the S/MIME key for all recipients (so you don't have to check by yourself anymore). This plugin is necessary because TB currently offers as sending defaults only two options: to never encrypt and to always encrypt. A third one (encrypt if there are certs available for all recipients) is missing.

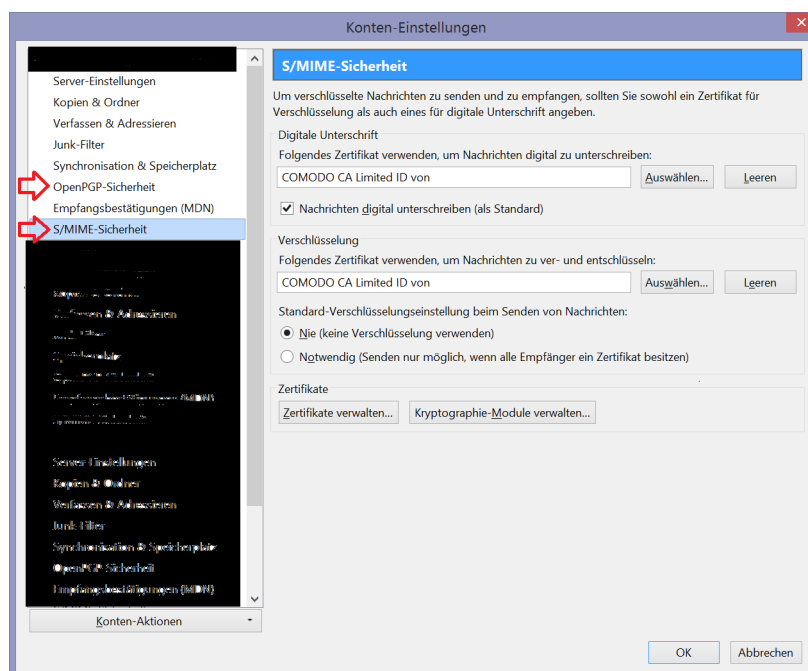
However, the current plugin has several flaws:

- If I answer "No" to the question whether I want to activate encryption (so explicitly switching off S/MIME encryption) the plugin asks me again periodically some minutes later.  
This is especially bad, if you have from a user both an S/MIME and a PGP key.
- It even asks if no recipient address is entered in the "To" field.  
(For whom did it find certificates as stated in the title?)



==> The Encrypt-if-possible functionality should be a native part of TB. As integrated part it should remember if the user already responded with "No", and don't ask again and again.

The behavior whether and when to encrypt could be shown in the dialog for the account parameters. AND: All the options for PGP and S/MIME should be offered and structured in dialogs with the same layout – so users easily know what's going on and where they are.



## 1.8. Bad usability, if an email cannot be S/MIME encrypted for some of the recipients, but for others

Here, the scenario is to send an email in encrypted manner to 14 recipients.

This was possible a while ago for the complete recipients list without any problem, but now some of the certificates are no more valid.

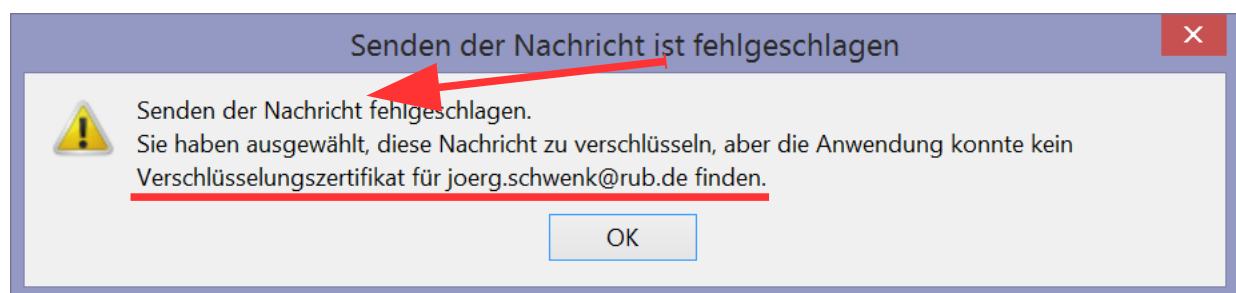
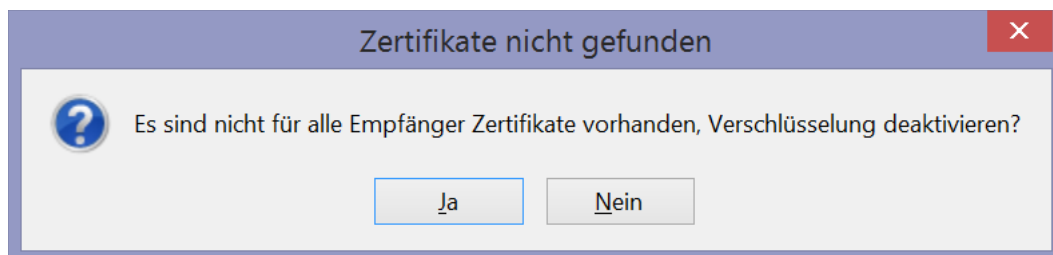
==> Users are left alone to find the reason and what to do.

### 1.8.1 First error dialog is ok, second is incomplete

a) If I click "nein" in the 1<sup>st</sup> dialog, then the 2<sup>nd</sup> error dialog ("Senden der Nachricht fehlgeschlagen") shows only one user as the reason.

b) However, there are 4 users preventing to send an encrypted email. This should be mentioned.

c) The reason is not that TB couldn't find an encryption certificate, but that the found one is no more valid ("konnte kein Verschlüsselungszertifikat für ... finden").

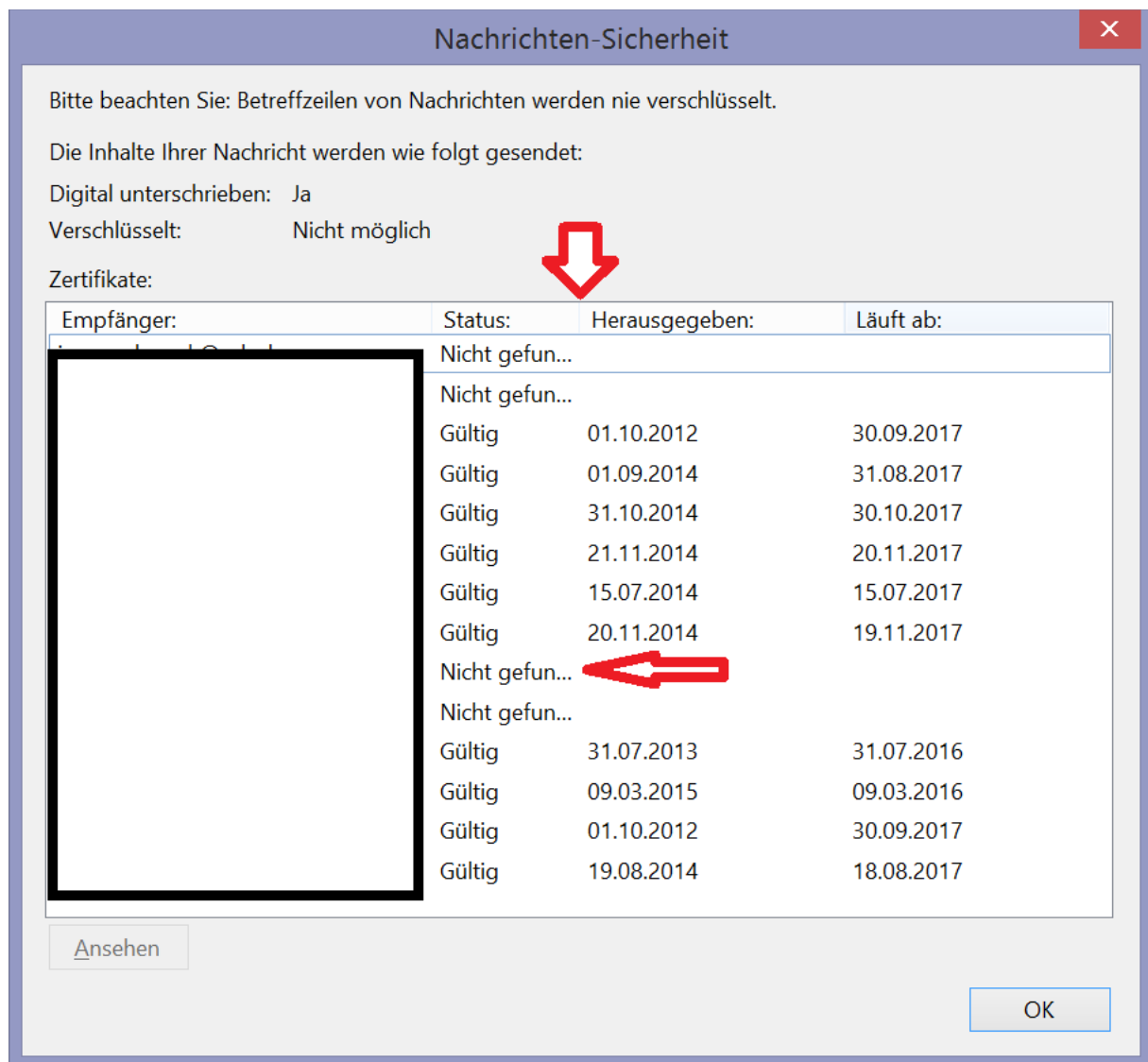


d) There should be support for the user, what to do. Options to be offered could be:

- encrypt with the existing certificates as long as it's just the end date which is no more valid (so send it to all 14 recipients in encrypted manner)
- encrypt for the rest (11 recipients), and create another mail to send it unencrypted to the 4 recipients with the outdated certificate.

### 1.8.2 Dialog "Message Security" has wrong wording ("not found" instead of "expired")

Below the menu bar (in the main windows of TB) there is the S/MIME icon with its drop-down control. Clicking there and selecting the item "Sicherheitsinformationen anzeigen", the following dialog says in the status column, that there is no certificate ("Nicht gefunden"). Instead it should say, that it is there but it is "abgelaufen" (= "expired") or what else the exact reason is (as the certificate still exists).



### 1.8.3 Bug in the spreadsheet control in the dialog "Message Security"

The spreadsheet within this dialog "Nachrichten-Sicherheit" has a bug – you cannot change the widths of the status column by drawing the border with the mouse nor by double-clicking at its right border (in the column's header).

## 1.9. Creation and prolongation of certificates from within TB

Currently you have to go to a website via a browser (FF) and there you have to request creating the key pairs, creating a certificate for the public key, exporting the keys from the FF (Mozilla) keystore and importing them into the TB keystore via a PK12 file.

==> This is much too complicated for a normal user.

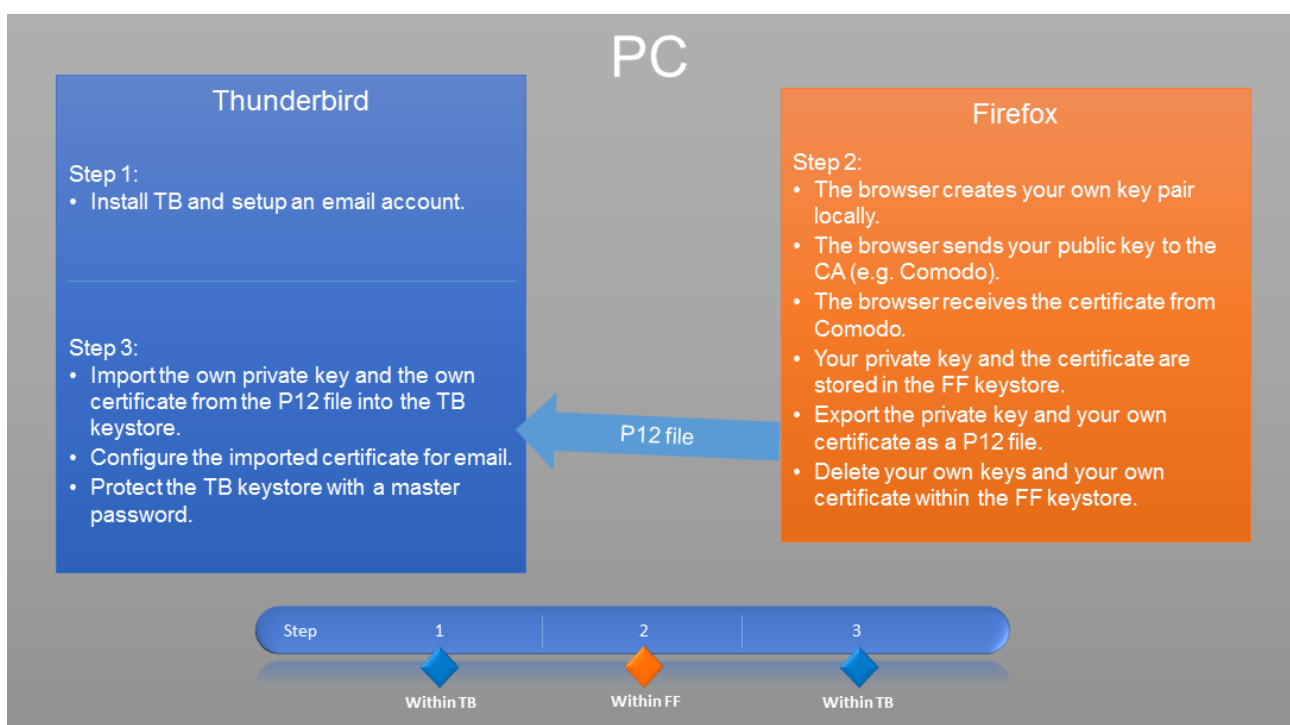
Users don't accept arguments like the ones found in the documentation: TB and FF are different products with own key stores. Users who have installed both, TB and FF, expect that they can request a certificate from WITHIN Thunderbird (It is possible in Outlook too. We know that Outlook uses the Windows (OS) keystore).

So the 1<sup>st</sup> step should be, that the created keypair and the cert can be put into the TB keystore without the intermediate transport file.

In a 2<sup>nd</sup> step, key generation and the certificate request should be possible from within TB.

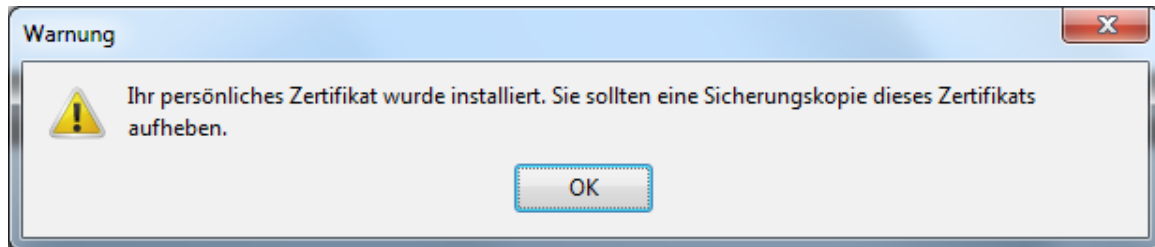
This would take away a big initial hurdle using S/MIME encrypted email.

The following graphics shows that users have to switch twice between the applications TB and FF just to get an initial certificate, and that the users have to deal with things like "keystore", "p12 file" which they normally don't know.



### Remark 1: False warnings

After you receive the certificate from the CA it is stored in the FF keystore. This is ok. However, you get a warning. This alienates users because nothing went wrong. The certificate was successfully stored.



Same false warning, when the certificates have been successfully imported into the TB keystore. This is no warning:



### Remark 2: Avoid unnecessary user interactions

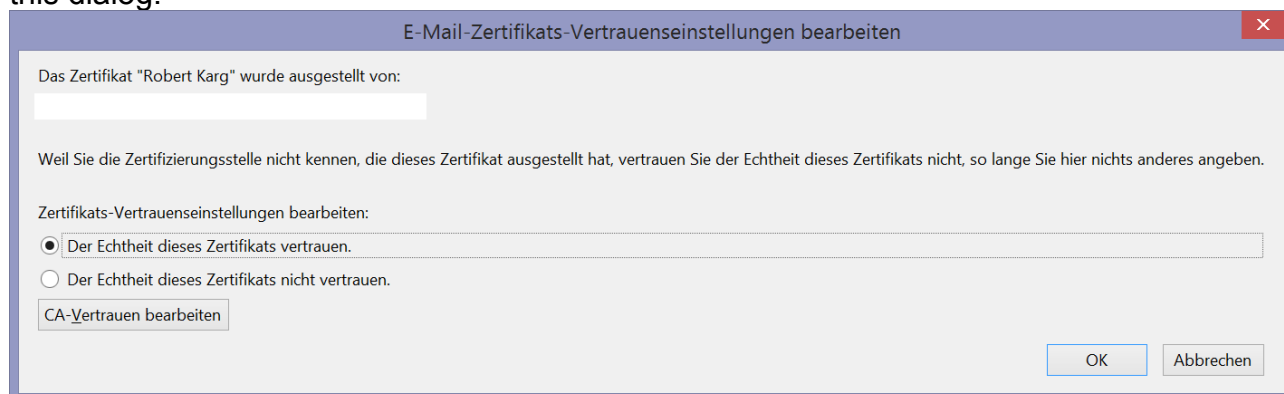
When installing certificates TB should act like a wizard: It should proactively offer the option to make this certificate available for your mail account.



## 1.10. Handling of partner certificates: Show icon as flag for user trust

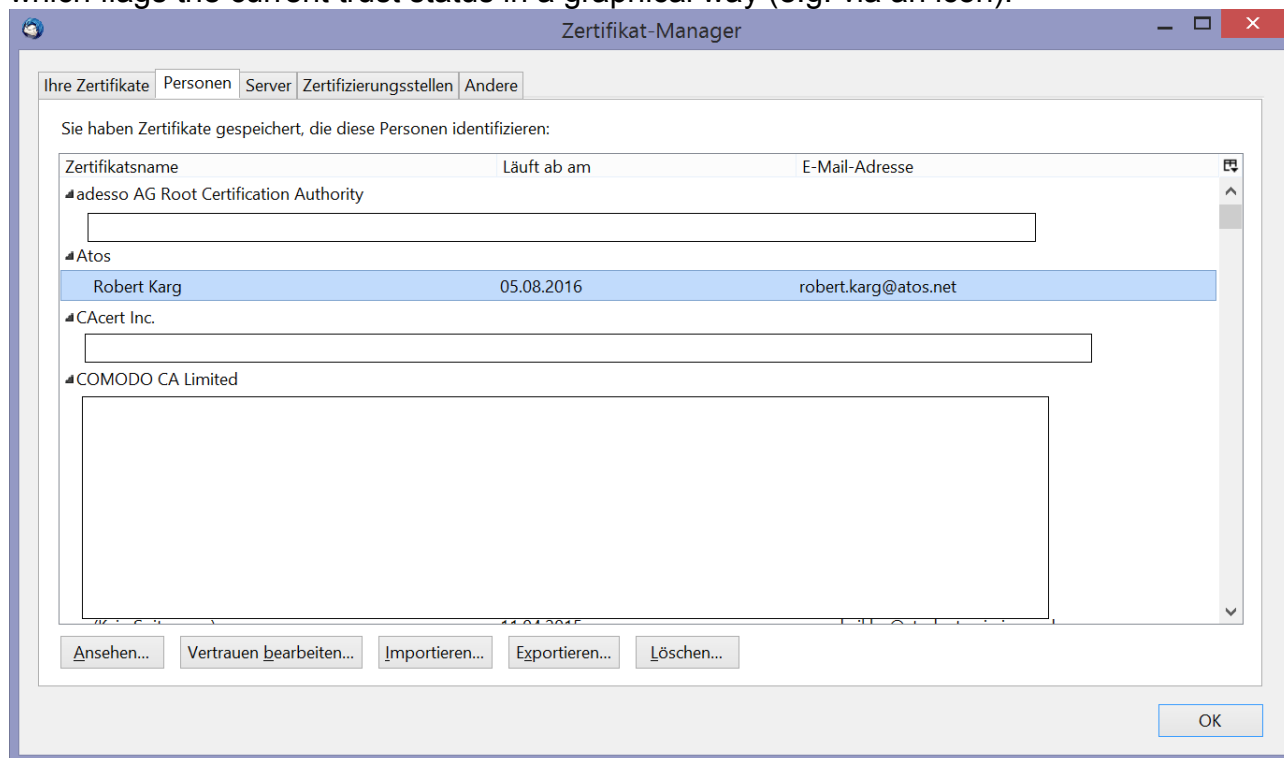
If you get a signed email the certificate of your communication partner is stored automatically in the TB keystore, which is good.

Looking, what trust you currently have in the cert of this user and in his signing CA, shows this dialog:



If the signing CA is not known to TB yet, you have to express trust to this partner's certificate.

Users are missing in the list of certificates for partners (other persons) another column which flags the current trust status in a graphical way (e.g. via an icon).



## **1.11. Search also through encrypted mails**

Another complaint expressed often by users is that the search capability with encrypted email is limited to the header information.

There should be a way a get rid of this restriction:

Maybe there could be an option to decrypt all mails at the beginning or when search is started.

Here, some more research has to be done, how to implement this is a good and efficient way.

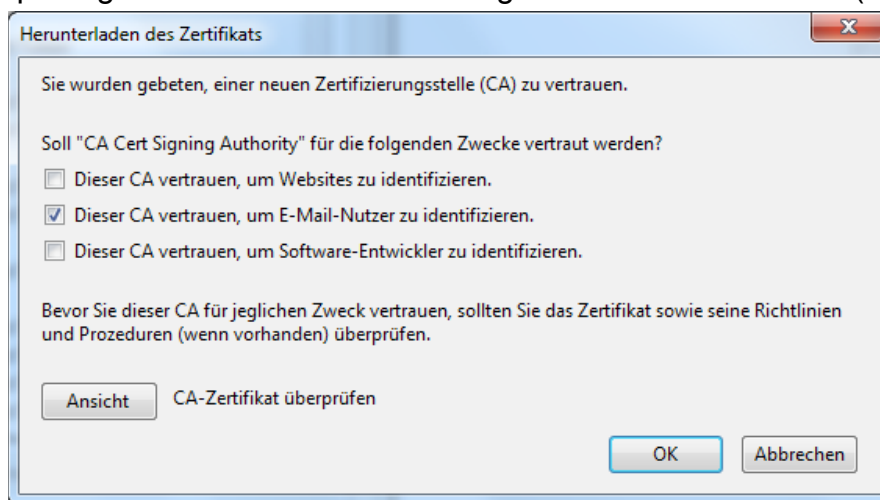
## 1.12. Importing of CA certificates into the TB keystore

a) This process only works if done in exactly the described way without any tolerance.

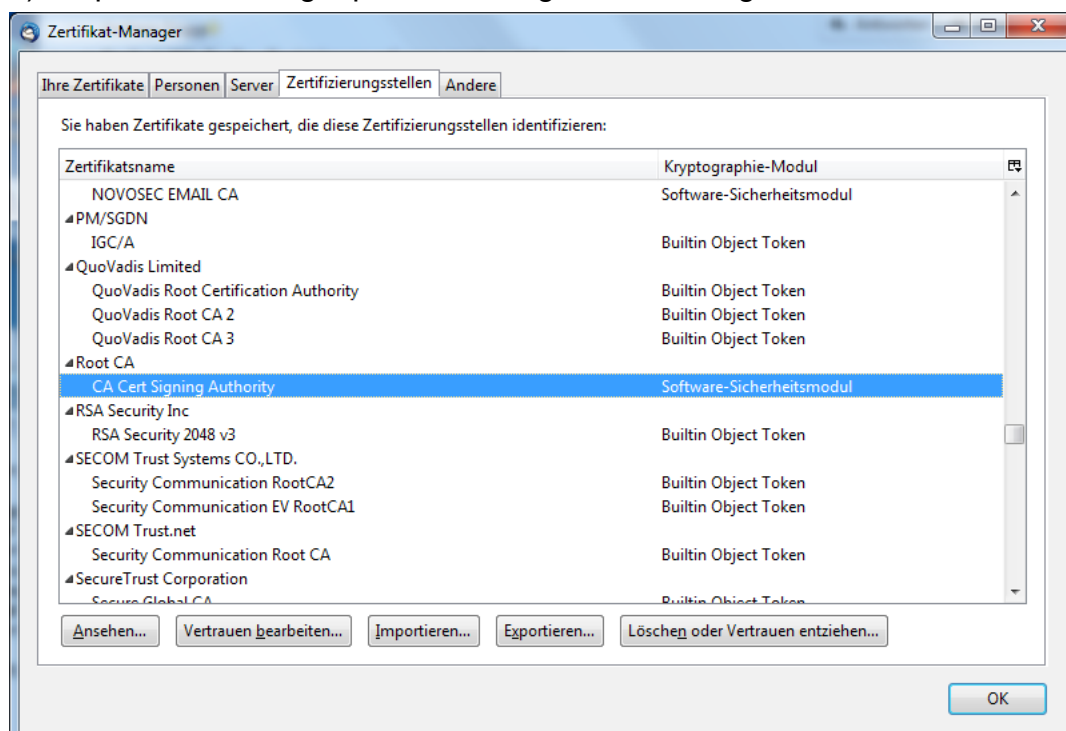
TB should

- update the shown information about the validity of an email directly after the import (currently users have to close the email and reopen it in order to see a correct signature)
- offer much more information about a received partner certificate:
  - did it include its signing CA?
  - did it include the whole certification path?
  - etc.

b) After importing a CA certificate and clicking on the button “Ansicht” (View),



then you get the list of certificates in its initial view. However, users want that the according tab (CAs) is opened at the right place showing the according root cert as selected:



## **1.13. Handling of own expiring certificates**

This is another bad user experience keeping users away from S/MIME even after they came across the initial hurdles.

### **1.13.1 Notification BEFORE a certificate expires**

Currently you normally don't notice if your certificate expires (normally once a year), but others cannot send encrypted emails to you and have to make you request a new certificate. So TB should warn you BEFORE your own certificate expires.

### **1.13.2 Support with certificate renewal**

After the notification TB should offer a wizard with guidance in order

- to renew the certificate (going to the website of the CA again and request a new certificate).
- to send a signed email to all users whom you already have been in secured email contact with:
  - The list of these mail addresses should be editable.
  - There should be a default text offered to send to these partners like  
"You get this signed email, as my old certificate (ID xxx) expires at xxxx-xx-xx.  
So here is the new one (ID xxx, Validity from xxxx-xx-xx to xxxx-xx-xx).

Research question: Would it be possible to send the email signed with the private key (fitting to the pubkey of the old cert as long as this old cert is still valid) and attach the new certificate?

## 2. TB used to mail with both S/MIME and Enigmail communication partners

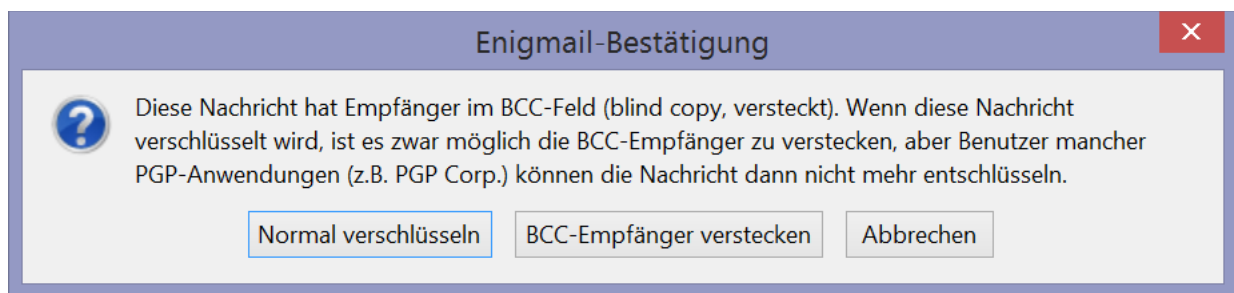
In this scenario there are 4 sets of partners you have email communication with: For some you have no pubkey; for some you only have an S/MIME certificate; for some you only have a PGP certificate; for the forth subset you have both, an S/MIME and a PGP key.

### 2.1. Message from Enigmail besides only using S/MIME for this mail

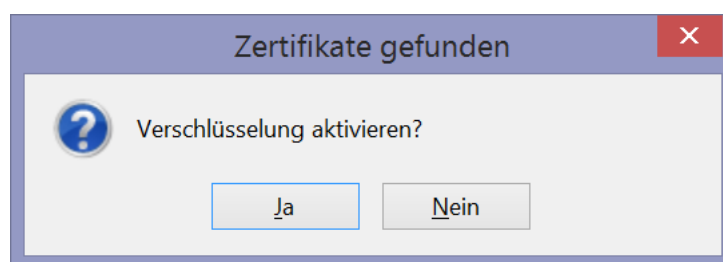
You wrote an S/MIME encrypted email with several BCC recipients.

The the following message appeared which has two flaws:

- It should not appear as long as I don't specify Enigmail to be used.
- No normal user understands this message (so I just clicked "Encrypt normally").



Then you get this message from TB:



==> A new version of TB integrating S/MIME and PGP should fix the user's uncertainty: Where does this message belong to? It should explain – maybe in the dialog's header – that its from TB and it's about S/MIME (not Enigmail or PGP). Suggestion for a new header's title: "S/MIME certificates found" = "S/MIME-Zertifikate gefunden".

Remark:

After I got such an Enigmail confirmation and sending it away as an unencrypted but signed S/MIME message some of the recipients complained that their umlauts were broken:

R=C3=BCcckblickend m=C3=B6chte ich

<==>

Rückblickend möchte ich

## 2.2. Different ways to activate/deactivate enc/sign properties and to see their status

### 2.2.1 The way of S/MIME

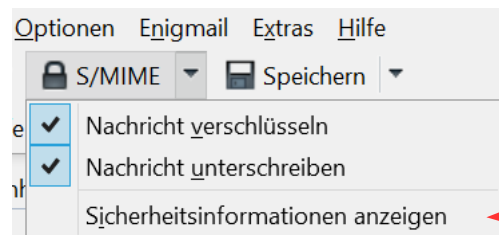
#### a) Activating the enc/sign properties

There is only one way to do so (compared to 3 ways with Enigmail):

--> The S/MIME button is always there in the 1st button bar in the writing window.

You have to select separately via menu encrypt and sign.

General properties can only be accessed in main window via the ≡ button (not here):



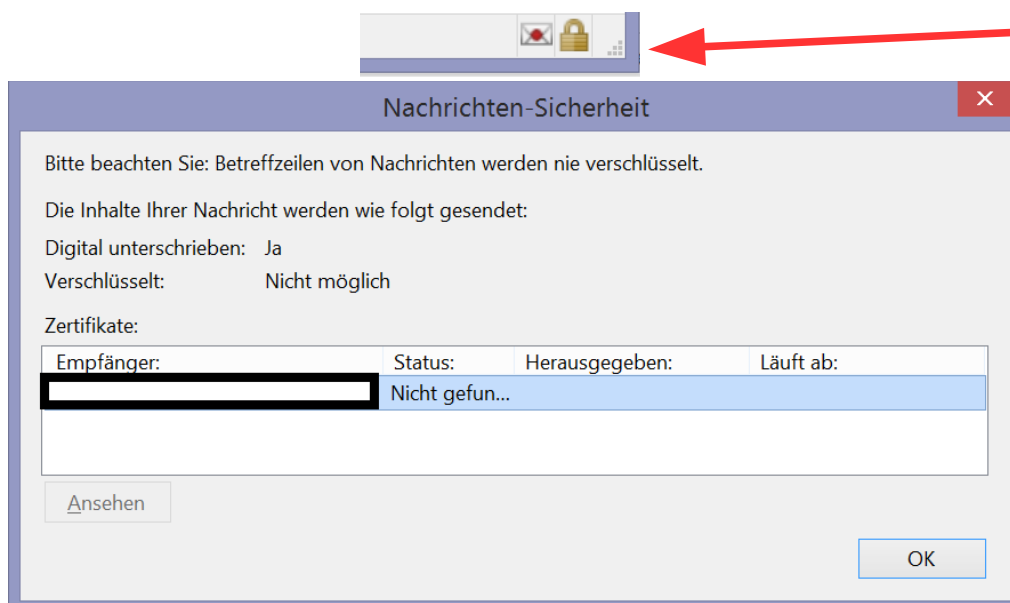
==> To change both, you need to do 4 clicks (pull-down, click encrypt; pull-down, click sign). Users who more often secure their emails want only 2 user interactions!

#### b) Status information

--> Icons in the normal status bar (at the bottom of the sending window) show whether enc or sign was activated.

Both icons can be clicked and then the same dialog is opened as when above clicking the menu item "Sicherheitinformationen anzeigen".

==> **Suggestion:** A better user experience would be if you can toggle with a mouse click the activation / deactivation of enc and of sign (grey means it is deactivated); and a context menu (right mouse click) for the button should show the security information.

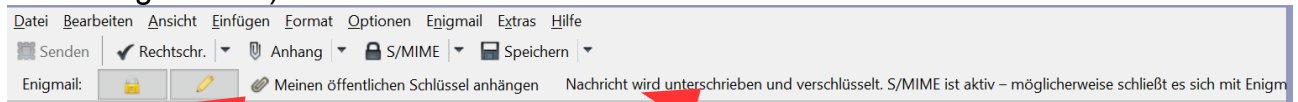


## 2.2.2 The way of Enigmail

### a) Activating the enc/sign properties

There are three ways to do so:

(1) Via the additional 2<sup>nd</sup> button line for enc/sign and status info (always visible in the writing window)



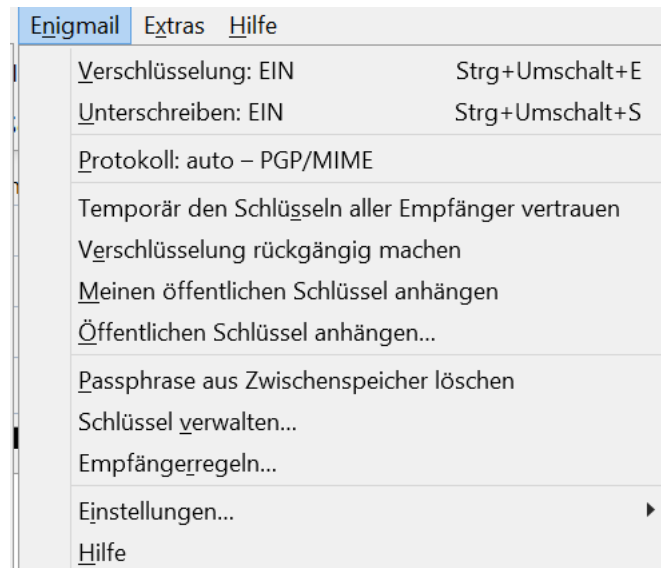
Push to activate,  
yellow if active

Status field:

- Click doesn't show the whole message text even if truncated → Bug!
- Click shows a window with the Enigmail sending options.

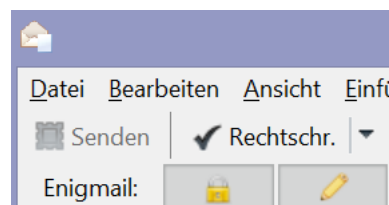
(2) Via menu (visible in main TB window only via Alt, and always in writing window)

(3) Via keyboard shortcuts



### b) Status information

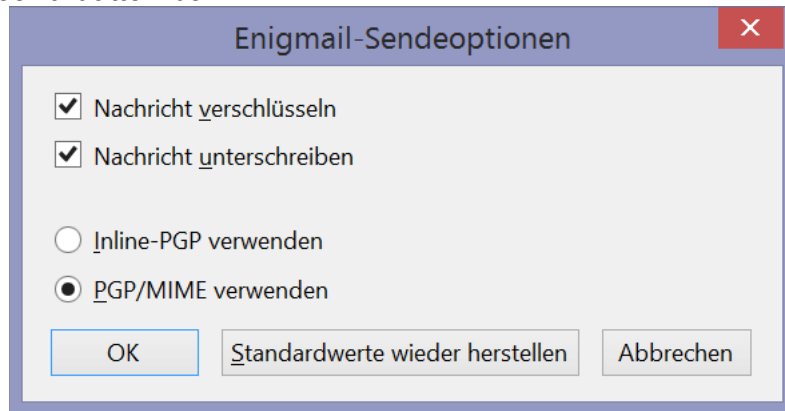
--> Color of the icons in the additional 2<sup>nd</sup> button line of the sending window. No entry in the normal status bar. Clicking doesn't open a dialog, but toggle the according property (enc or no enc; sign or no sign).



==> This should be unified! Currently, new users are very confused.

### Just for information:

This is the window with the **Enigmail sending options** which you get when clicking into the *status field* [see the screenshot below the headline 2.2.2 part a)] behind the Enigmail buttons in the second button bar:



## **2.3. Conflicting parameters – PGP is overruled, lower security might be used**

Scenario: If you have the S/MIME property sign activated (which is my default):  
And then you write a sensitive message for which you select PGP enc and sign.

==> The result is, that S/MIME dominates and sends out an unencrypted email.

==> This can be dangerous. At least the user should be warned, that the program will apply only the S/MIME property.

**This very obviously shows that there is a real need that the two mail security standards S/MIME and PGP should be implemented internally (aka within TB itself) and in a coordinated manner!**



## **2.4. Sending an email to recipients with different key types – from the user's perspective**

### **2.4.1 Coexistence and both-support – Request 1**

This is an advanced topic coming into reality when TB is to support both S/MIME and PGP.

After writing the text of a message you want to send the email to two users: to user A and to user B.

Scenario:

Your keystore has from A only a PGP key, and from B only an S/MIME key.

Then it should be possible, that TB deals like a wizard offering a much better user experience by

- informing the user about the situation,
- creating one session key,
- encrypting this email in OpenPGP format for user A, and another mail in CMS format for user B.
- sending out two emails.

It would be great if in addition this could be shown later in the Sent window as one email.

### **2.4.2 Coexistence and both-support – Request 2**

Maybe, in the future a common keystore could exist as the public keys could be extracted from both and TB knows what key and format is used with which email security standard.

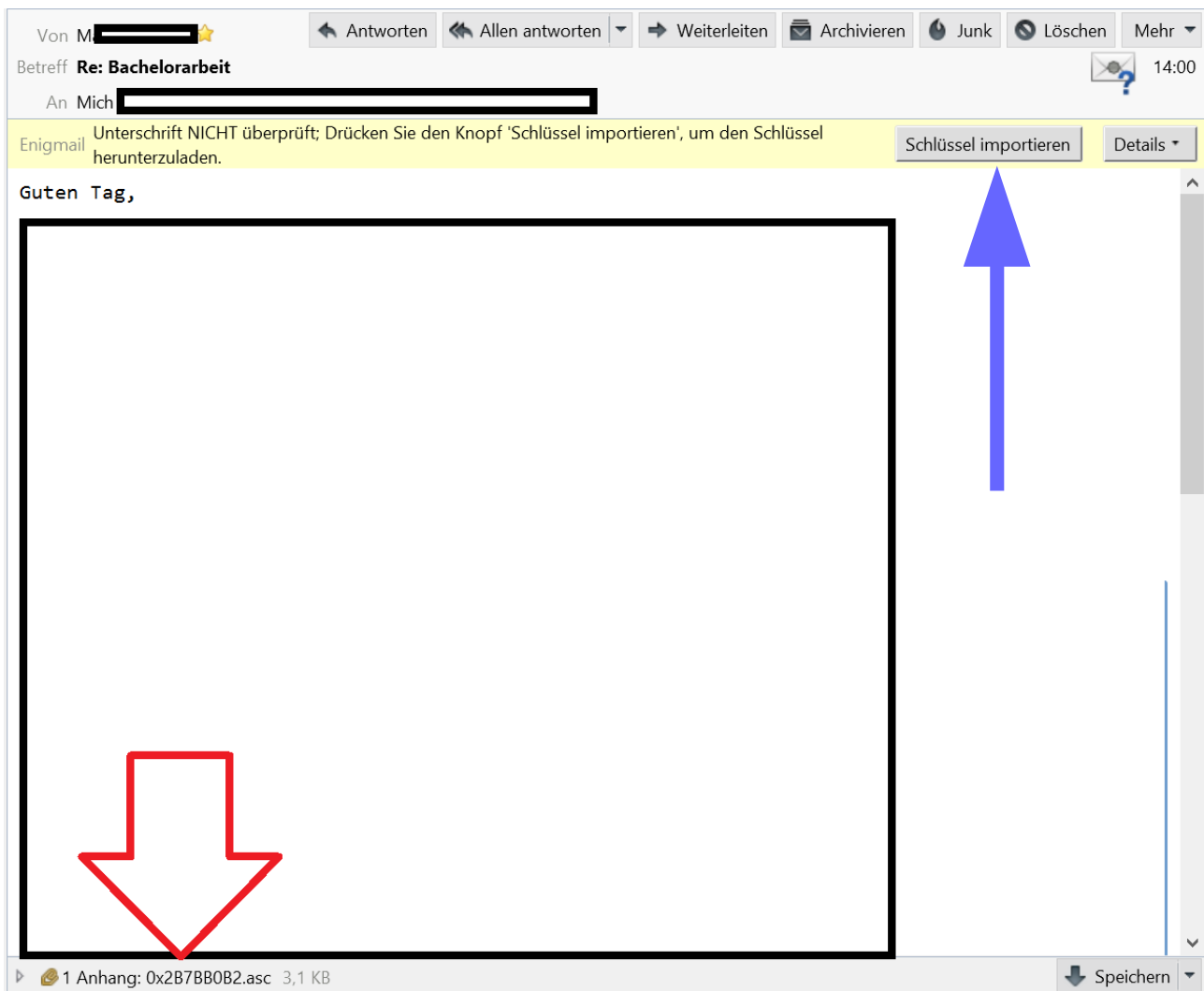
However, you only could transfer an S/MIME key into a PGP pubkey format, but not the other way around (as the S/MIME key has to be signed by a trustcenter).

Here more research and thinking has to be done to implement this properly.

### 3. Some Enigmail-only issues

#### 3.1. Scenario where the trust level isn't shown correctly, and the attached key isn't handled accordingly

Scenario: We get a PGP-signed email where the sender attached his PGP key.



a) When getting a signed email with the sender's key attached, Enigmail doesn't have the sender's pubkey in its keystore yet, and can't check the validity of the signature. That is ok.

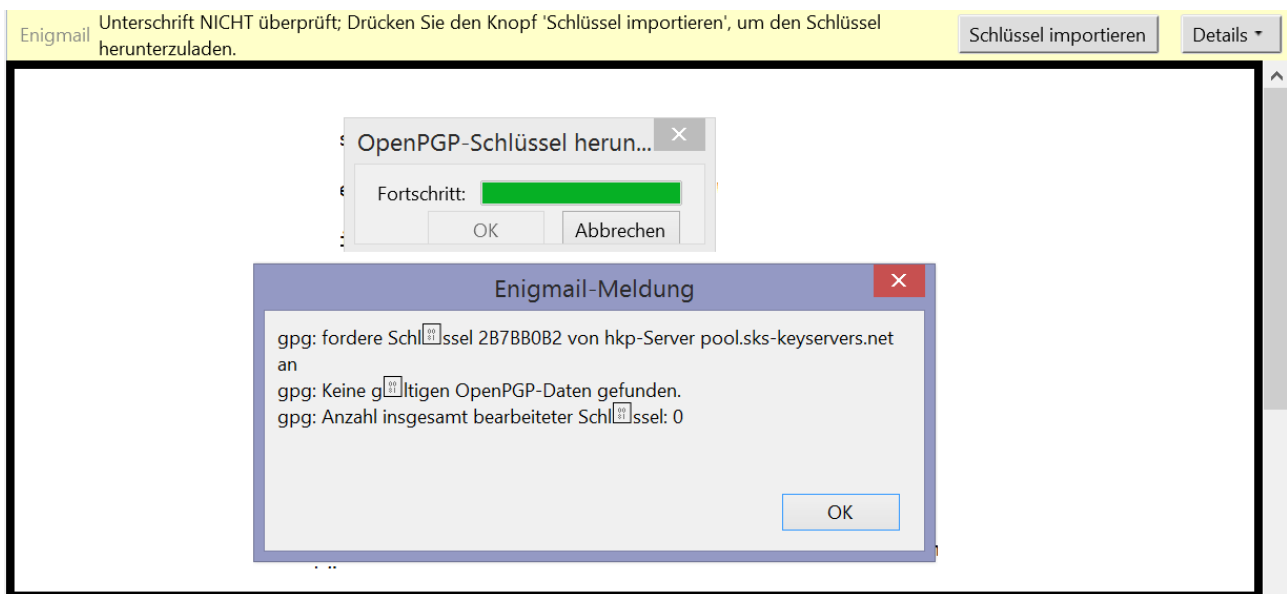
However, then it asks me to push the button “Import key” (“Schlüssel importieren”), in order to **download** the pubkey. It would be much more appropriate, to directly import the attached pubkey and check whether the sender is its owner? This is what the sender expects, when he attaches his pubkey.

b) After clicking the button "Import key", it shows the dialog "Select key server". And then it shows the following 2 windows: "Download OpenPGP key" and "Enigmail Message".

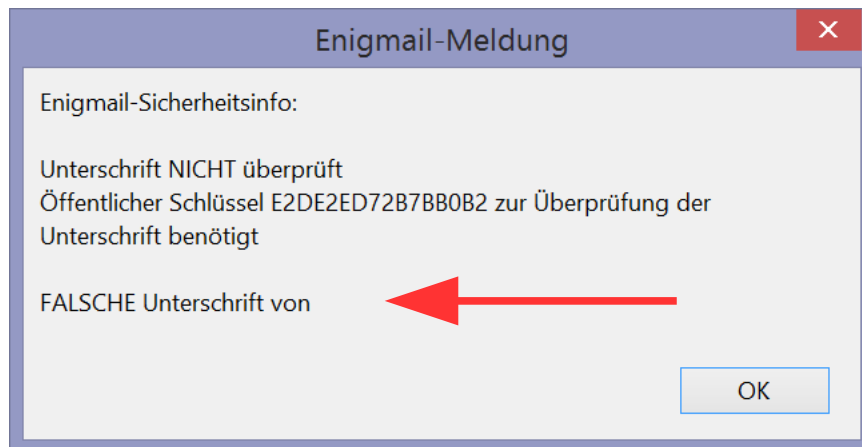
- The 1<sup>st</sup> dialog was too small.
- The 2<sup>nd</sup> dialog tells that there was no success to download the pubkey of the sender.

This was NOT what could be expected as the sender just did attach his pubkey because he didn't want to make it available at a key server. This is a decision which should be left to a sender using PGP.

→ So the described behavior is a bug in Enigmail.



c) Clicking on “Security information” we get:



---

Unterschrift NICHT überprüft  
Öffentlicher Schlüssel E2DE2ED72B7BB0B2 zur Überprüfung der Unterschrift benötigt  
FALSCHE Unterschrift von

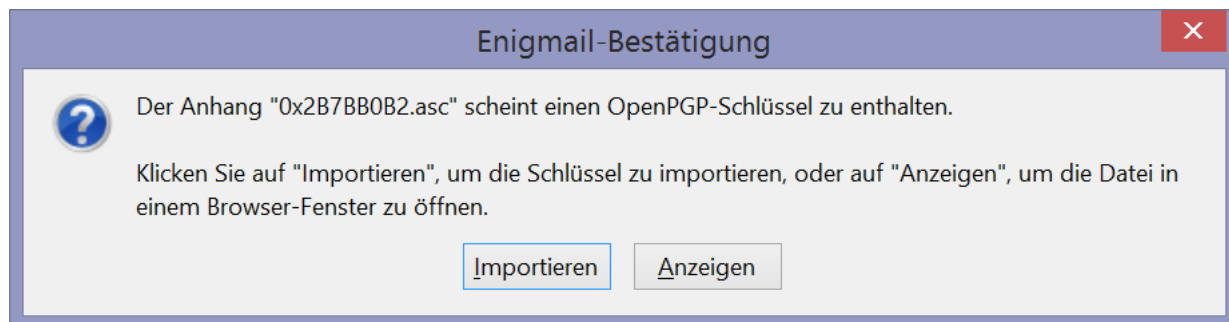
---

Why does it state at the end, that the signature is wrong – this is something it cannot state definitely.

Enigmail should state, it cannot validate the signature as it doesn't have the pubkey from the alleged sender? So the middle chapter (“Unterschrift NICHT ... benötigt”) is ok; the last chapter (“FALSCHE Unterschrift von”) is wrong and – in addition – it appears to be incomplete.

And a pure formal thing: All complete sentences should have a dot at their end.

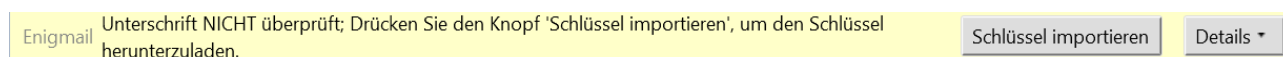
d) Now I double-clicked at the attachment, and it perfectly worked to import the attached pubkey into the PGP keystore.



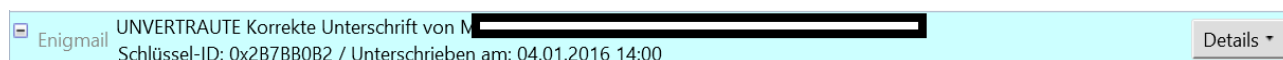
Again the formal thing: Some more umlaut errors.



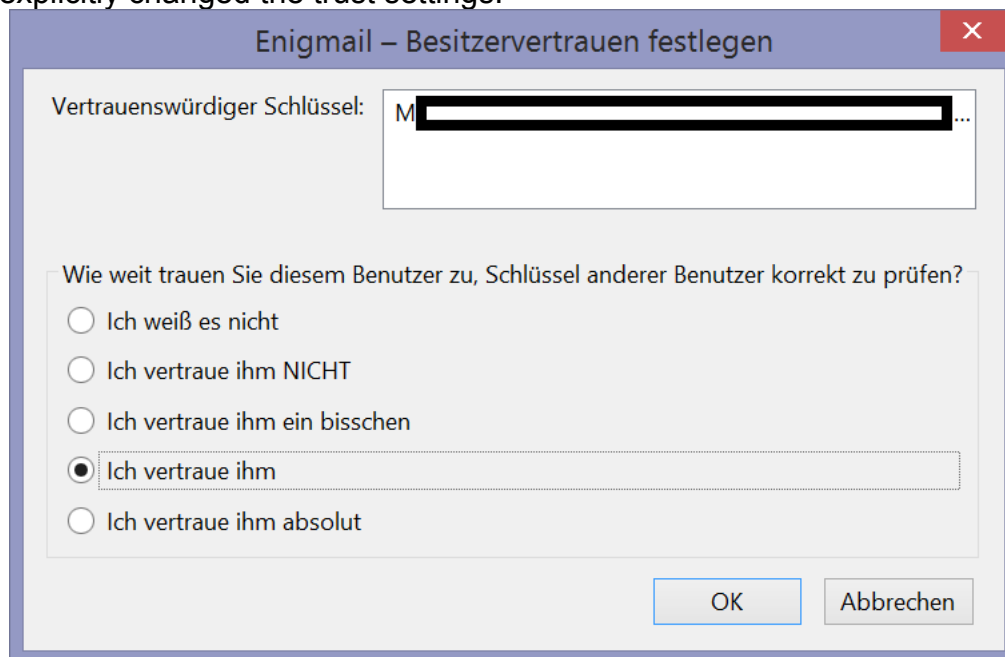
e) Besides having the key imported correctly I still see the yellow-based message, that the message hasn't been validated yet.



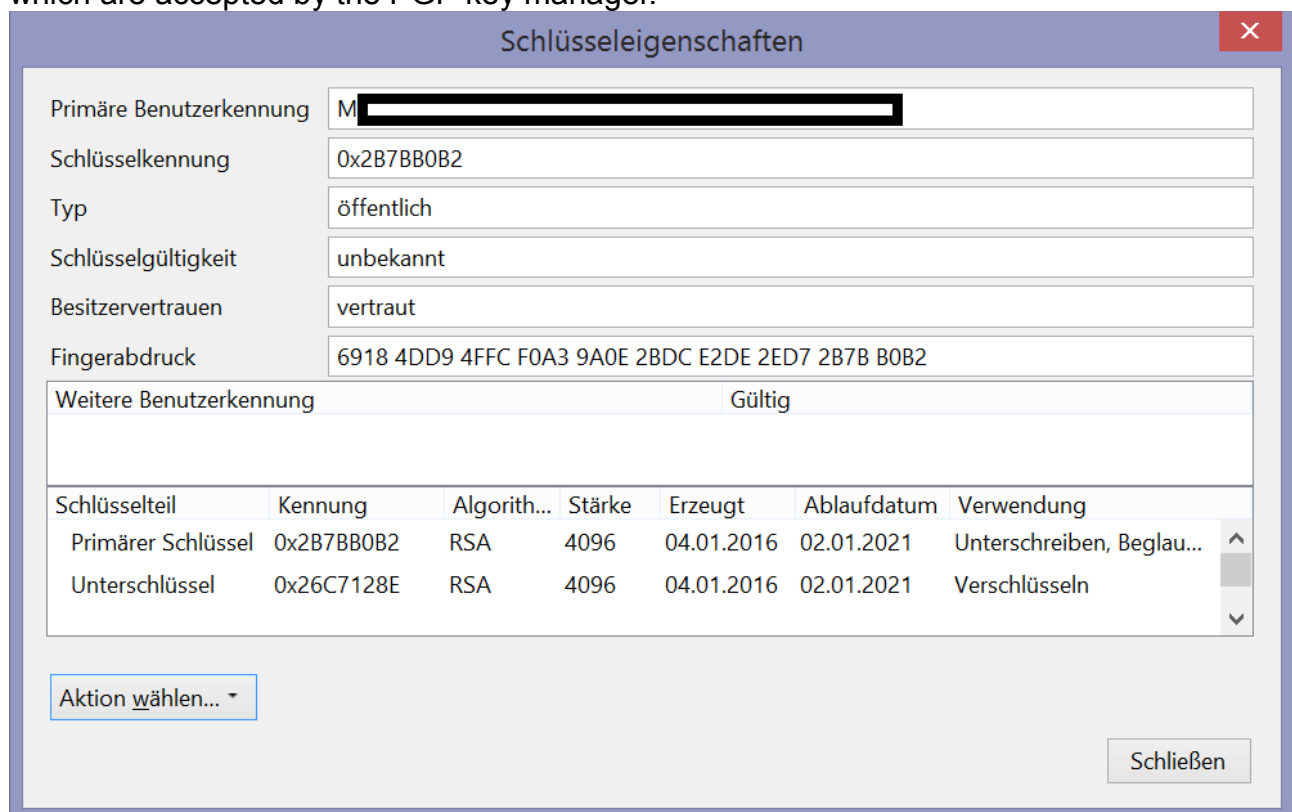
Then I shortly click on another email, and back to this one, which changes to the correct blue-based message: Signature ok, but not trusted.



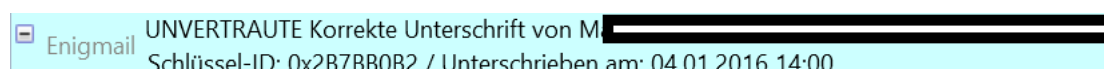
f) Then I explicitly changed the trust settings:



which are accepted by the PGP key manager.



Nevertheless, the email header continues to state "UNVERTRAUT":



## 3.2. Scenario where the trust level isn't shown correctly, and the attached key isn't handled accordingly

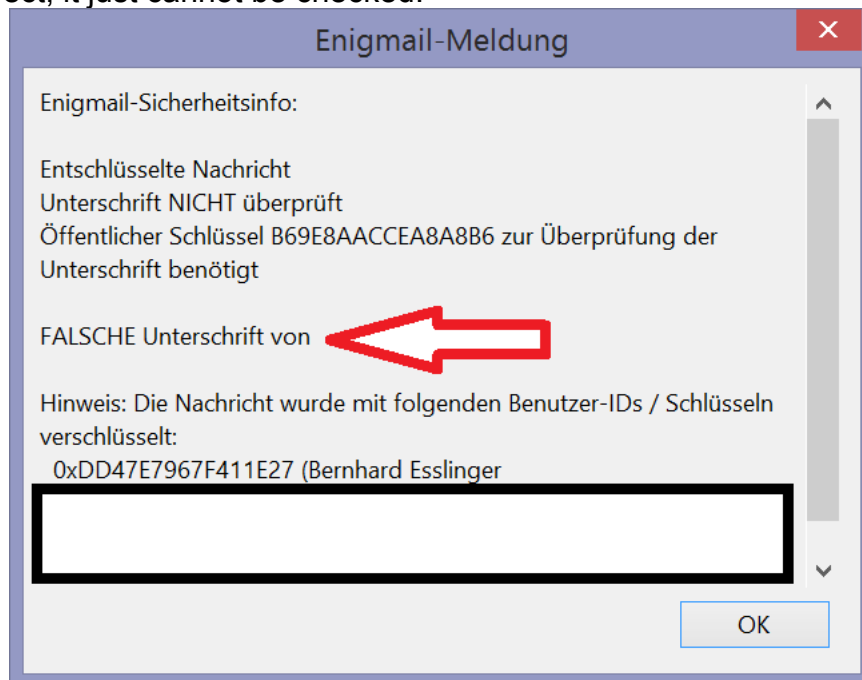
This is the same scenario as in chapter 3.1, however, before double-clicking at the attachment (chapter 3.1, part d) we tried the Enigmail menu.



### 3.2.1 Wrong messages after getting an encrypted email with the sender's pubkey attached

The difference to the scenario in chapter 3.1 is that here the received email was already encrypted for me.

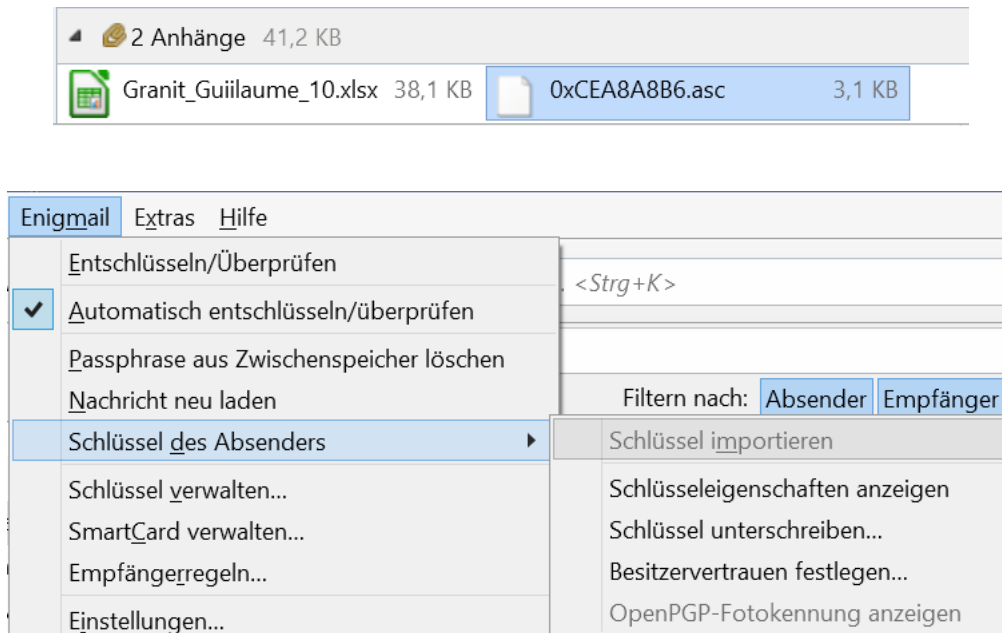
The dialog states, that the signature is wrong ("FALSCHE Unterschrift von "). That's not correct, it just cannot be checked.





### 3.2.2 Case where Enigmail menu entry “Import key” doesn't work correctly

Selecting the pubkey attachment (blue now) and clicking in the Enigmail menu on “Schlüssel des Absenders --> Schlüssel importieren”.



==> Nothing happens.

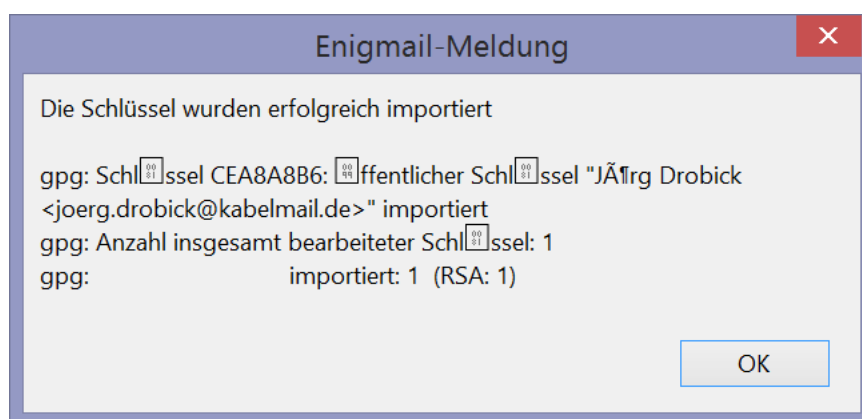
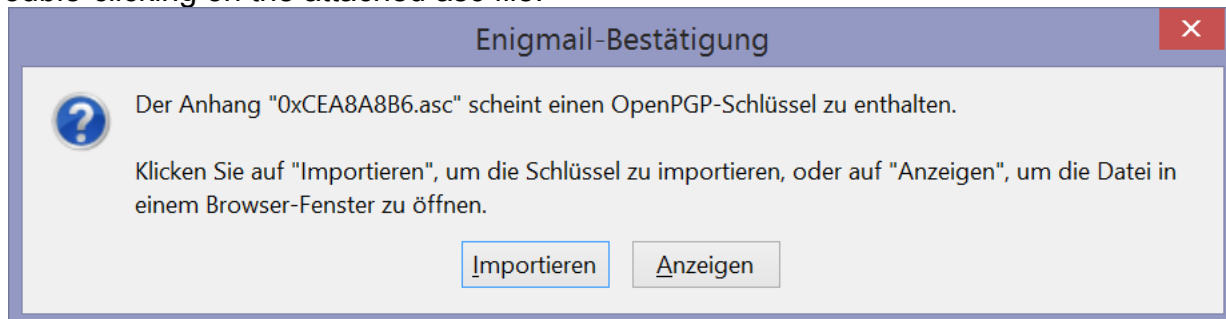
### 3.2.3 Case where Enigmail menu entry “Decrypt / Verify” doesn't work correctly

Selecting the pubkey attachment (blue now) and clicking in the Enigmail menu on “Entschlüsseln/Überprüfen”.

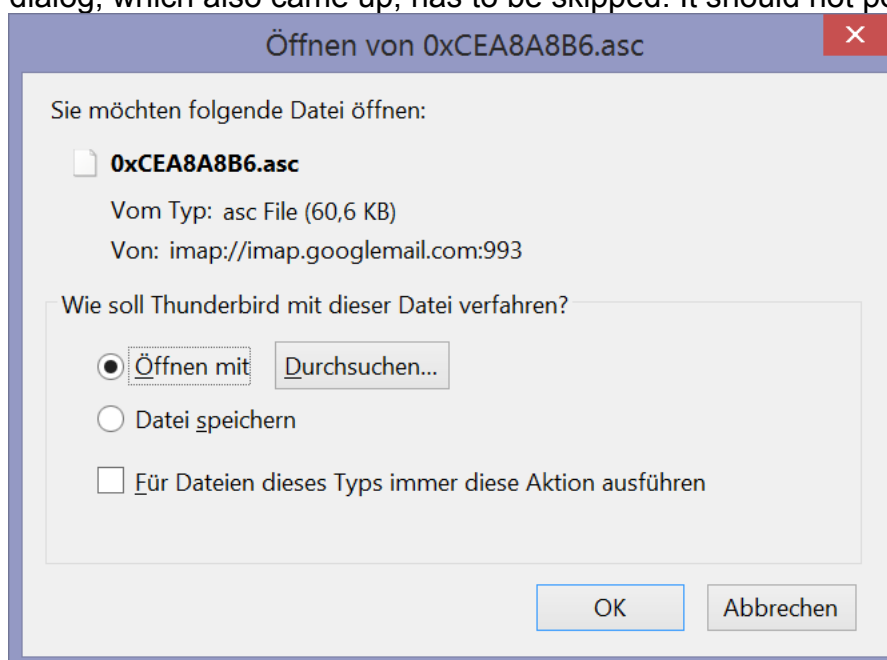
==> Nothing happens.

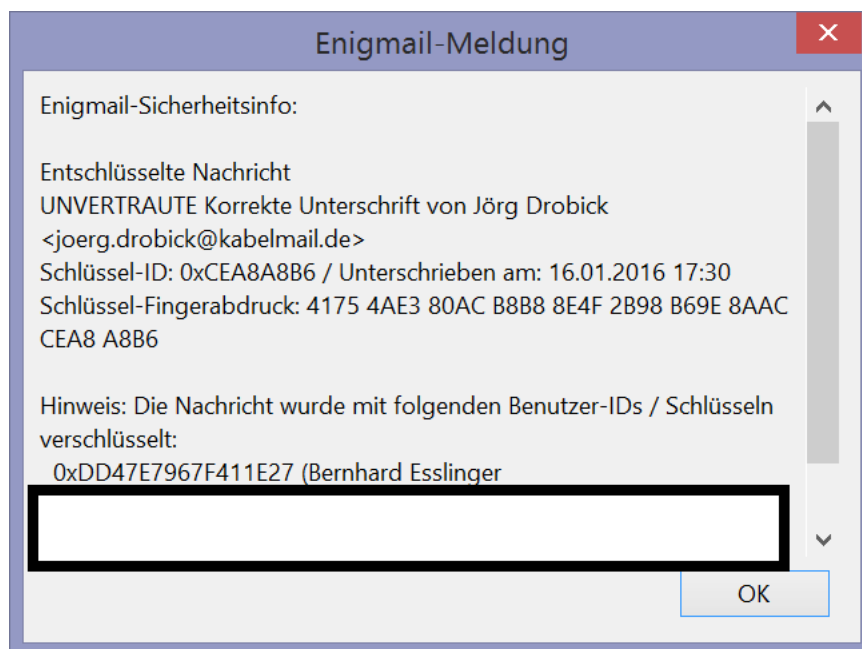
### 3.2.4 Double click on the attached pubkey works fine, but some texts are misleading

Double-clicking on the attached asc file:



The following dialog, which also came up, has to be skipped. It should not pop up!





Then the color at the message header within TB changes from yellow to blue, which is ok.

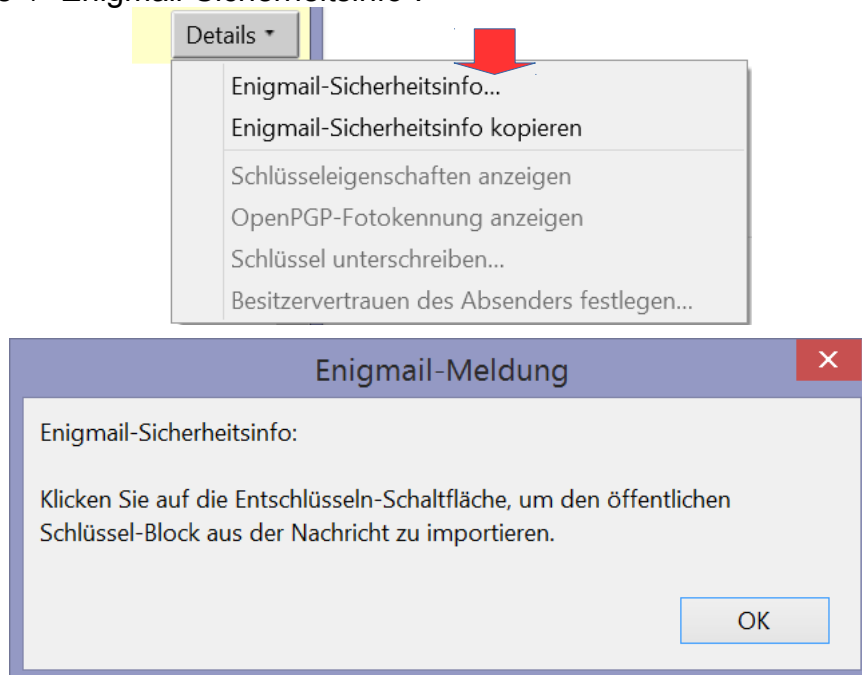


```

gNud6IFjU+fsyJc0/4FgoiCZU2BRyNsPDVrv9ADbIdEVKS6rd+rDUhCI3neTPGnJ
UWftwVa5YLwwYKmrVICwDZe83E38yLrXc42CQyf8GxpnX1/NI+rhnUenGh4qXspZ
tsThnRpHqy1as1I/YvxMp+/r/hXa5QGI0vHNABEBAAG0LFVscmljaCBLdw5pdHog
PHVscmljaC5rdW5pdHpAZGVpbmUtdGFsZXIuZGU+iQE4BBMBAGAiAhsDAh4BAheA
BQJVVIw8BgsJCACDAgYVCAIJCgsEFgIDAQAKCRAHTr1joDBd9X8iCACXnZ8C9rzC
ejtDo0Z90BWqFdVA/1SdfPZ1KMno+ws9xDblqe0FSyRNMiq9KdQ5U8vBh19TtsYh
CWtsQ1unGW8kEmkvZDNFTvy7kNhc5zL8RKQqpCx2sGF1mNv4Ngk4F44BCW0DQ54
4xKChq4J2CdzB8I8d8kpzEHEyWBJ7P0Kq/QQLe8G6KCTt/Kgje9FugMECmVTaDHD
Cf/RL/93rcg6DDZ+W2CGa4iJqr+qcJWI4HUWfh+HBwTV6xWLRfVVRjZvuRbdvffQ1
ryYYwwW12VBQ9qrW907XgM8ZiyU/rLSI9Hx0lrUDEd0zix1nSxyXDMX08MDzx+2g
Cmt/zhnjYJQutDSVbHJpY2ggS3VuaXR6IDx1bGkua3VuaXR6QGdtYWlsLmNvbT6J
ATsEEwECACUCGwMGCwkIBwMCBhUIAgKCKwQWAgMBAh4BAheABQJVVIw0AhkBAAoJ
EAdOvW0gMF31XCcIAJYP33ew1pJfRq6R5SQmGUcm/3FZ1J0EqbaMQdERihF60L7s
6sJI2unLK67aSBXqxxs/8tfBJQK4uqQ2siRUqBHUNYPd+pNheybY8c6e75GSR9zh
mwfvC7DtC4JGyfuFqu0JlQCCXtiEC3Wn12j+vjwNGpeuiaEyVa2Qgm1rxukqFU6J
vG1yZidnHirYImNwikKfODNoiXF5BETxVS9oEiWtCi6Als/C/knPlio01WIXBKbp
ZrI4DBxEo4EH/70xE1T64lykgERg5bKqW7kjKZGbHaC74aSCFidDKTLDDas2z19l
WJrwRL6VfLQB269bmtcIZ4gXkahjRMOc4s+sMK+5AQ0ESAnSdAEIALh/nxhANKqC
9b96vMrI/xtxdDSVbGeovbfffent4gTgZuvjI0k9tNDYUqBwqHB0/mucrlwSLGv1w1
qHbTgYqrm/PPorz9fqHJKD00BZV9aFvcxn5LRa+8Z3SQfKF9E0/JJ5vQS4aILu76
v+xLMYI953fFyzKA5Ma51leKWPEfkJbAvky1WRiuZW69UTM24+RZc41/Fe08LUa1
BR0L5bDqzYPSf/8IgQ+j/S8/uiyVbExxIbjvyuqehKLdfoxf/zCPdESjAwzM2Utf
iFhbfeolCPJ3zLI5Vxepcv3V6DaKzms+FdFa38Y1PmsHhBQNZeovQnBXLtu4jyuI
40fVKKH7YUAEQEAAyKBHwQYAIACQUCSAnSdAIBDAKACRAHTr1joDBd9WKfB/9C
mBoc1AQZtyGkQ9npwZ55RxLI5x64sZSTB1Yikf1LudThz3Chm3MvRNTOVAmiqmr
gnAowNftwZezvL+sw3PCQxY4uug+Nky6jn0Kg9ae9DS3jzRMJD61m8bmCMAS47h
xh83nvTraZo0aBKYPxgy120XpXSymANCMbfmyGNF7wLrXjZ39P6QzomVXqJ8w96
+akAArmZ1DxC1h085ufc67U2GMOjixf28sdabv963gANDIsTYYYeow/VpNkx+n5S
9MuPeITWS/iZxeilmc2kBXLotUAiLcLJdT2tR3C11v9C9bfZCCCTPYkGypxGmrn1
Jn0h4F0UEgkB6j8PJIPR
=1vYX
-----END PGP PUBLIC KEY BLOCK-----

```

b) The yellow mail header states to click a button “Decrypt”. Same info via the drop-down control “Details” / “Enigmail-Sicherheitsinfo”:

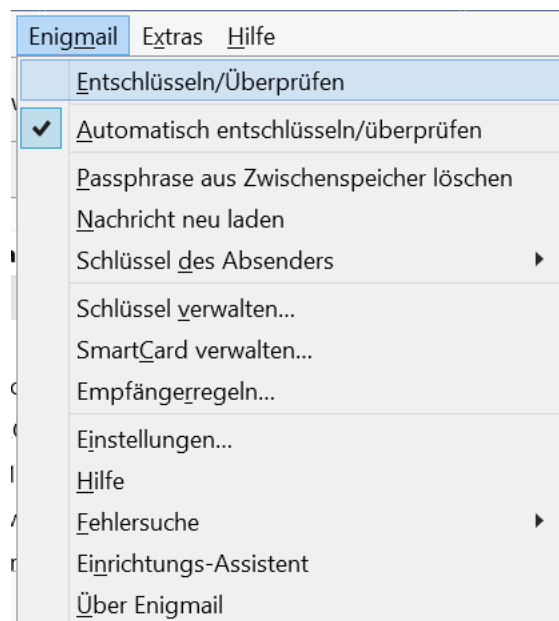


Remark:

The three dots after “Enigmail-Sicherheitsinfo” have to be deleted, as you just can click on ok.

c) It is NOT obvious for a normal user what to do now:

- Many users do not know that they can use Alt at their keyboard to alternate viewing the menu bar. This 1<sup>st</sup> point may be not the developers' fault.
- However, the 2<sup>nd</sup> point is an error:  
You have to click on the first menu entry in the Enigmail menu.  
But the text says click on the button “Encrypt / Verify” (Schaltfläche = Button).
- And it should specify the name of the menu item in its exact way:  
“Klicken Sie im Enigmail-Menü auf den Eintrag “Entschlüsseln/Überprüfen”, um den öffentlichen Schlüssel-Block aus der Nachricht zu importieren.”



### **3.4. Offer comment to each PGP key added in the keystore**

Another requirement which has nothing to with the scenario above – it's not important, but it would be nice in the long run to have a fix:

For each key available in the keystore there should be a comment field. Some standard records should be added by Enigmail / PGP by themselves like “Pub key received as file attachment”, “Pub key downloaded from key server xyz”, ...

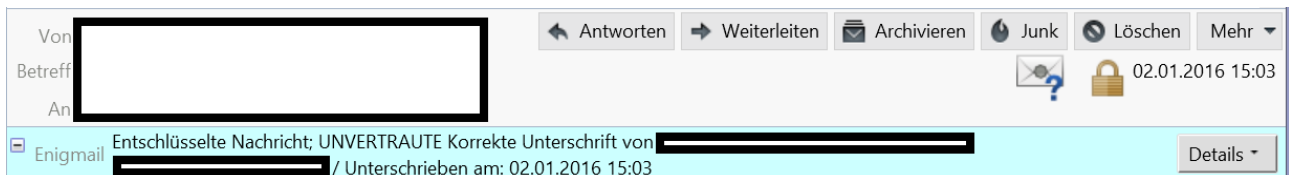
### **3.5. Offer as default: Send PGP-signed emails (like in S/MIME)**

- a) Have an option to send PGP signed as default.
- b) Have an option to add the public key (certificate) as default.

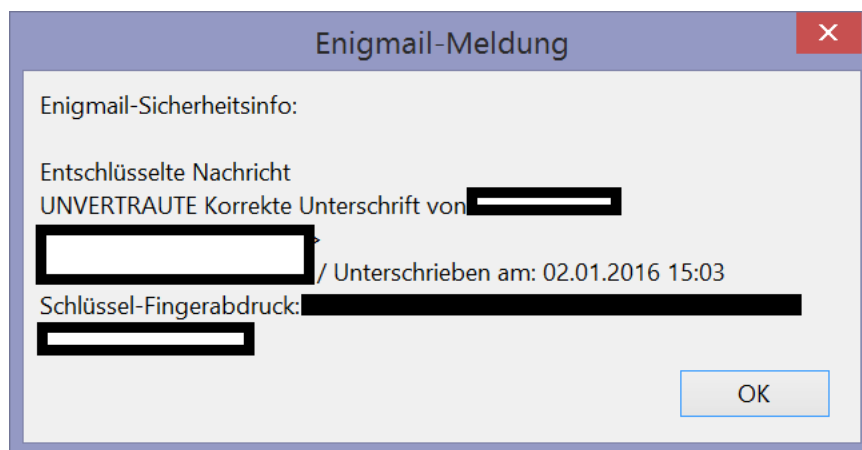
This saves new recipients to look for partner keys in a key server.

### 3.6. Sometimes signatures and keys are UNVERTRAUT besides I spent user trust (maybe my fault)

This is the header of a received email:



If I click to the question mark at the seal I get:

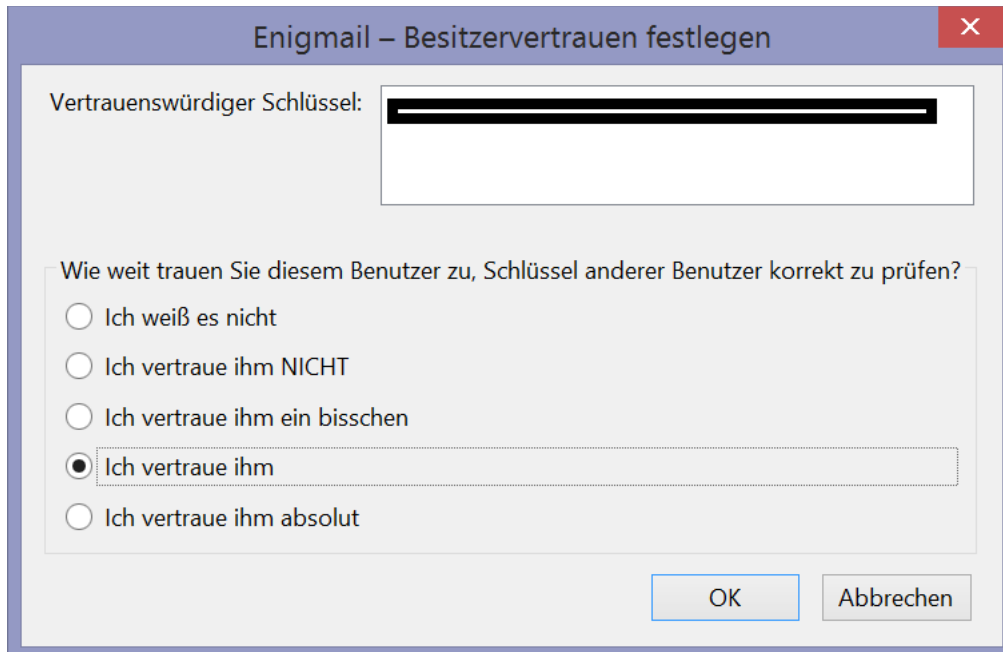


Remark:

I'd like to be able to mark and copy all the texts within a field.  
Within the pale blue field one only can mark the 2<sup>nd</sup> line.



If you click on "Details" and request more information, you can see that the "Ich vertraue ihm" (= "I trust him") is active.



Enigmail – Besitzervertrauen festlegen

Vertrauenswürdiger Schlüssel:

Wie weit trauen Sie diesem Benutzer zu, Schlüssel anderer Benutzer korrekt zu prüfen?

☐ Ich weiß es nicht

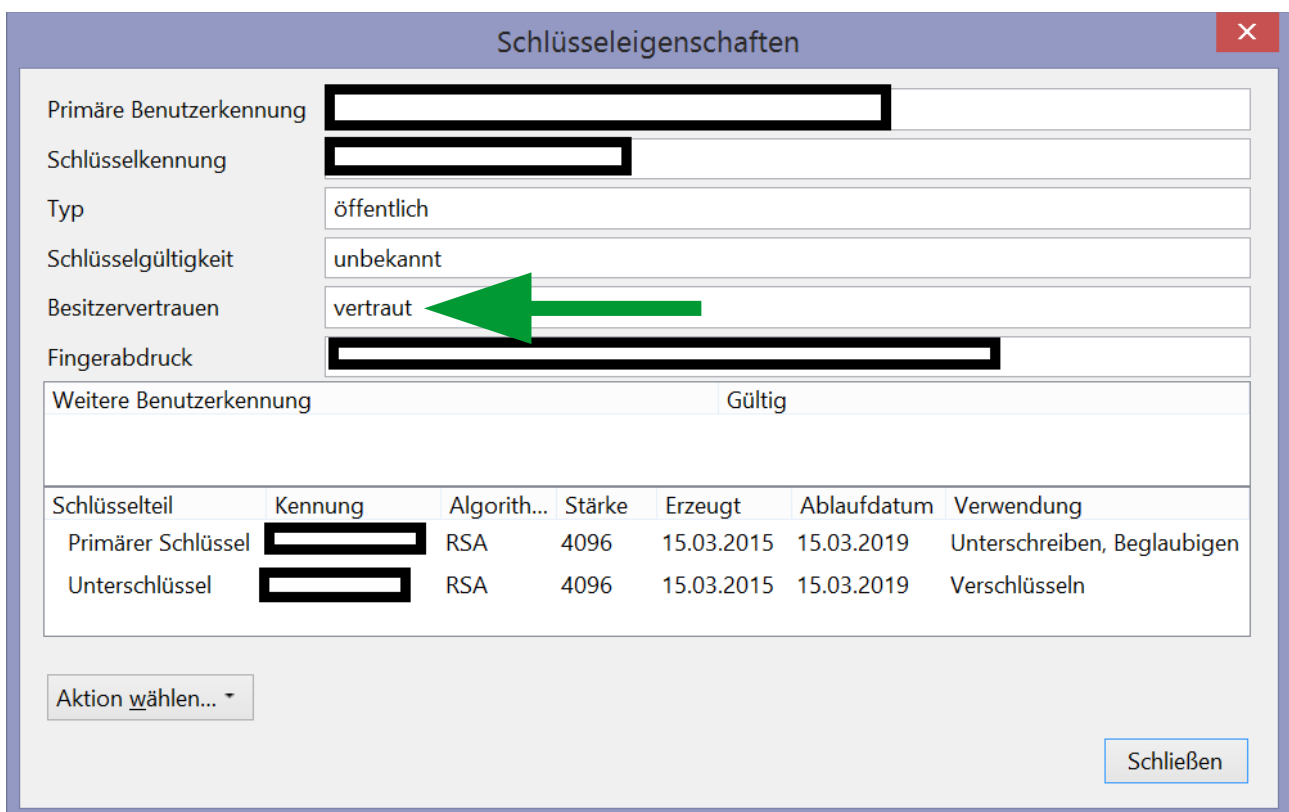
☐ Ich vertraue ihm NICHT

☐ Ich vertraue ihm ein bisschen

☒ Ich vertraue ihm

☐ Ich vertraue ihm absolut

OK Abbrechen



Schlüsseleigenschaften

Primäre Benutzerkennung

Schlüsselkennung

Typ öffentlich

Schlüsselgültigkeit unbekannt

Besitzervertrauen vertraut

Fingerabdruck

Weitere Benutzerkennung		Gültig				
Schlüsselteil	Kennung	Algorith...	Stärke	Erzeugt	Ablaufdatum	Verwendung
Primärer Schlüssel	<input type="text"/>	RSA	4096	15.03.2015	15.03.2019	Unterschreiben, Beglaubigen
Unterschlüssel	<input type="text"/>	RSA	4096	15.03.2015	15.03.2019	Verschlüsseln

Aktion wählen... ▾

Schließen

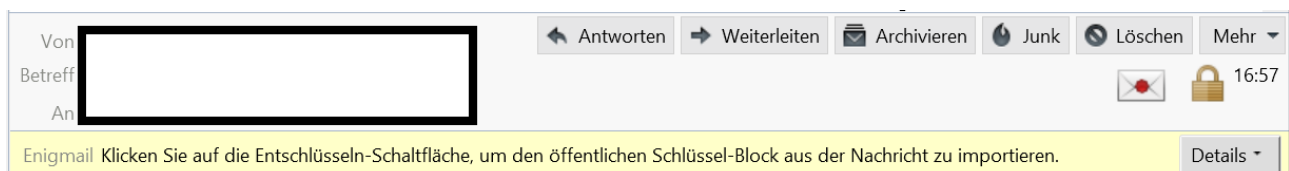
Remark:

For "user trust" (= "Benutzervertrauen") it should NOT be necessary to sign the pubkey in addition.

### 3.7. Received S/MIME message contains a PGP key as attachment

Scenario: You get an email, encrypted with S/MIME, which has a PGP key as attachment.

- a) Does it make sense, that Enigmail looks into an S/MIME encrypted email?
- b) More serious: The Enigmail hint in the yellow area is misleading: Where is the decrypt button (Entschlüsseln-Schaltfläche) mentioned?  
(I guess Enigmail meant the menu entry "Entschlüsseln/Überprüfen) after pressing Alt in order to get the Enigmail menu item in the main window?)

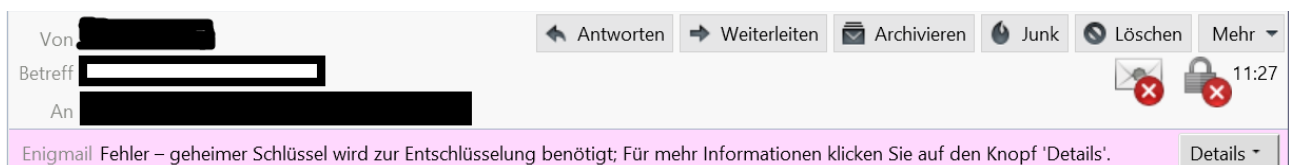


### 3.8. After receiving a PGP-encrypted email you did not enter the key at once

Scenario: You received new emails but did not enter the PGP key.

The message then has a header like the one below: Wouldn't it be nice to offer a "Decrypt" or "Enter key" button which asks for the key again?

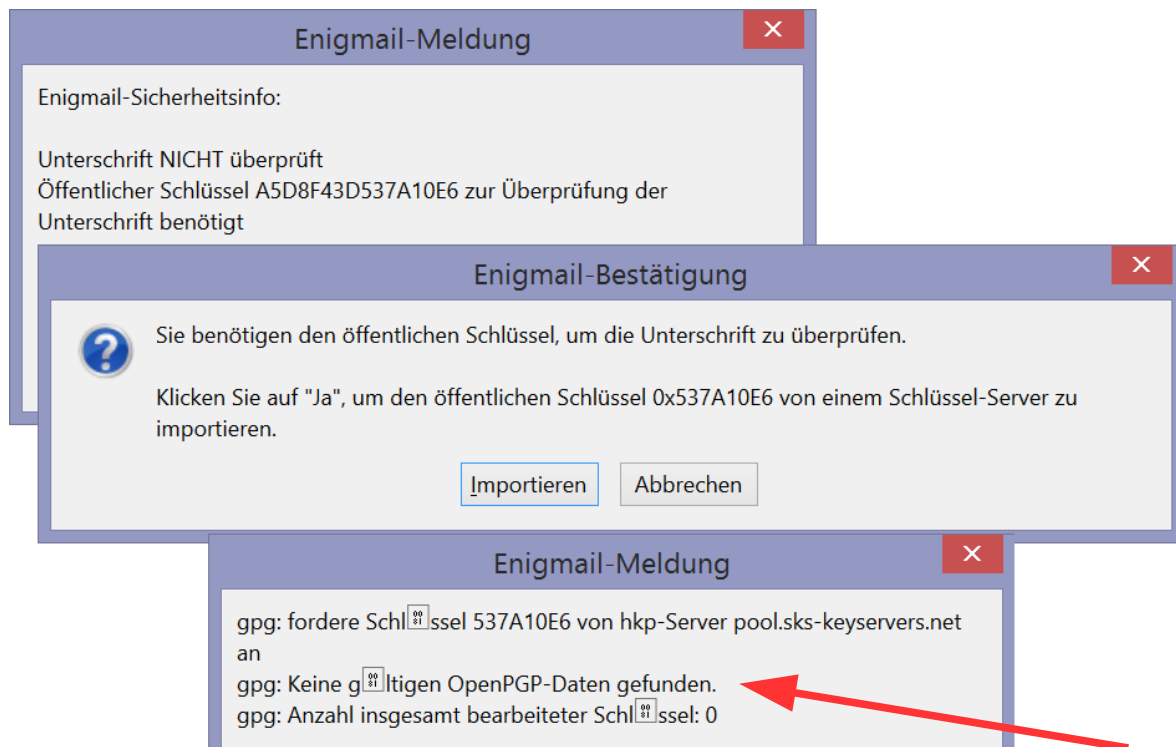
The only way I found to deal with this was, to click on another email, and then click on this email again: Afterwards you automatically get the key entry dialog.



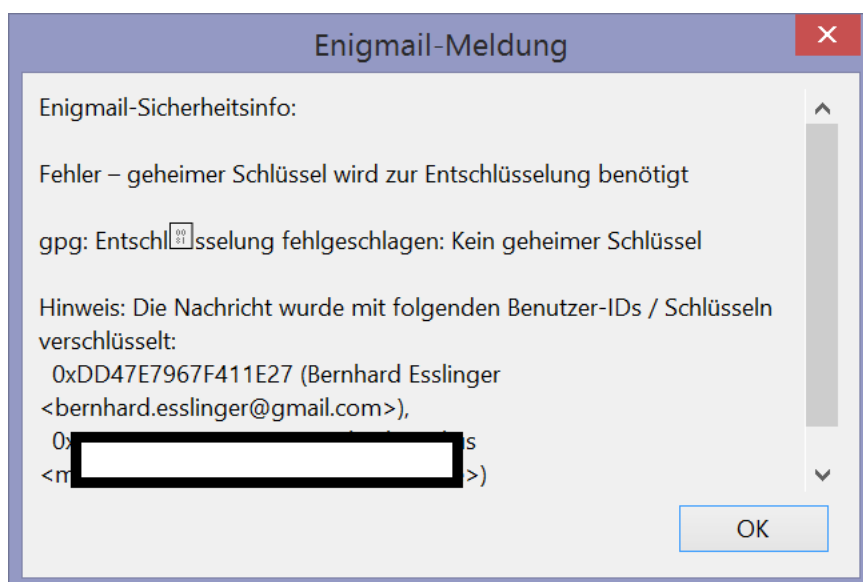
**==> Enigmail should be integrated within TB and no further plug-in or add-on should be needed.**

### 3.9. Umlaut problems in some Enigmail triggered dialogs

This is annoying and makes users think the software isn't mature.



Another example ( "ü" sometimes is shown correctly, sometimes not! ):

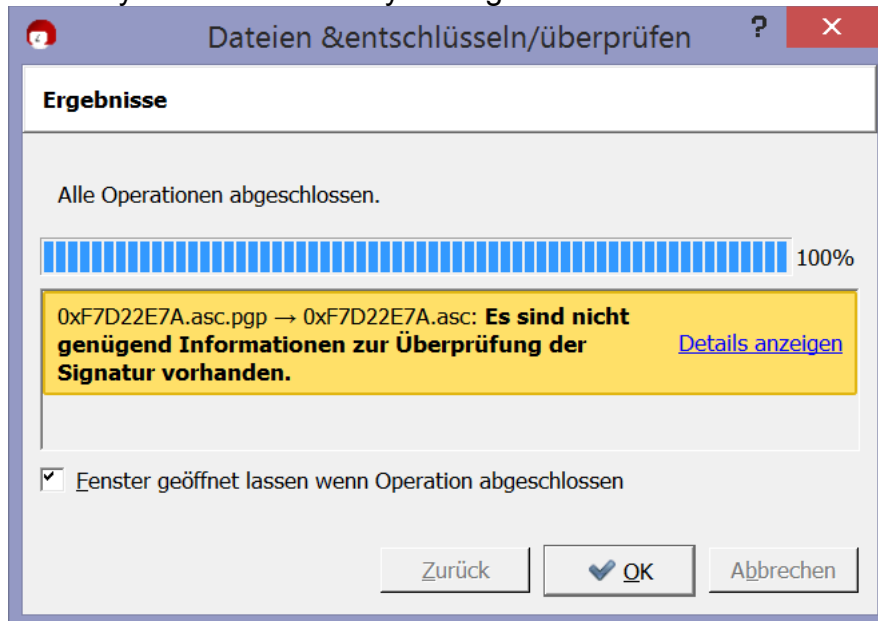


Fehler – geheimer Schlüssel wird zur Entschlüsselung benötigt  
 gpg: Entschlüsselung fehlgeschlagen: Kein geheimer Schlüssel  
 Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:  
 0xDD47E7967F411E27 (Bernhard Esslinger <bernhard.esslinger@gmail.com>),  
 ...

## 4. Appendix

### 4.1. GnuPG: User feedback in case of decryption

After entering my password and performing the decryption GnuPG should look into the PGP key store and say in more detail why the signature cannot be verified.



Clicking on “Details anzeigen” shows only that it cannot be validated, but not why:

