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 27th, 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)

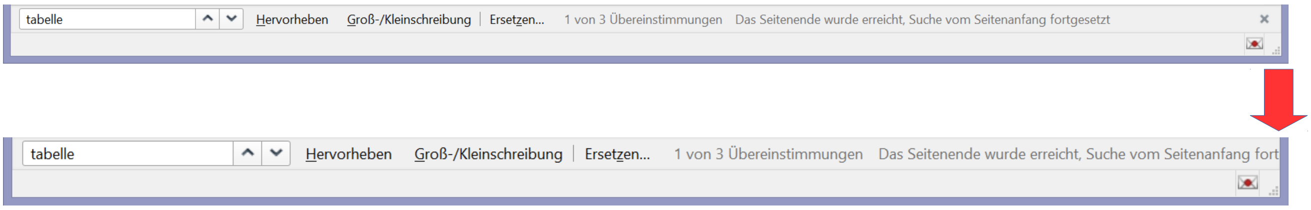
Content

1. Thunderbird solely

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.)



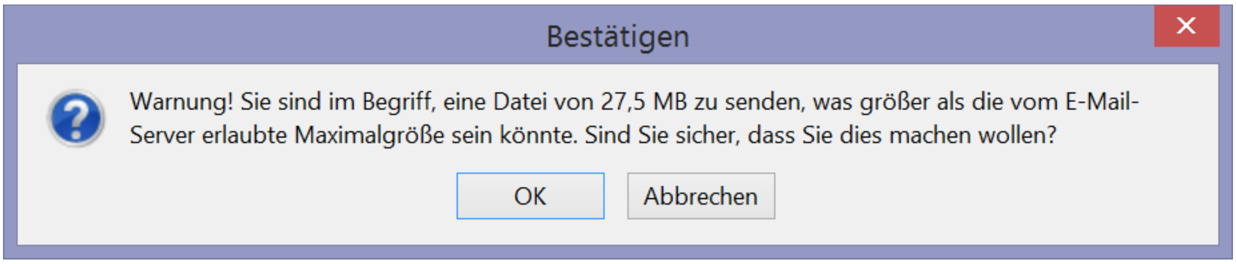
1 von 3 Übereinstimmungen Das Seitenende wurde erreicht, Suche vom Seitenanfang fortgesetzt

1 von 3 Übereinstimmungen Das Seitenende wurde erreicht, Suche vom Seitenanfang fort

1.2. Attachments too big. Warning but no advice

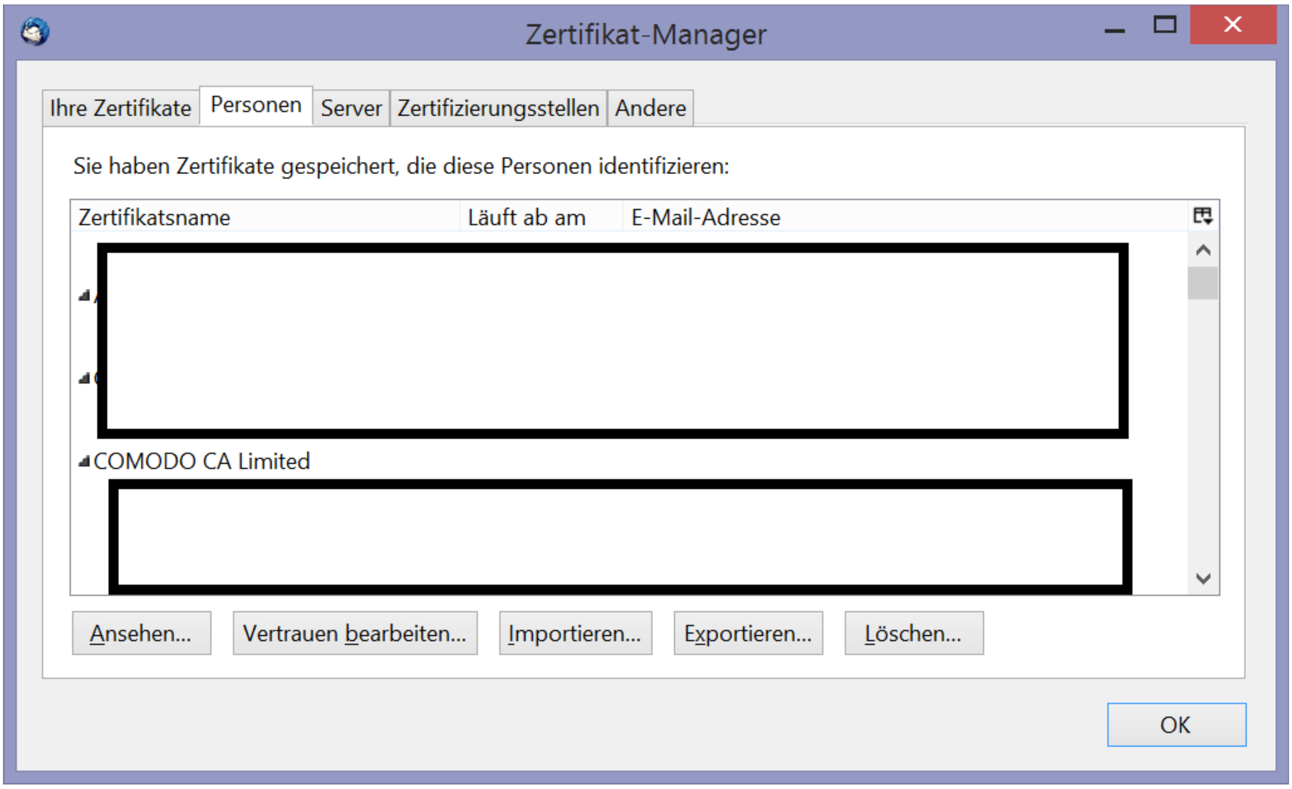
(This is no important issue, and independent of S/MIME.)

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



Warnung! Sie sind im Begriff, eine Datei von 27,5 MB zu senden, was größer als die vom E-Mail-Server erlaubte Maximalgröße sein könnte. Sind Sie sicher, dass Sie dies machen wollen?

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



Sie haben Zertifikate gespeichert, die diese Personen identifizieren:

Zertifikatsname	Läuft ab am	E-Mail-Adresse
[redacted]		
COMODO CA Limited		
[redacted]		

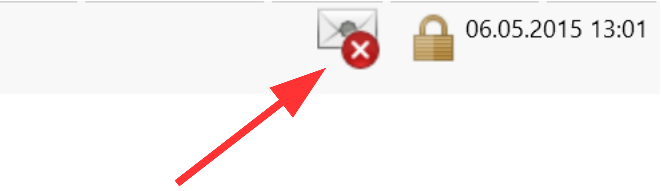
A search field is necessary e.g. if you want to know the reason why there is no valid certificate: Did the time of its validity period end, or do you have no certificate for this email address in your keystore?

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

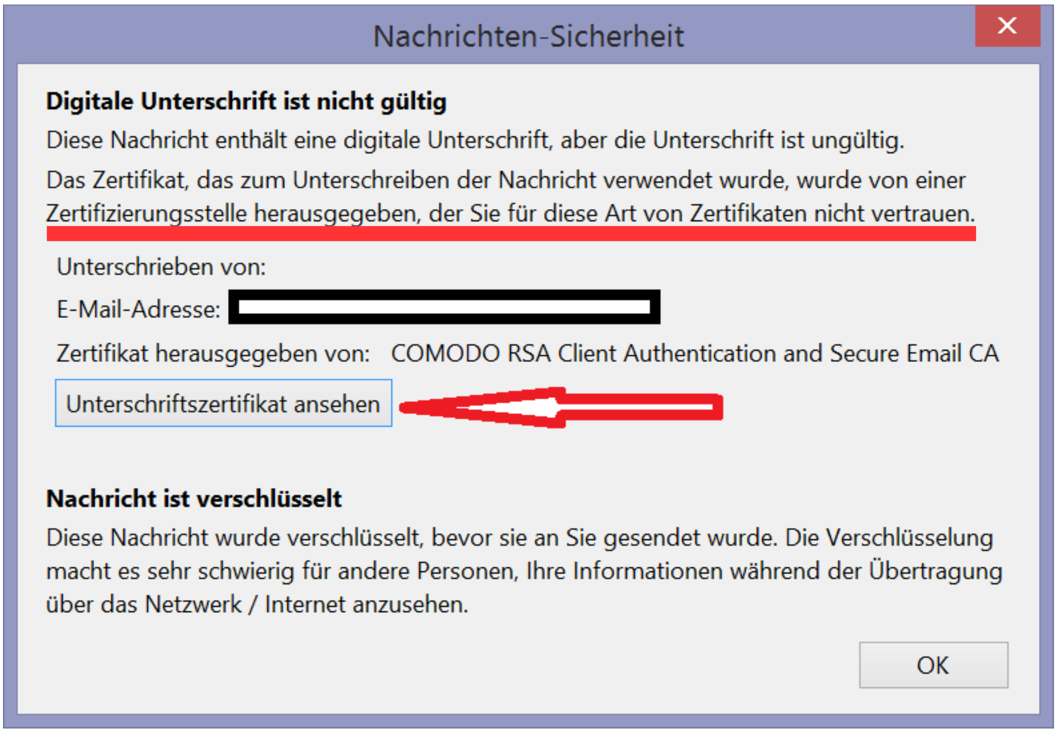
(This is an important issue from the user perspective when he wants to secure his emails.)

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.



Nachrichten-Sicherheit

Digitale Unterschrift ist nicht gültig

Diese Nachricht enthält eine digitale Unterschrift, aber die Unterschrift ist ungültig.

Das Zertifikat, das zum Unterschreiben der Nachricht verwendet wurde, wurde von einer Zertifizierungsstelle herausgegeben, der Sie für diese Art von Zertifikaten nicht vertrauen.

Unterschrieben von:

E-Mail-Adresse: [redacted]

Zertifikat herausgegeben von: COMODO RSA Client Authentication and Secure Email CA

Nachricht ist verschlüsselt

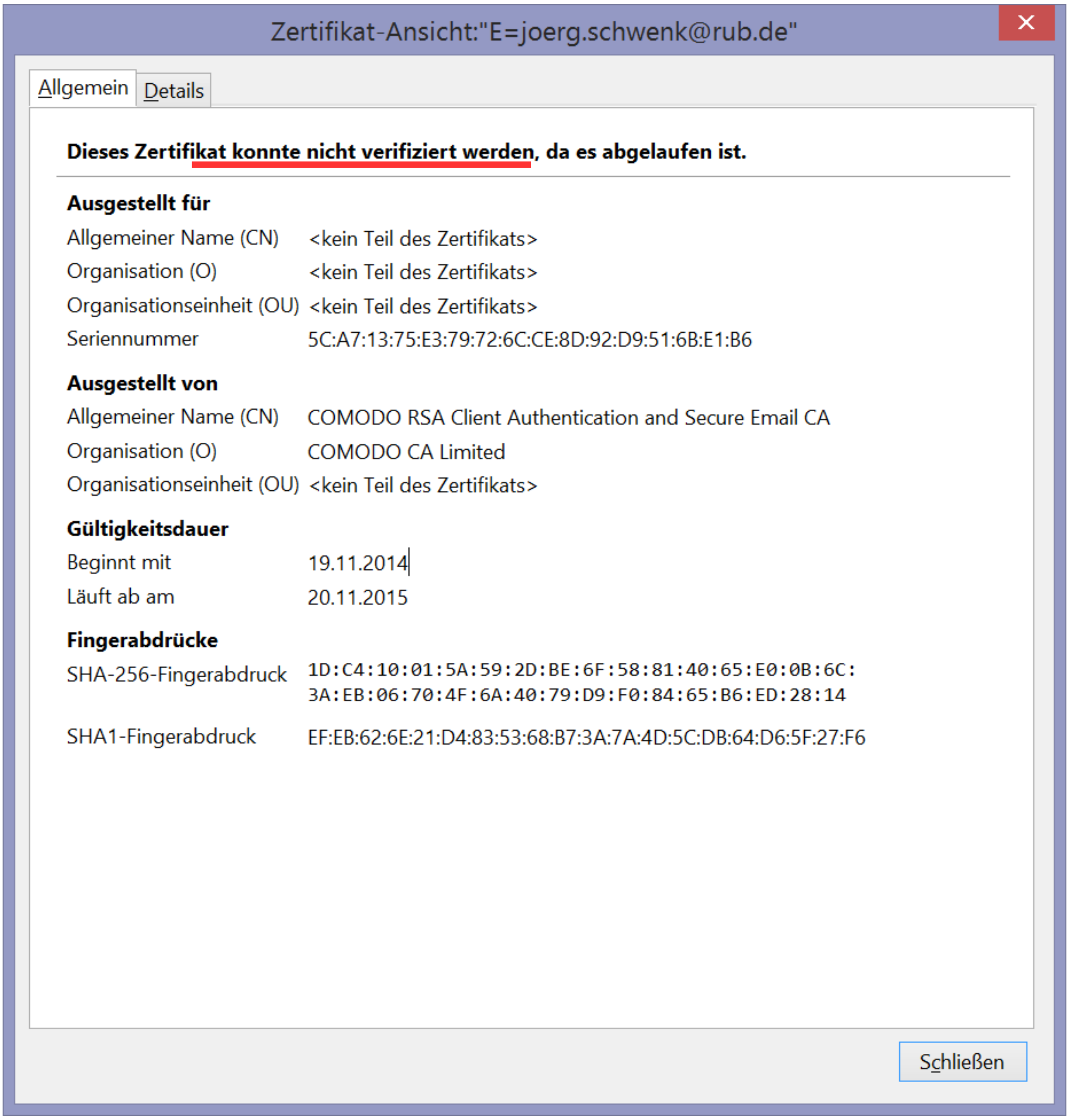
Diese Nachricht wurde verschlüsselt, bevor sie an Sie gesendet wurde. Die Verschlüsselung macht es sehr schwierig für andere Personen, Ihre Informationen während der Übertragung über das Netzwerk / Internet anzusehen.

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”.



Dieses Zertifikat konnte nicht verifiziert werden, da es abgelaufen ist.

Ausgestellt für

Allgemeiner Name (CN)	<kein Teil des Zertifikats>
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	5C:A7:13:75:E3:79:72:6C:CE:8D:92:D9:51:6B:E1:B6

Ausgestellt von

Allgemeiner Name (CN)	COMODO RSA Client Authentication and Secure Email CA
Organisation (O)	COMODO CA Limited
Organisationseinheit (OU)	<kein Teil des Zertifikats>

Gültigkeitsdauer

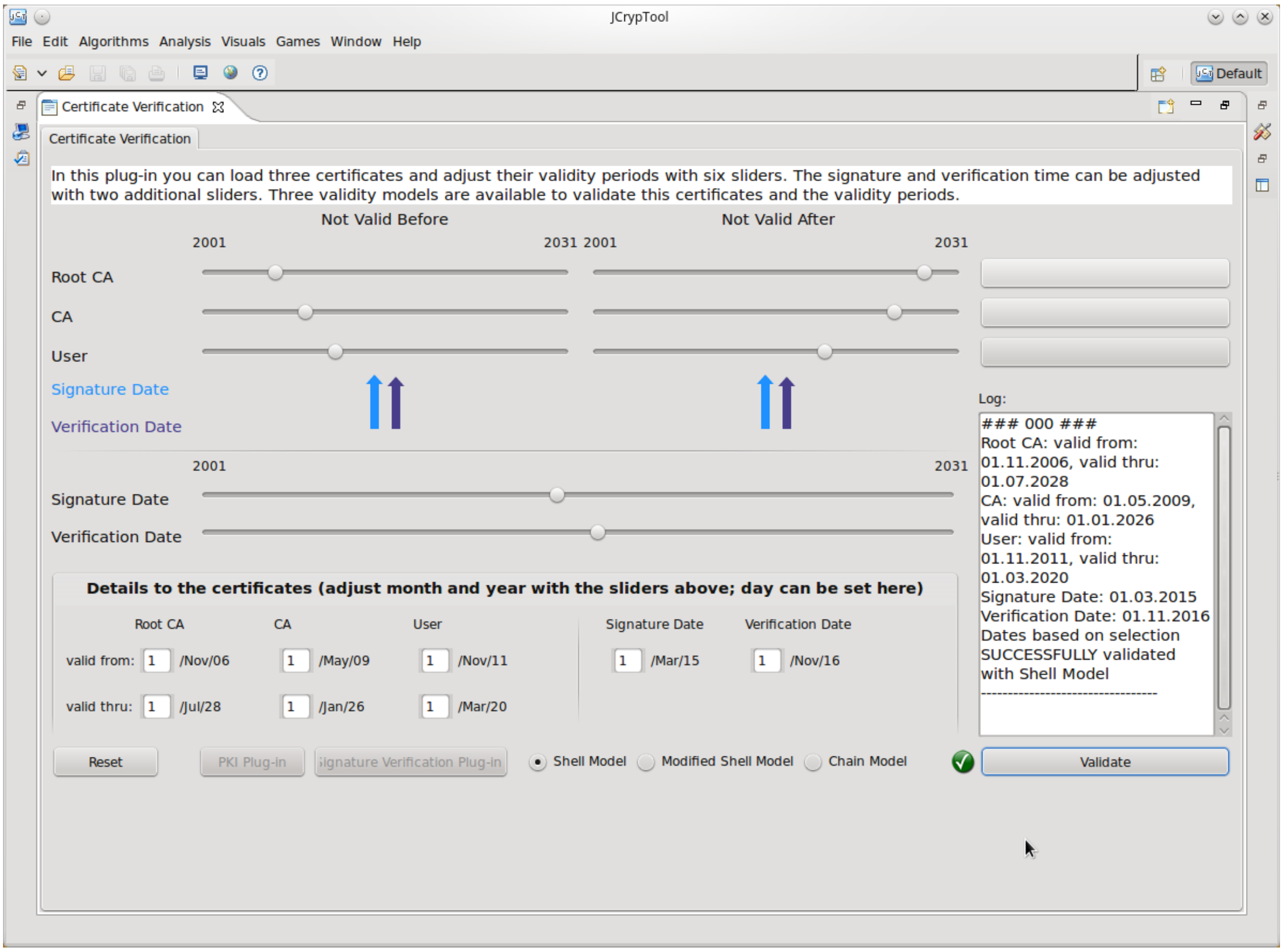
Beginnt mit	19.11.2014
Läuft ab am	20.11.2015

Fingerabdrücke

SHA-256-Fingerabdruck	1D:C4:10:01:5A:59:2D:BE:6F:58:81:40:65:E0:0B:6C: 3A:EB:06:70:4F:6A:40:79:D9:F0:84:65:B6:ED:28:14
SHA1-Fingerabdruck	EF:EB:62:6E:21:D4:83:53:68:B7:3A:7A:4D:5C:DB:64:D6:5F:27:F6

Just for information:

The e-learning program JavaCrypTool (JCT) from 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 Schalenmodel und Kettenmodell), and how you interactively can learn this playfully. S/MIME uses Schalenmodell = PKIX-Model = layer model.



In this plug-in you can load three certificates and adjust their validity periods with six sliders. The signature and verification time can be adjusted with two additional sliders. Three validity models are available to validate this certificates and the validity periods.

Details to the certificates (adjust month and year with the sliders above; day can be set here)

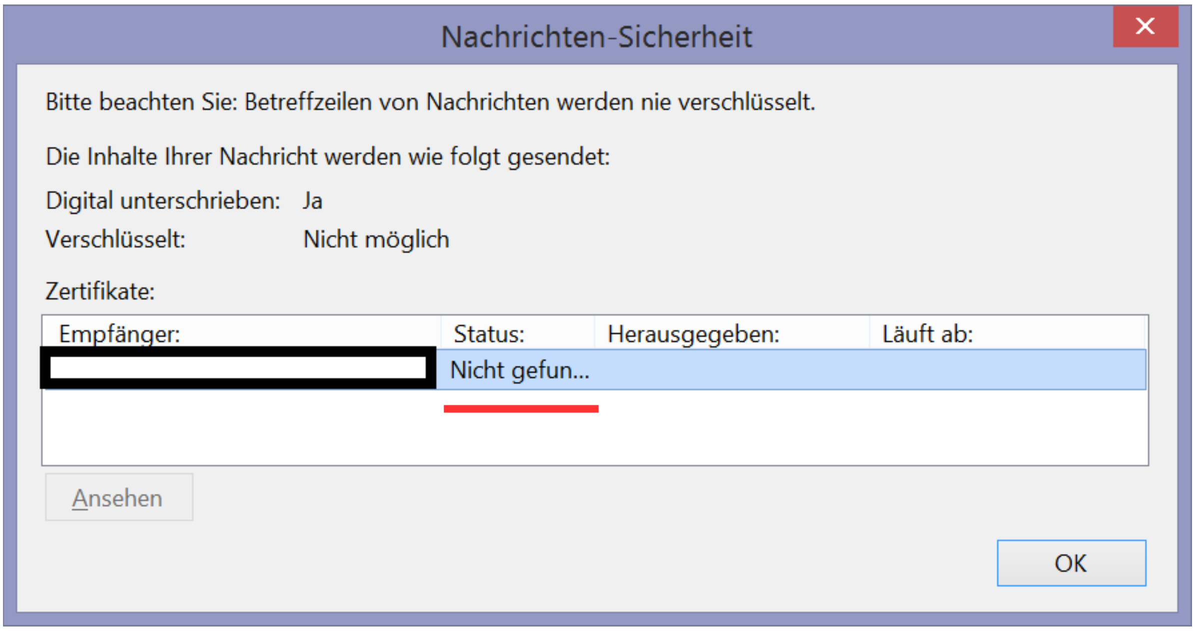
	Root CA	CA	User	Signature Date	Verification Date
valid from:	1 /Nov/06	1 /May/09	1 /Nov/11	1 /Mar/15	1 /Nov/16
valid thru:	1 /Jul/28	1 /Jan/26	1 /Mar/20		

● Shell Model ○ Modified Shell Model ○ Chain Model

```
### 000 ###
Root CA: valid from:
01.11.2006, valid thru:
01.07.2028
CA: valid from: 01.05.2009,
valid thru: 01.01.2026
User: valid from:
01.11.2011, valid thru:
01.03.2020
Signature Date: 01.03.2015
Verification Date: 01.11.2016
Dates based on selection
SUCCESSFULLY validated
with Shell 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”]:



Nachrichten-Sicherheit

Bitte beachten Sie: Betreffzeilen von Nachrichten werden nie verschlüsselt.

Die Inhalte Ihrer Nachricht werden wie folgt gesendet:

Digital unterschrieben: Ja
Verschlüsselt: Nicht möglich

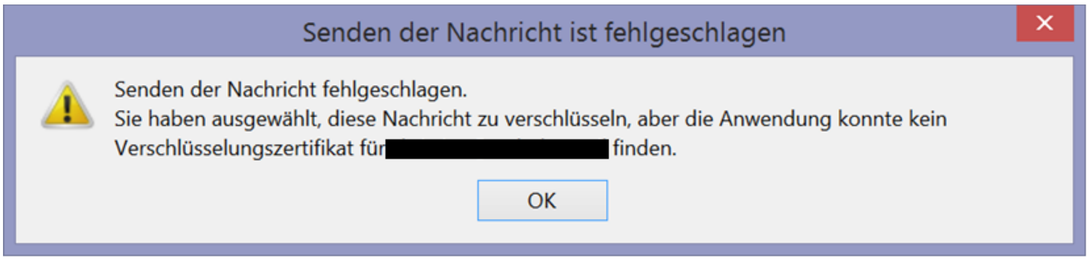
Zertifikate:

Empfänger:	Status:	Herausgegeben:	Läuft ab:
[redacted]	Nicht gefun...		

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.

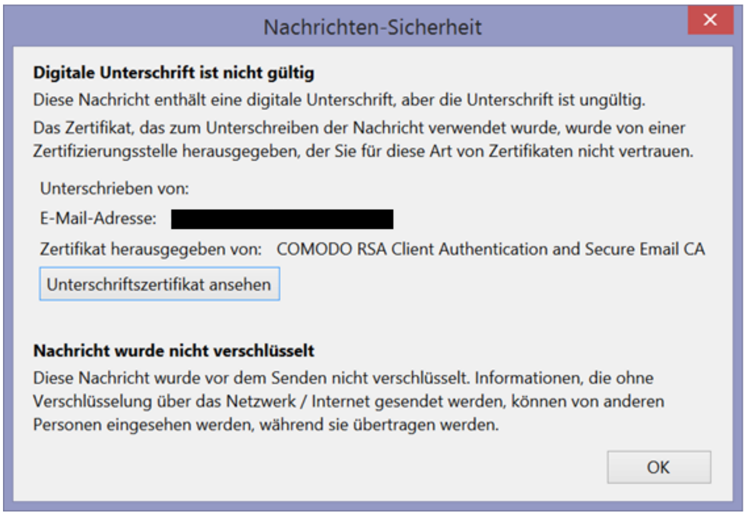
1.4.3 Certificate was revoked: No recommendation what the user should do

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.



Senden der Nachricht ist fehlgeschlagen

Senden der Nachricht fehlgeschlagen.
Sie haben ausgewählt, diese Nachricht zu verschlüsseln, aber die Anwendung konnte kein Verschlüsselungszertifikat für [redacted] finden.



Nachrichten-Sicherheit

Digitale Unterschrift ist nicht gültig

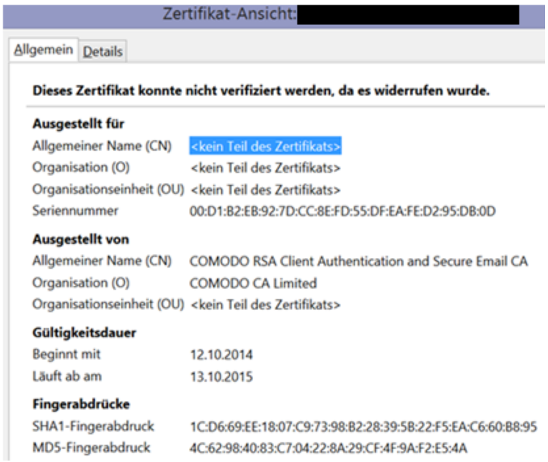
Diese Nachricht enthält eine digitale Unterschrift, aber die Unterschrift ist ungültig.

Das Zertifikat, das zum Unterschreiben der Nachricht verwendet wurde, wurde von einer Zertifizierungsstelle herausgegeben, der Sie für diese Art von Zertifikaten nicht vertrauen.

Unterschrieben von:
E-Mail-Adresse: [redacted]
Zertifikat herausgegeben von: COMODO RSA Client Authentication and Secure Email CA

Nachricht wurde nicht verschlüsselt

Diese Nachricht wurde vor dem Senden nicht verschlüsselt. Informationen, die ohne Verschlüsselung über das Netzwerk / Internet gesendet werden, können von anderen Personen eingesehen werden, während sie übertragen werden.



Zertifikat-Ansicht: [redacted]

Dieses Zertifikat konnte nicht verifiziert werden, da es widerrufen wurde.

Ausgestellt für	
Allgemeiner Name (CN)	<kein Teil des Zertifikats>
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	00:D1:B2:EB:92:7D:CC:8E:FD:55:DF:EA:FE:D2:95:DB:0D
Ausgestellt von	
Allgemeiner Name (CN)	COMODO RSA Client Authentication and Secure Email CA
Organisation (O)	COMODO CA Limited
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Gültigkeitsdauer	
Beginnt mit	12.10.2014
Läuft ab am	13.10.2015
Fingerabdrücke	
SHA1-Fingerabdruck	1C:D6:69:EE:18:07:C9:73:98:B2:28:39:5B:22:F5:EA:C6:60:B8:95
MD5-Fingerabdruck	4C:62:98:40:83:C7:04:22:8A:29:CF:4F:9A:F2:E5:4A

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 aware 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?

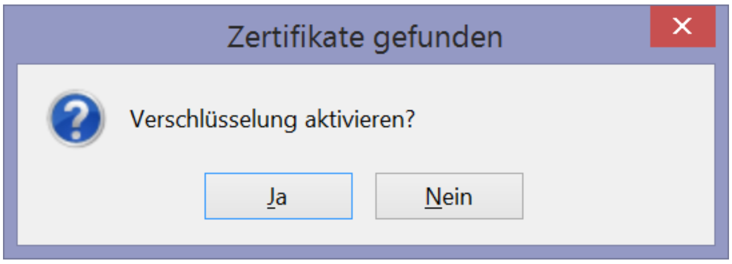
If not this is a request, as a PGP certificate can contain for a user several email addresses.

1.7. TB needs an equivalent to the Encrypt-if-Possible plugin as a 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?)

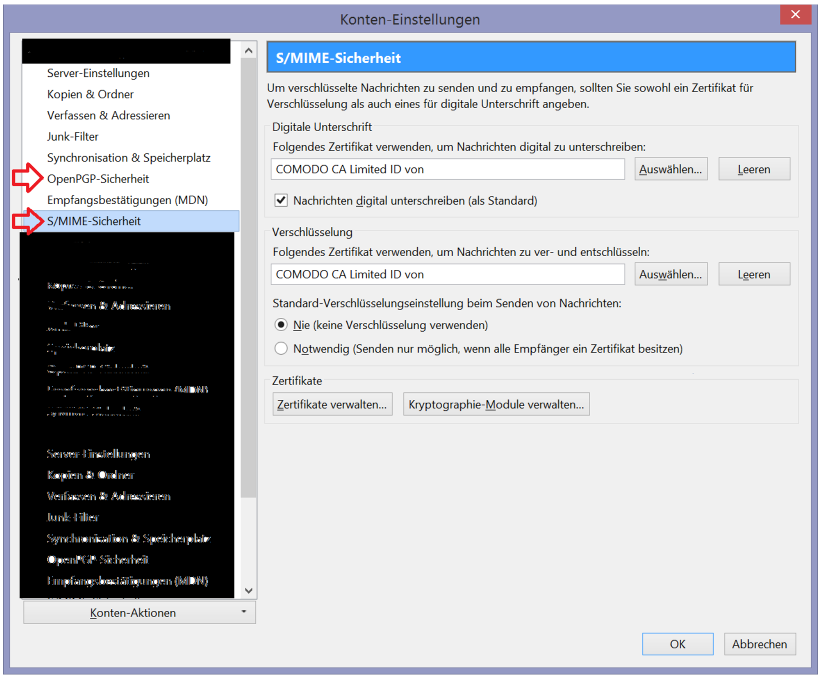


Zertifikate gefunden

Verschlüsselung aktivieren?

==> 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 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.



S/MIME-Sicherheit

Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.

Digitale Unterschrift

Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben:

COMODO CA Limited ID von

Auswählen... Leeren

☑ Nachrichten digital unterschreiben (als Standard)

Verschlüsselung

Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:

COMODO CA Limited ID von

Auswählen... Leeren

Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:

● Nie (keine Verschlüsselung verwenden)

○ Notwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen)

Zertifikate

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.

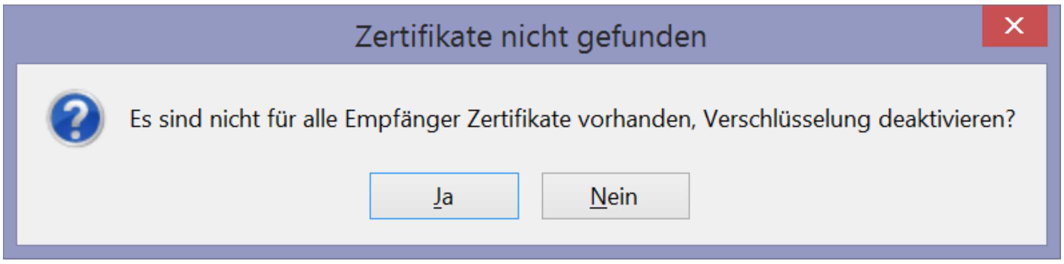
==> Users are left alone to find the reason and what to do.

1.8.1 First error dialog is ok, second is incomplete

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

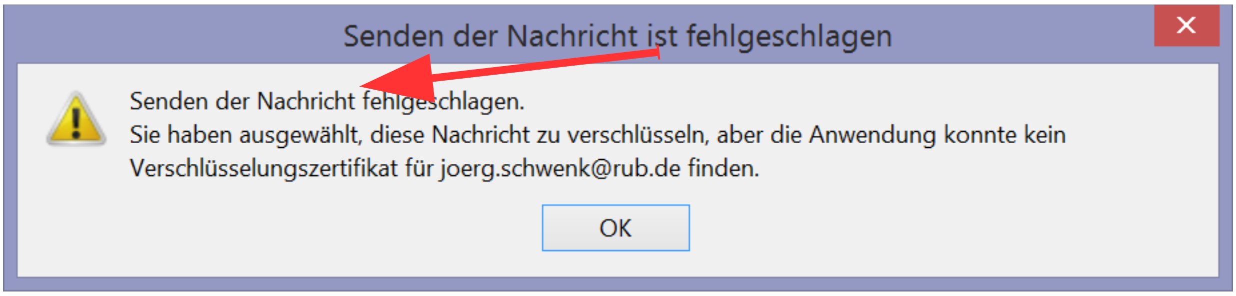
b) However, there are 4 users preventing to send an encrypted email. This should be mentioned.

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”).



Zertifikate nicht gefunden

Es sind nicht für alle Empfänger Zertifikate vorhanden, Verschlüsselung deaktivieren?



Senden der Nachricht ist fehlgeschlagen

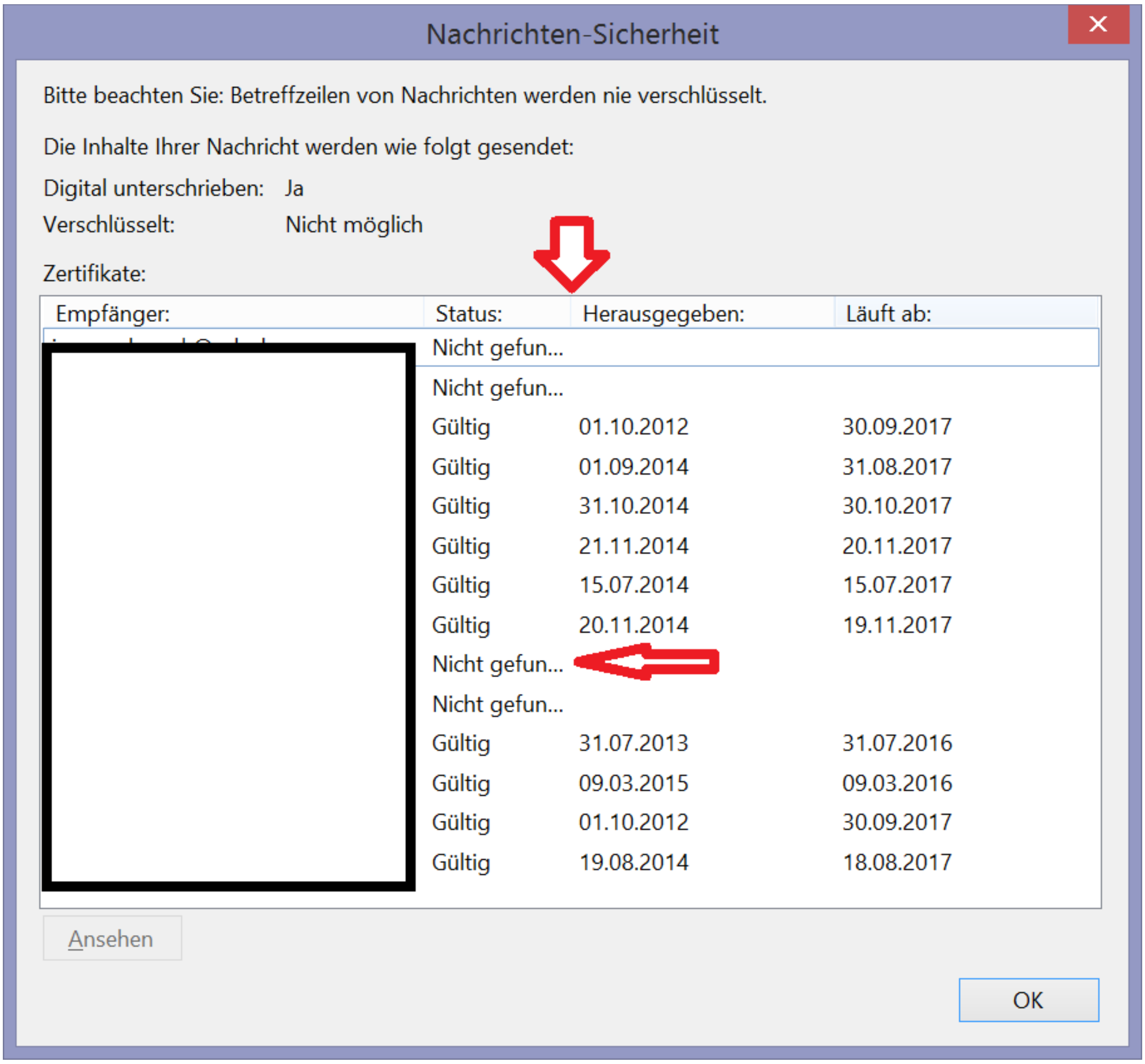
Senden der Nachricht fehlgeschlagen.
Sie haben ausgewählt, diese Nachricht zu verschlüsseln, aber die Anwendung konnte kein Verschlüsselungszertifikat für joerg.schwenk@rub.de finden.

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 its just the end date which is no more valid (so send it 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 instea 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).



Nachrichten-Sicherheit

Bitte beachten Sie: Betreffzeilen von Nachrichten werden nie verschlüsselt.

Die Inhalte Ihrer Nachricht werden wie folgt gesendet:

Digital unterschrieben: Ja

Verschlüsselt: Nicht möglich

Zertifikate:

Empfänger:	Status:	Herausgegeben:	Läuft ab:
[redacted]	Nicht gefun...		
[redacted]	Nicht gefun...		
[redacted]	Gültig	01.10.2012	30.09.2017
[redacted]	Gültig	01.09.2014	31.08.2017
[redacted]	Gültig	31.10.2014	30.10.2017
[redacted]	Gültig	21.11.2014	20.11.2017
[redacted]	Gültig	15.07.2014	15.07.2017
[redacted]	Gültig	20.11.2014	19.11.2017
[redacted]	Nicht gefun...		
[redacted]	Nicht gefun...		
[redacted]	Gültig	31.07.2013	31.07.2016
[redacted]	Gültig	09.03.2015	09.03.2016
[redacted]	Gültig	01.10.2012	30.09.2017
[redacted]	Gültig	19.08.2014	18.08.2017

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 key from the FF (Mozilla) keystore and importing it into the TB keystore via a PK12 file.

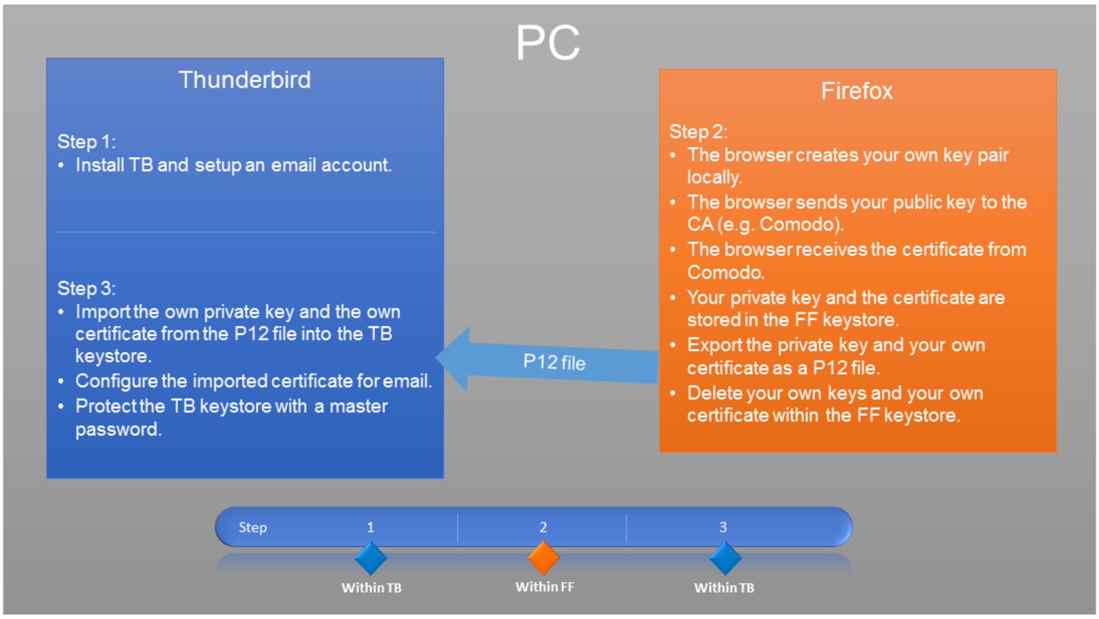
==> This is much too complicated for a normal user.
Users don't accept arguments like the ones found in the documentation: TB and FF are different products with own key stores. Users who have installed both, TB and FF, expect that they can request a certificate from WITHIN Thunderbird (It is possible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

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

In a 2nd 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 jut for to get an initial certificate, and that the users have to do deal with things like “keystore”, “p12 file” they normally don't know.



PC

Thunderbird

Step 1:
- Install TB and setup an email account.

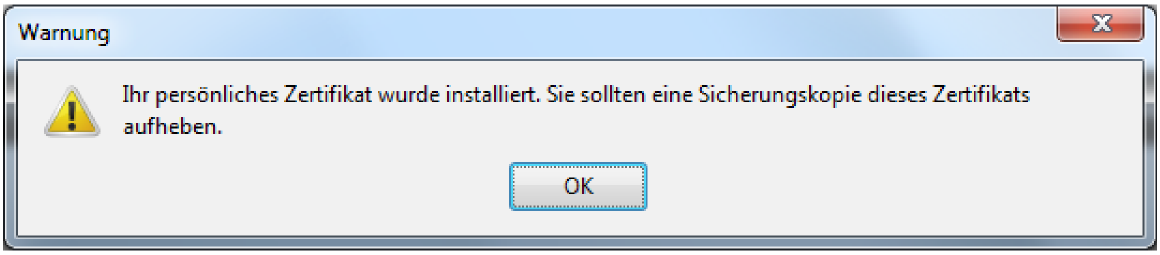
Step 3:
- Import the own private key and the own certificate from the P12 file into the TB keystore.
- Configure the imported certificate for email.
- Protect the TB keystore with a master password.

Firefox

Step 2:
- The browser creates your own key pair locally.
- The browser sends your public key to the CA (e.g. Comodo).
- The browser receives the certificate from Comodo.
- Your private key and the certificate are stored in the FF keystore.
- Export the private key and your own certificate as a P12 file.
- Delete your own keys and your own certificate within the FF keystore.

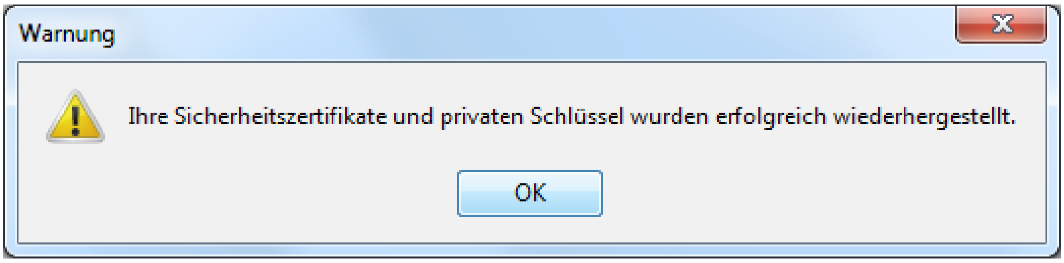
Remark 1: False warnings

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.



Ihr persönliches Zertifikat wurde installiert. Sie sollten eine Sicherungskopie dieses Zertifikats aufheben.

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



Ihre Sicherheitszertifikate und privaten Schlüssel wurden erfolgreich wiederhergestellt.

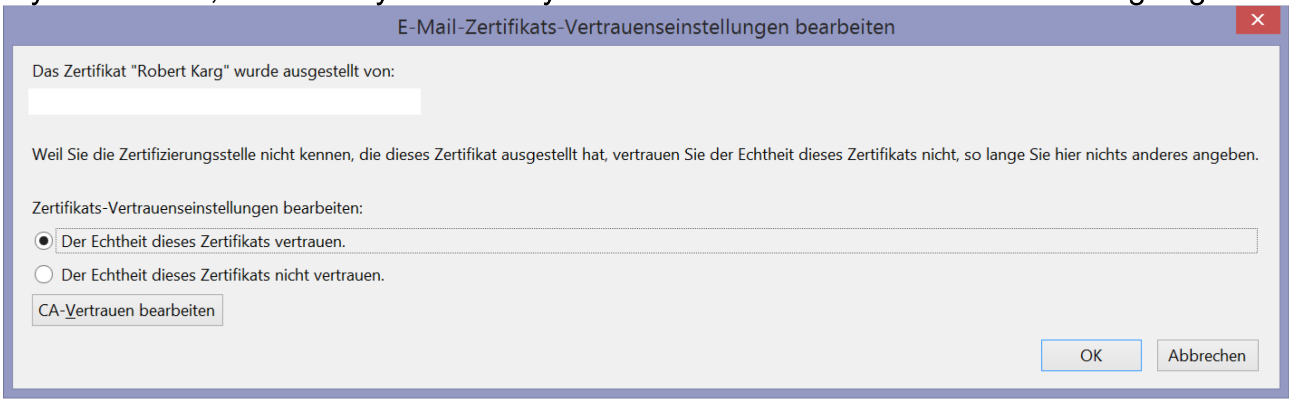
Remark 2: Avoid unnecesssary user interactions

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.

If you look at it, what trust you currently have in the cert of this user and in his signing CA.



E-Mail-Zertifikats-Vertrauenseinstellungen bearbeiten

Das Zertifikat "Robert Karg" wurde ausgestellt von:

Weil Sie die Zertifizierungsstelle nicht kennen, die dieses Zertifikat ausgestellt hat, vertrauen Sie der Echtheit dieses Zertifikats nicht, so lange Sie hier nichts anderes angeben.

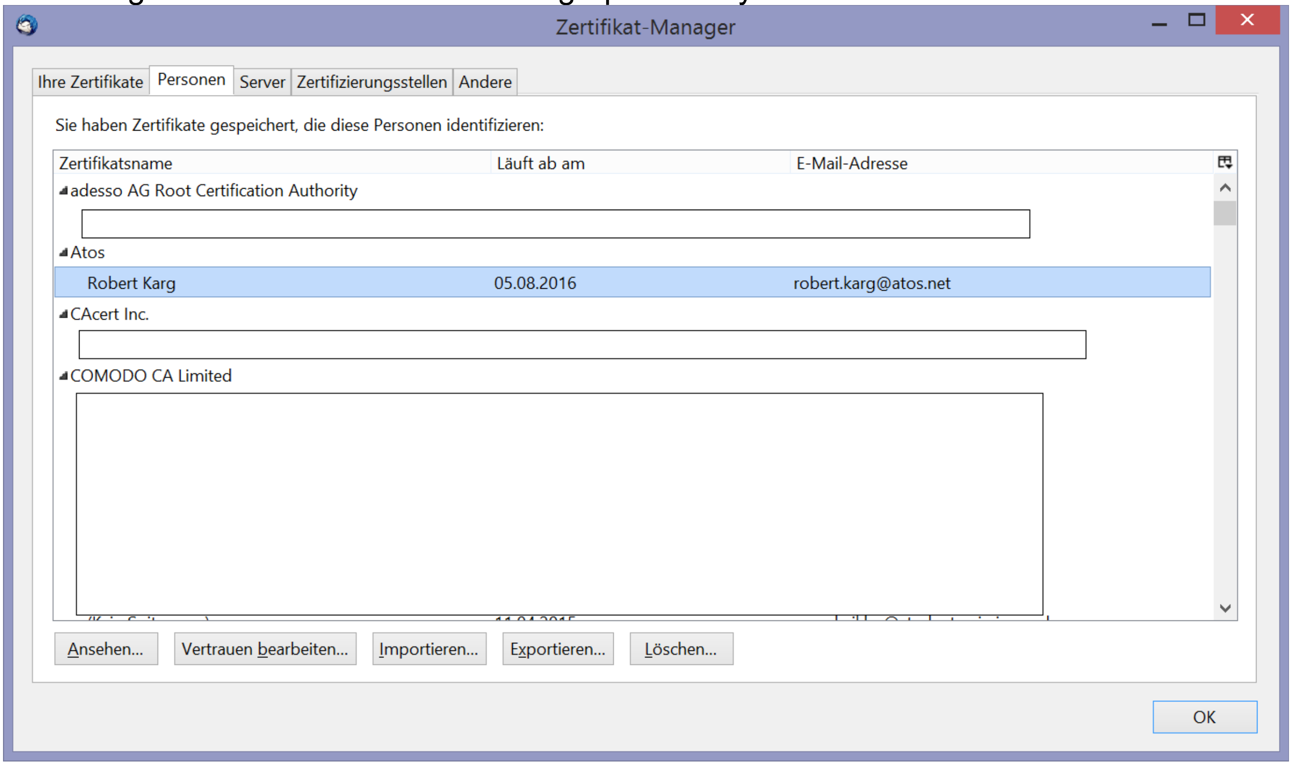
Zertifikats-Vertrauenseinstellungen bearbeiten:

● Der Echtheit dieses Zertifikats vertrauen.

○ Der Echtheit dieses Zertifikats nicht vertrauen.

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.



Zertifikat-Manager

Sie haben Zertifikate gespeichert, die diese Personen identifizieren:

Zertifikatsname	Läuft ab am	E-Mail-Adresse
◢adesso AG Root Certification Authority		
◢Atos		
Robert Karg	05.08.2016	robert.karg@atos.net
◢CAcert Inc.		
◢COMODO CA Limited		

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.

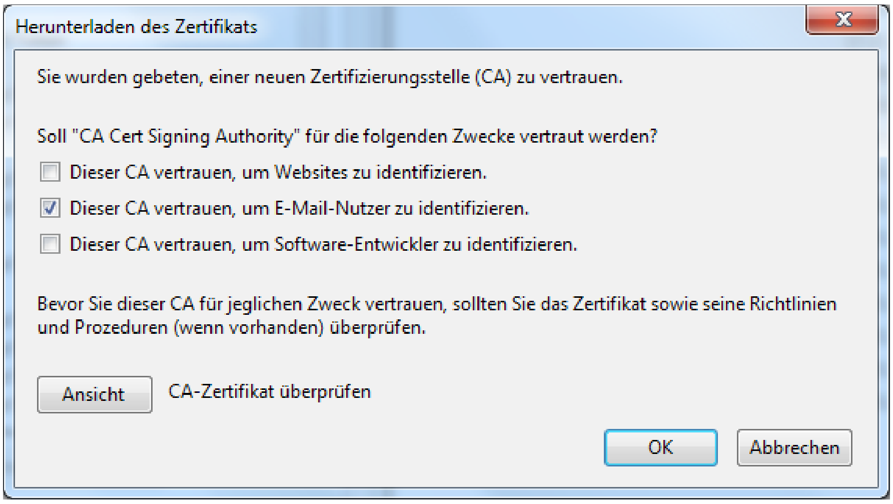
There should be a way a get rid of this restriction:
Maybe there could be an option to decrypt all mails at the beginning or when search is started. Here also, some more research has to be done, how to implement this is a good and efficient way.

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),



Herunterladen des Zertifikats

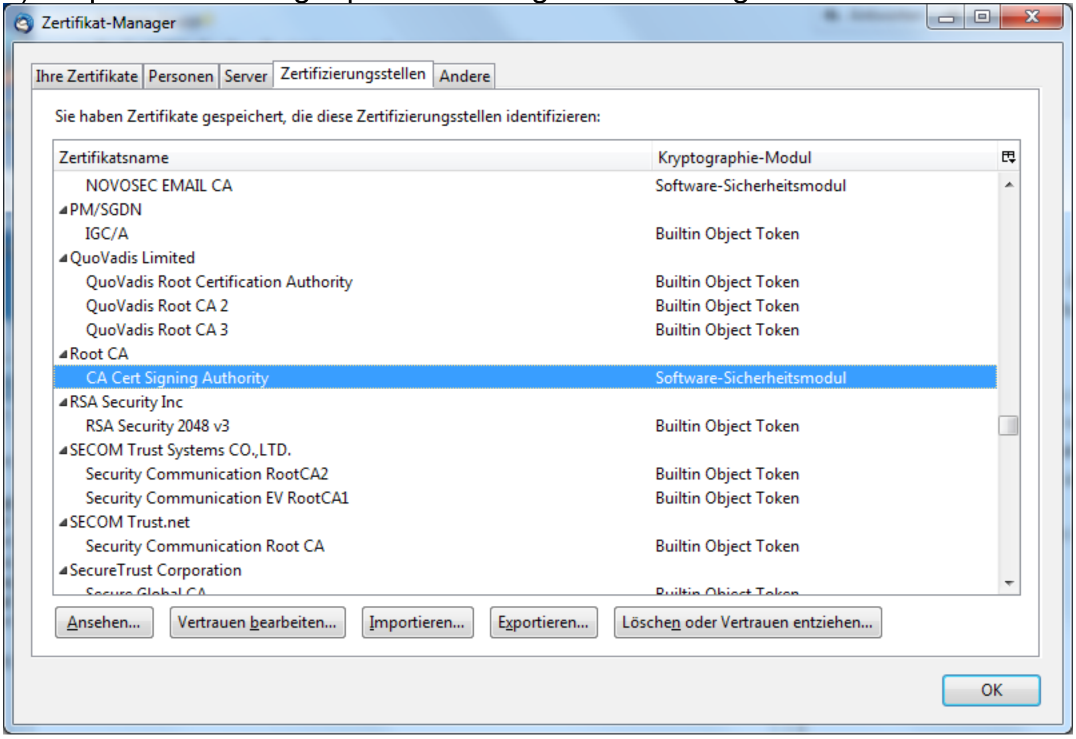
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.

Soll "CA Cert Signing Authority" für die folgenden Zwecke vertraut werden?

☐ Dieser CA vertrauen, um Websites zu identifizieren.
☑ Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
☐ Dieser CA vertrauen, um Software-Entwickler zu identifizieren.

Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.

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:



Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:

Zertifikatsname	Kryptographie-Modul
NOVOSEC EMAIL CA	Software-Sicherheitsmodul
◢PM/SGDN	
IGC/A	Builtin Object Token
◢QuoVadis Limited	
QuoVadis Root Certification Authority	Builtin Object Token
QuoVadis Root CA 2	Builtin Object Token
QuoVadis Root CA 3	Builtin Object Token
◢Root CA	
CA Cert Signing Authority	Software-Sicherheitsmodul
◢RSA Security Inc	
RSA Security 2048 v3	Builtin Object Token
◢SECOM Trust Systems CO.,LTD.	
Security Communication RootCA2	Builtin Object Token
Security Communication EV RootCA1	Builtin Object Token
◢SECOM Trust.net	
Security Communication Root CA	Builtin Object Token
◢SecureTrust Corporation	
Secure Global CA	Builtin Object Token

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

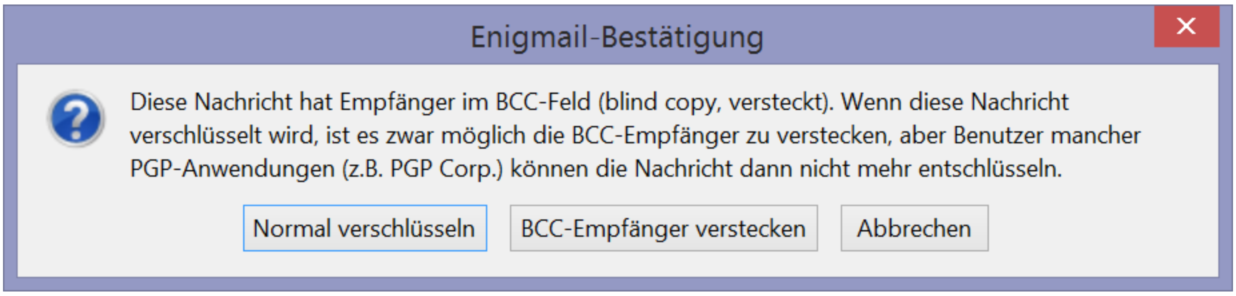
In this scenario there are 4 sets of partners you have email communication with: For some you have no pubkey; for some you only have an S/MIME certificate; for some you only have a PGP certificate; for the first subset you have both, an S/MIME and a PGP key.

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:

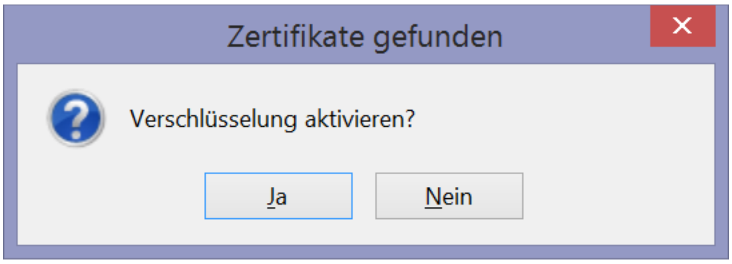
- It should not appear as long as I don't specify Enigmail to be used.
- No normal user understands this message (so I just clicked "Encrypt normally").



Enigmail-Bestätigung

Diese Nachricht hat Empfänger im BCC-Feld (blind copy, versteckt). Wenn diese Nachricht verschlüsselt wird, ist es zwar möglich die BCC-Empfänger zu verstecken, aber Benutzer mancher PGP-Anwendungen (z.B. PGP Corp.) können die Nachricht dann nicht mehr entschlüsseln.

Then you get this message from TB:



Zertifikate gefunden

Verschlüsselung aktivieren?

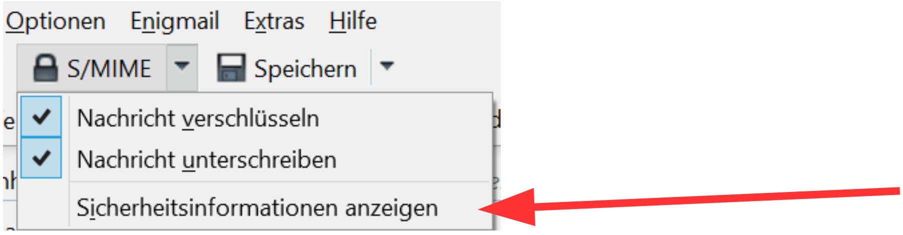
==> A new version of TB integrating S/MIME and PGP should fix the user's uncertainty: Where does this message belong to? It should explain – maybe in the dialog's header – that its from TB and its about S/MIME (not Enigmail or PGP). Suggestion for a new header's title: “S/MIME certificates found” = “S/MIME-Zertifikate 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=BCckblickend m=C3=B6chte ich <==> Rückblickend möchte ich

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

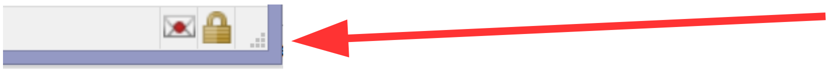
2.2.1 The way of S/MIME

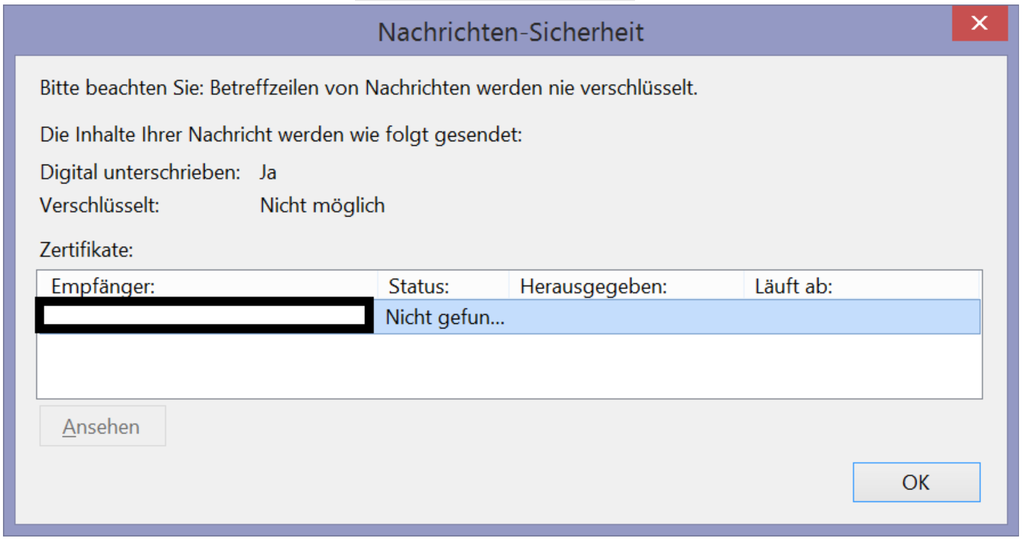
a) Activating the enc/sign properties
There is only one way to do so (compared to 3 ways with Enigmail):
--> The S/MIME button is always there in the 1st button bar in the writing window.
You have to select separately via menu encrypt and sign.
General properties can only be accessed in main window via the ≡ button (not here):


Optionen
Enigmail
Extras
Hilfe
S/MIME
Speichern
✓ Nachricht verschlüsseln
✓ Nachricht unterschreiben
Sicherheitsinformationen anzeigen

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





Nachrichten-Sicherheit

Bitte beachten Sie: Betreffzeilen von Nachrichten werden nie verschlüsselt.

Die Inhalte Ihrer Nachricht werden wie folgt gesendet:

Digital unterschrieben: Ja
Verschlüsselt: Nicht möglich

Zertifikate:

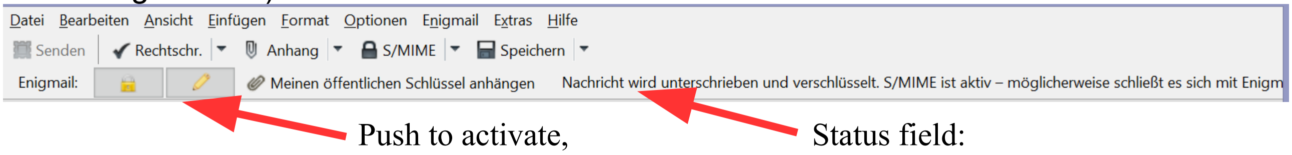
Empfänger:	Status:	Herausgegeben:	Läuft ab:
[redacted]	Nicht gefun...		

2.2.2 The way of Enigmail

a) Activating the enc/sign properties

There are three ways to do so:

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


Datei Bearbeiten Ansicht Einfügen Format Optionen Enigmail Extras Hilfe
Senden
Rechtschr.
Anhang
S/MIME
Speichern
Enigmail:
Meinen öffentlichen Schlüssel anhängen

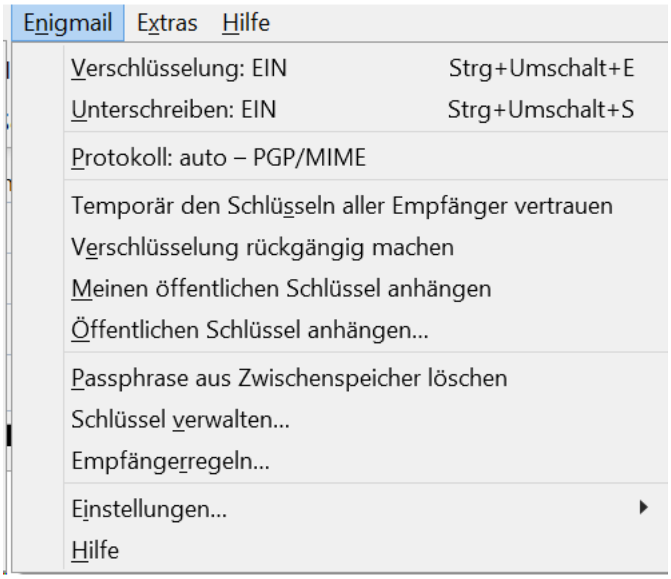
Nachricht wird unterschrieben und verschlüsselt. S/MIME ist aktiv – möglicherweise schließt es sich mit Enigm

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.

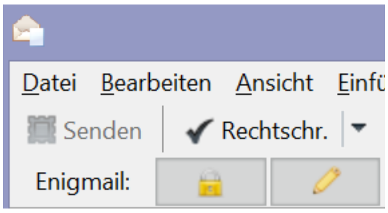
(2) Via menu (visible in main TB window only via Alt, and always in writing window)

(3) Via keyboard shortcuts


Enigmail Extras Hilfe
Verschlüsselung: EIN Strg+Umschalt+E
Unterschreiben: EIN Strg+Umschalt+S
Protokoll: auto – PGP/MIME
Temporär den Schlüsseln aller Empfänger vertrauen
Verschlüsselung rückgängig machen
Meinen öffentlichen Schlüssel anhängen
Öffentlichen Schlüssel anhängen...
Passphrase aus Zwischenspeicher löschen
Schlüssel verwalten...
Empfängerregeln...
Einstellungen...
Hilfe

b) Status information

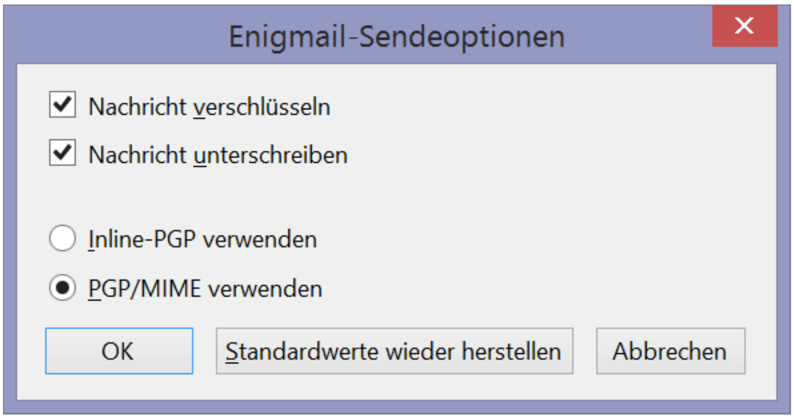
--> Color of the icons in the additional 2nd button line of the sending window. No entry in the normal status bar. Clicking doesn't open a dialog, but toggle the according property (enc or no enc; sign or no sign).



==> 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:



☑ Nachricht verschlüsseln

☑ Nachricht unterschreiben

○ Inline-PGP verwenden

● PGP/MIME verwenden

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.

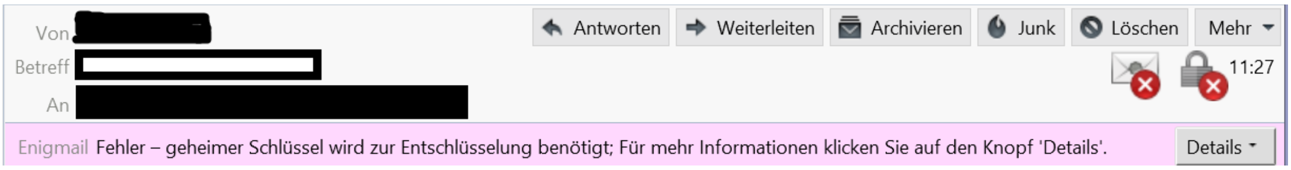
This very obviously shows that there is a real need that the two mail security standards S/MIME and PGP should be implemented internally and in a coordinated manner!

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

I 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: Afterwords you automatically get the key entry dialog.



Von [redacted]
Betreff [redacted]
An [redacted]

11:27

Enigmail Fehler – geheimer Schlüssel wird zur Entschlüsselung benötigt; Für mehr Informationen klicken Sie auf den Knopf 'Details'.

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

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

2.5.1 Coexistence and both-support – Request 1

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

If you write the text of a message which you then want to send it 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.

2.5.2 Coexistence and both-support – Request 2

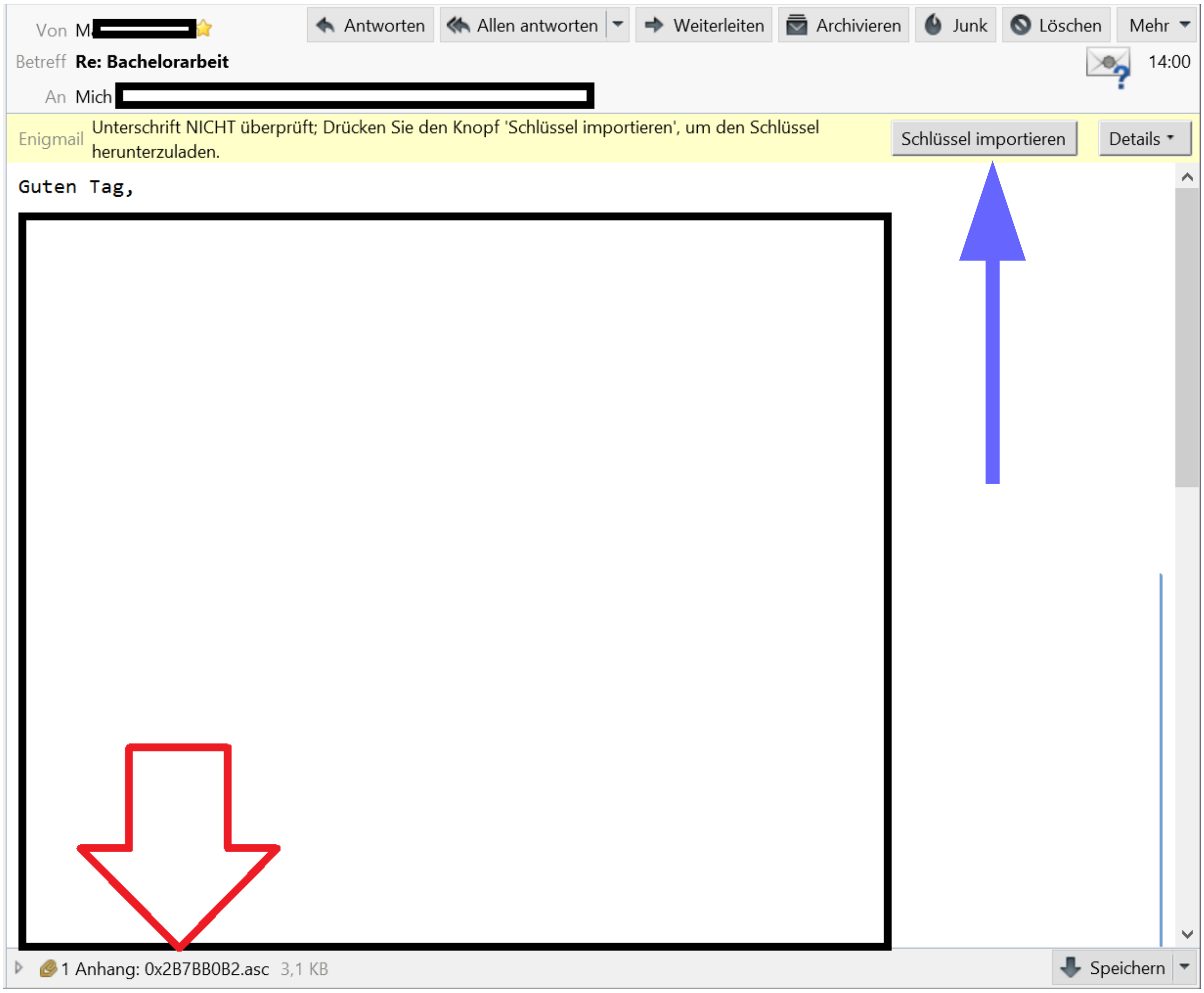
Maybe, in the future there could also exist a common keystore as the public keys could be extracted from both.
However, you only could transfer an S/MIME key into a PGP pubkey format, but not the other way around (as the S/MIME key has to be signed by a trustcenter).

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 attached key isn't handled accordingly

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



Von M[redacted]

Betreff **Re: Bachelorarbeit**

An Mich [redacted]

Enigmail Unterschrift NICHT überprüft; Drücken Sie den Knopf 'Schlüssel importieren', um den Schlüssel herunterzuladen.

Guten Tag,

[redacted]

1 Anhang: 0x2B7BB0B2.asc 3,1 KB

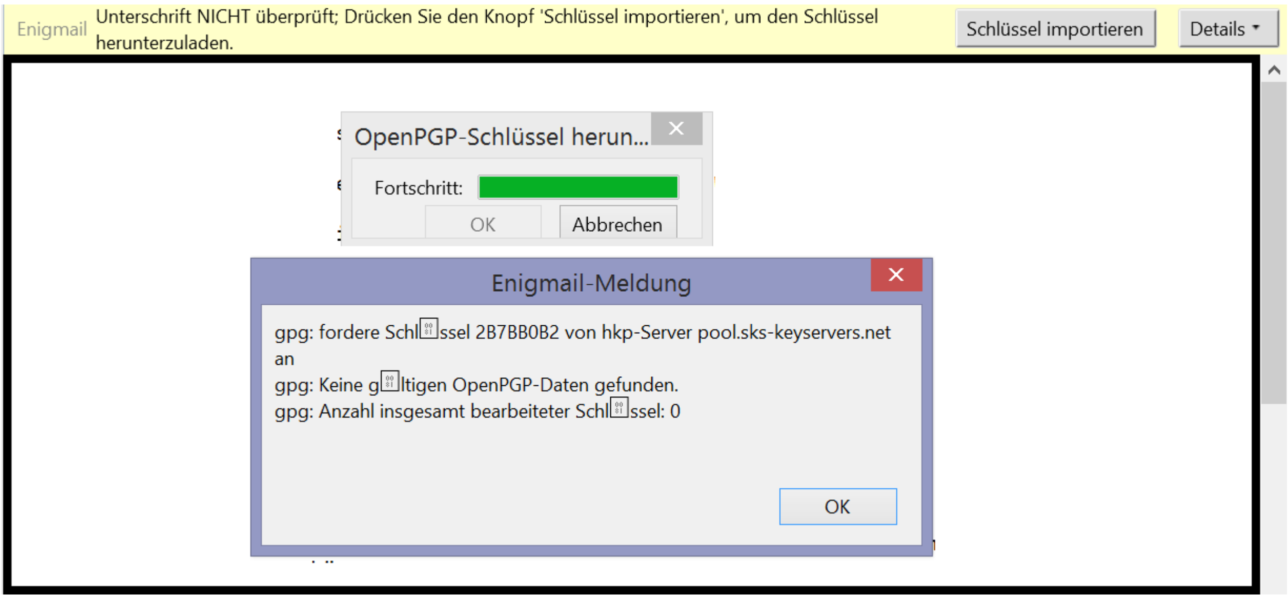
a) When getting a signed email with the sender's key attached, Enigmail doesn't have the sender's pubkey in its keystore yet, and can't check the validity of the signature. That is ok.

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

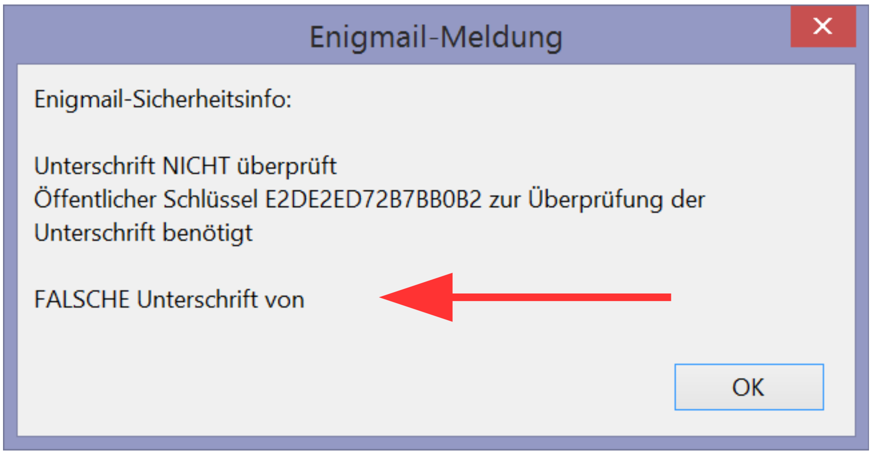
This was NOT what could be expected as the sender just did attach his pubkey because he didn't want to make it available at a key server. This is a decision which should be left to a sender using PGP.

→ So the described behavior is a bug in Enigmail.


Enigmail Unterschrift NICHT überprüft; Drücken Sie den Knopf 'Schlüssel importieren', um den Schlüssel herunterzuladen.

gpg: fordere Schl□ssel 2B7BB0B2 von hkp-Server pool.sks-keyservers.net an
gpg: Keine g□ltigen OpenPGP-Daten gefunden.
gpg: Anzahl insgesamt bearbeiteter Schl□ssel: 0

c) Clicking on “Security information” we get:



Enigmail-Sicherheitsinfo:

Unterschrift NICHT überprüft
Öffentlicher Schlüssel E2DE2ED72B7BB0B2 zur Überprüfung der Unterschrift benötigt

FALSCHE Unterschrift von

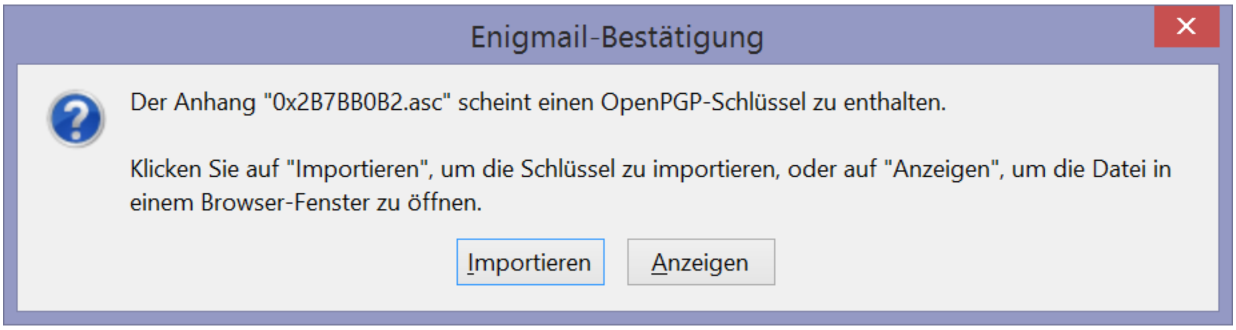
Unterschrift NICHT überprüft
Öffentlicher Schlüssel E2DE2ED72B7BB0B2 zur Überprüfung der Unterschrift benötigt
FALSCHE Unterschrift von

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

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

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

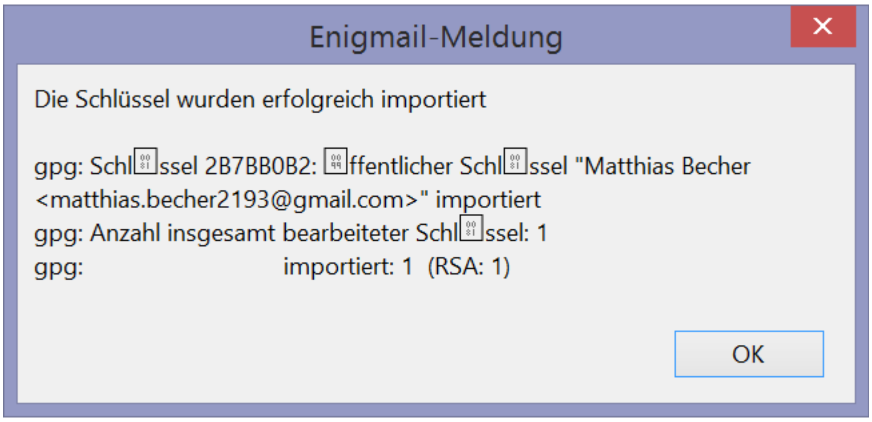
d) Now I double-clicked at the attachment, and it perfectly worked to import the attached pubkey into the PGP keystore.


Enigmail-Bestätigung

Der Anhang "0x2B7BB0B2.asc" scheint einen OpenPGP-Schlüssel zu enthalten.

Klicken Sie auf "Importieren", um die Schlüssel zu importieren, oder auf "Anzeigen", um die Datei in einem Browser-Fenster zu öffnen.

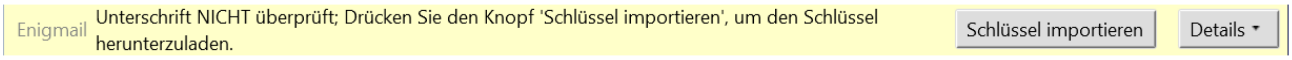
Again the formal thing: Some umlaut errors.


Enigmail-Meldung

Die Schlüssel wurden erfolgreich importiert

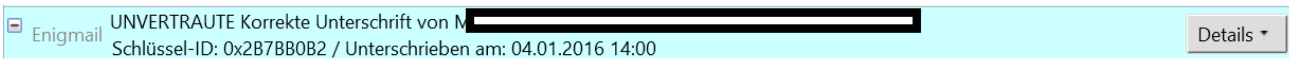
```
gpg: Schl□ssel 2B7BB0B2: □ffentlicher Schl□ssel "Matthias Becher
<matthias.becher2193@gmail.com>" importiert
gpg: Anzahl insgesamt bearbeiteter Schl□ssel: 1
gpg:                    importiert: 1  (RSA: 1)
```

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



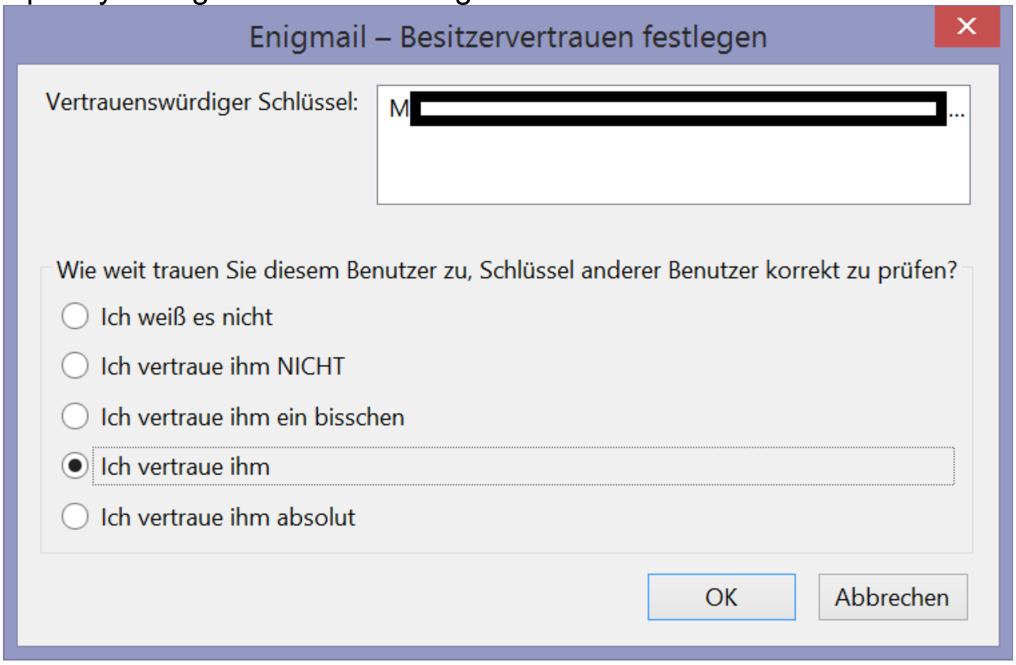
Unterschrift NICHT überprüft; Drücken Sie den Knopf 'Schlüssel importieren', um den Schlüssel herunterzuladen.

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.



UNVERTRAUTE Korrekte Unterschrift von M[redacted]
Schlüssel-ID: 0x2B7BB0B2 / Unterschrieben am: 04.01.2016 14:00

f) Then I explicitly changed the trust settings:



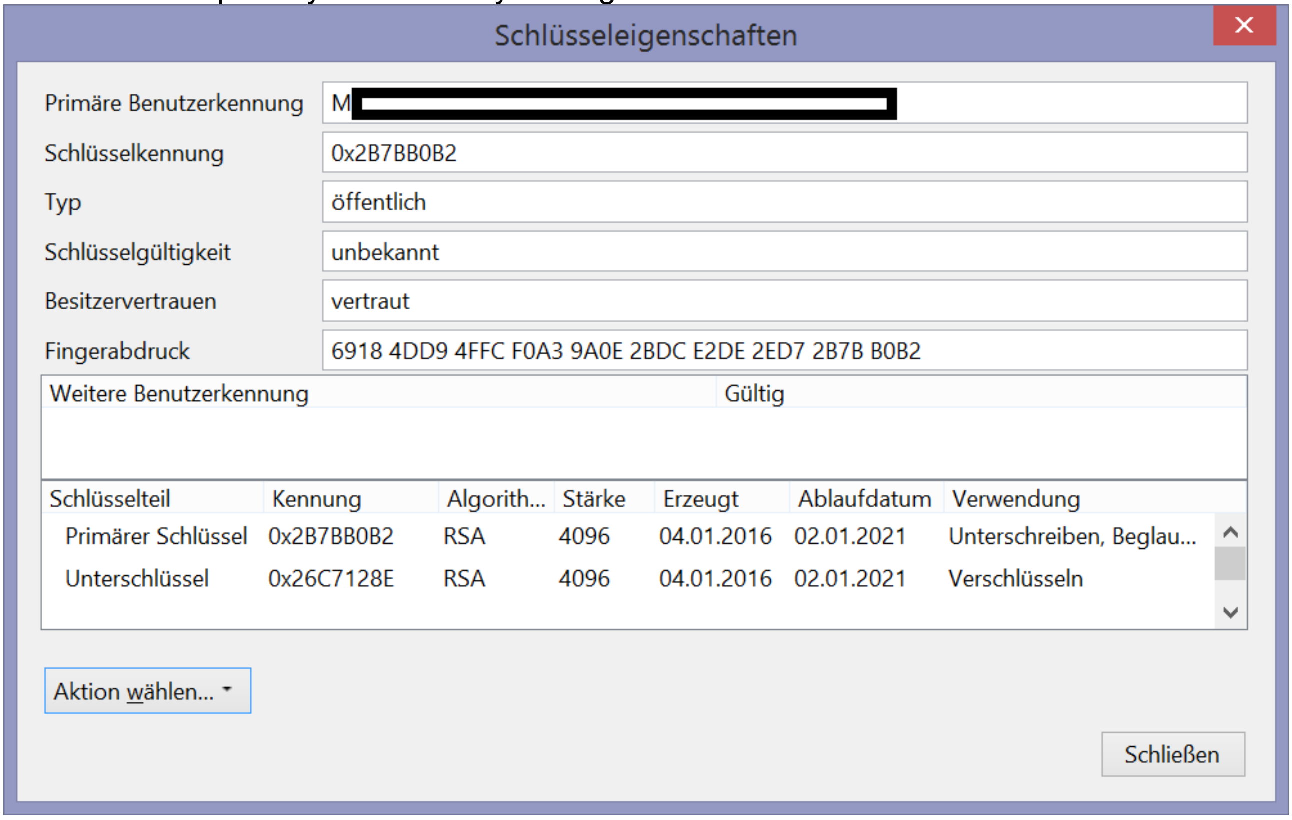
Enigmail – Besitzervertrauen festlegen

Vertrauenswürdiger Schlüssel: M[redacted]...

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

which are accepted by the PGP key manager.



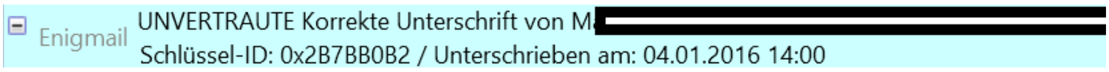
Schlüsseleigenschaften

Primäre Benutzerkennung	M[redacted]
Schlüsselkennung	0x2B7BB0B2
Typ	öffentlich
Schlüsselgültigkeit	unbekannt
Besitzervertrauen	vertraut
Fingerabdruck	6918 4DD9 4FFC F0A3 9A0E 2BDC E2DE 2ED7 2B7B B0B2

Weitere Benutzerkennung	Gültig

Schlüsselteil	Kennung	Algorith...	Stärke	Erzeugt	Ablaufdatum	Verwendung
Primärer Schlüssel	0x2B7BB0B2	RSA	4096	04.01.2016	02.01.2021	Unterschreiben, Beglau...
Unterschlüssel	0x26C7128E	RSA	4096	04.01.2016	02.01.2021	Verschlüsseln

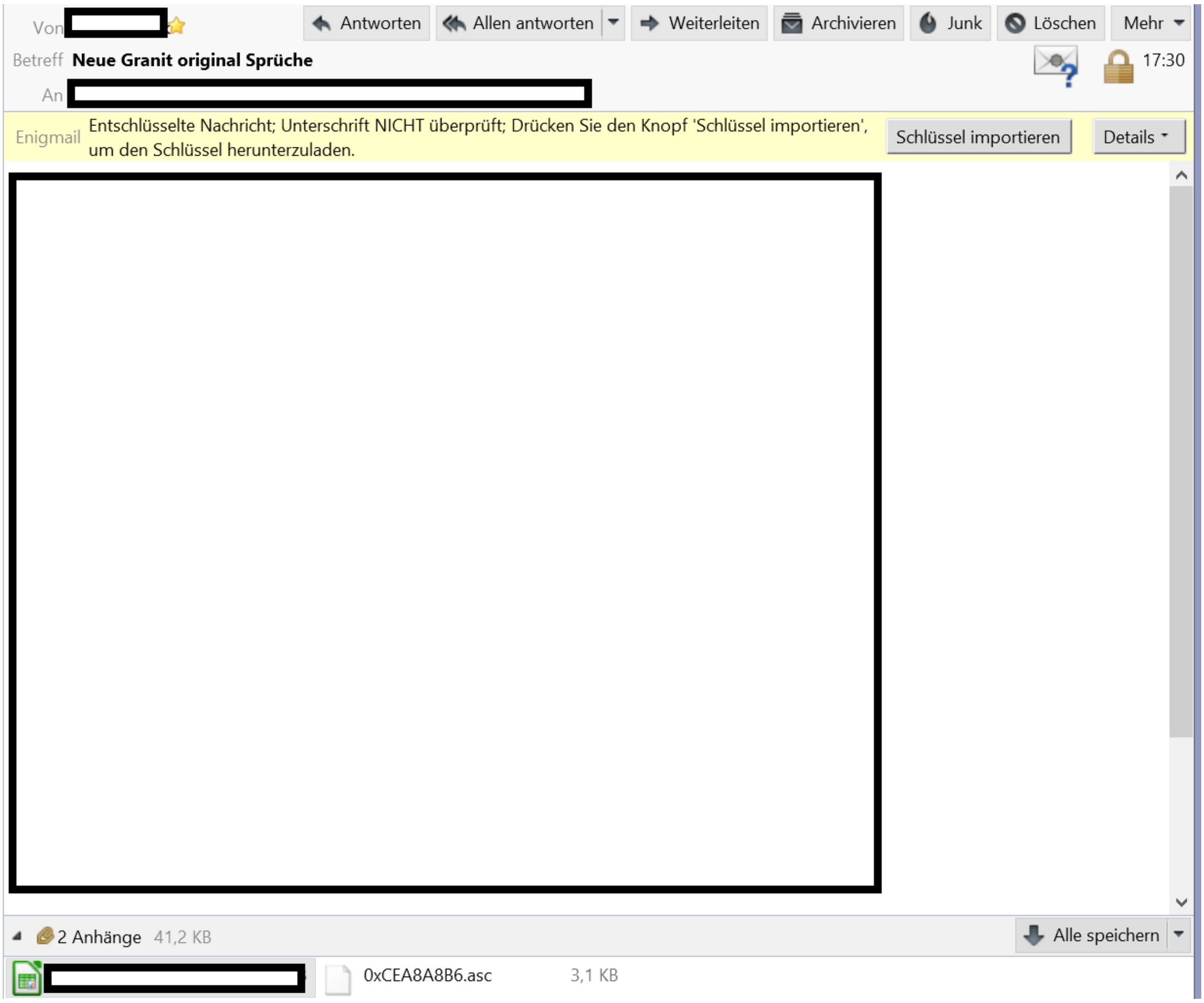
Nevertheless, the email header continues to state “UNVERTRAUT”:



UNVERTRAUTE Korrekte Unterschrift von M[redacted]
Schlüssel-ID: 0x2B7BB0B2 / Unterschrieben am: 04.01.2016 14:00

3.2. Scenario where the trust level isn't shown correctly, and 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.



Von [redacted]

Betreff **Neue Granit original Sprüche**

An [redacted]

17:30

Enigmail Entschlüsselte Nachricht; Unterschrift NICHT überprüft; Drücken Sie den Knopf 'Schlüssel importieren', um den Schlüssel herunterzuladen.

[redacted]

2 Anhänge 41,2 KB

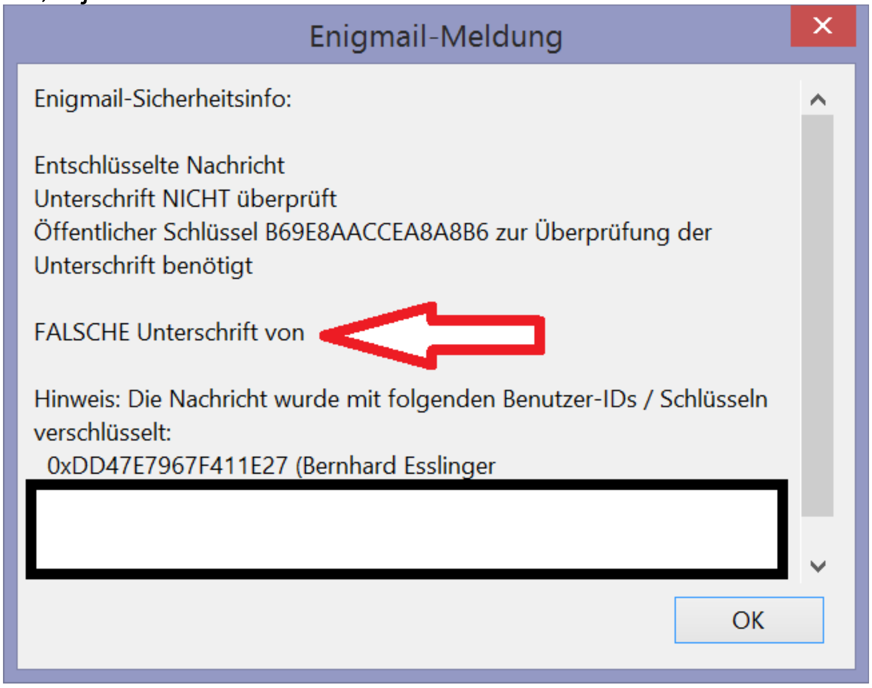
[redacted]

0xCEA8A8B6.asc 3,1 KB

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.



Enigmail-Sicherheitsinfo:

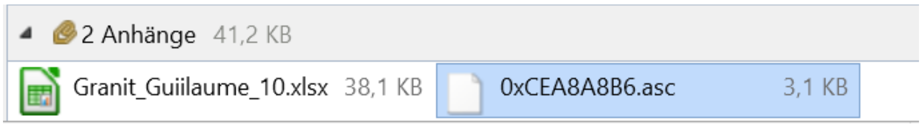
Entschlüsselte Nachricht
Unterschrift NICHT überprüft
Öffentlicher Schlüssel B69E8AACCEA8A8B6 zur Überprüfung der Unterschrift benötigt

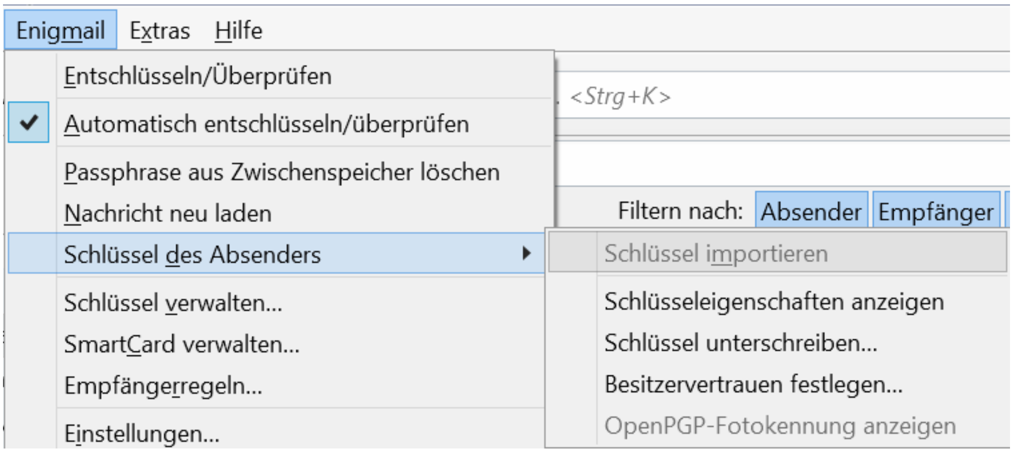
FALSCHE Unterschrift von

Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:
0xDD47E7967F411E27 (Bernhard Esslinger
[redacted]

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.

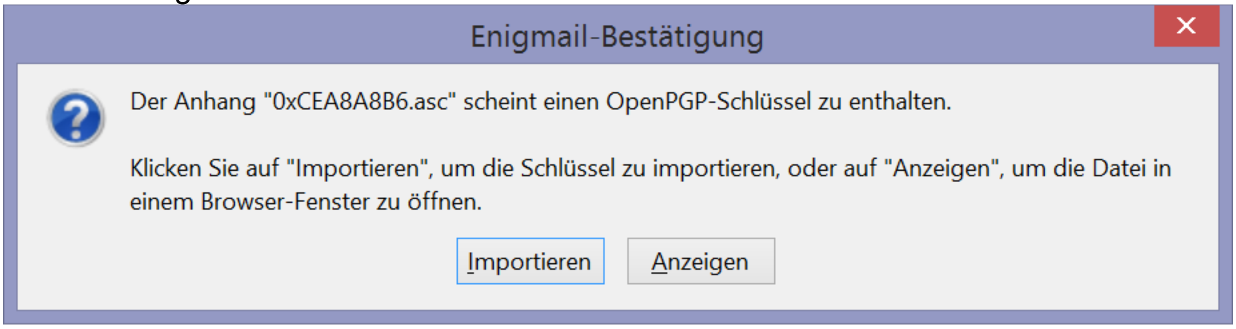
3.2.3 Case where Enigmail menu entry “Decrypt / Verify” doesn't work correctly

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

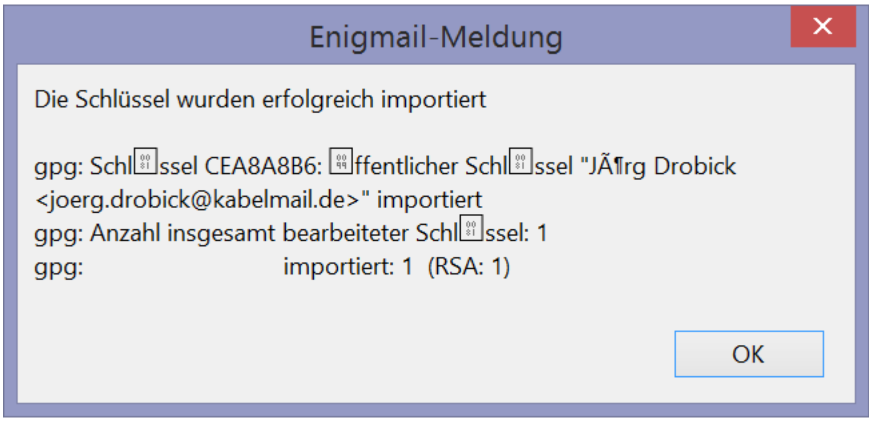
Double-clicking on the attached asc file:



Enigmail-Bestätigung

Der Anhang "0xCEA8A8B6.asc" scheint einen OpenPGP-Schlüssel zu enthalten.

Klicken Sie auf "Importieren", um die Schlüssel zu importieren, oder auf "Anzeigen", um die Datei in einem Browser-Fenster zu öffnen.

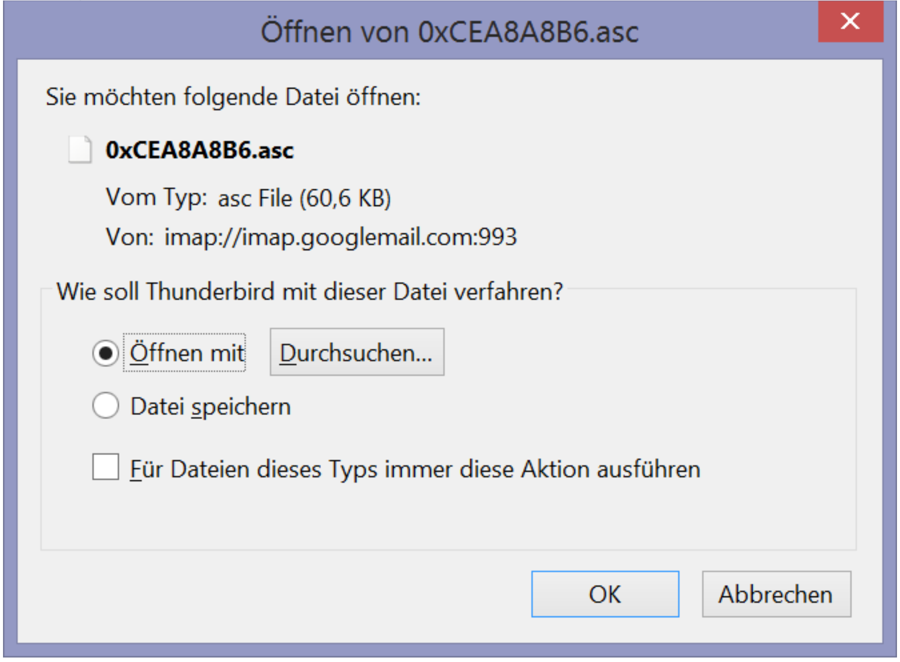


Enigmail-Meldung

Die Schlüssel wurden erfolgreich importiert

```
gpg: Schl□ssel CEA8A8B6: □ffentlicher Schl□ssel "JÃ¶rg Drobick
<joerg.drobick@kabelmail.de>" importiert
gpg: Anzahl insgesamt bearbeiteter Schl□ssel: 1
gpg:               importiert: 1  (RSA: 1)
```

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



Öffnen von 0xCEA8A8B6.asc

Sie möchten folgende Datei öffnen:

0xCEA8A8B6.asc

Vom Typ: asc File (60,6 KB)

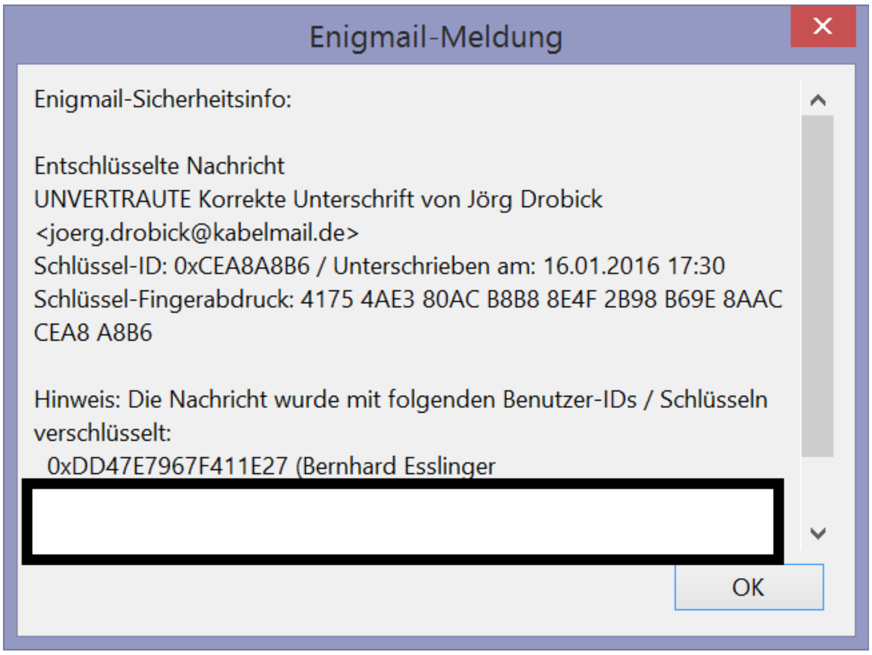
Von: imap://imap.googlemail.com:993

Wie soll Thunderbird mit dieser Datei verfahren?

● Öffnen mit

○ Datei speichern

□ Für Dateien dieses Typs immer diese Aktion ausführen



Enigmail-Sicherheitsinfo:

Entschlüsselte Nachricht
UNVERTRAUTE Korrekte Unterschrift von Jörg Drobick
<joerg.drobick@kabelmail.de>
Schlüssel-ID: 0xCEA8A8B6 / Unterschrieben am: 16.01.2016 17:30
Schlüssel-Fingerabdruck: 4175 4AE3 80AC B8B8 8E4F 2B98 B69E 8AAC
CEA8 A8B6

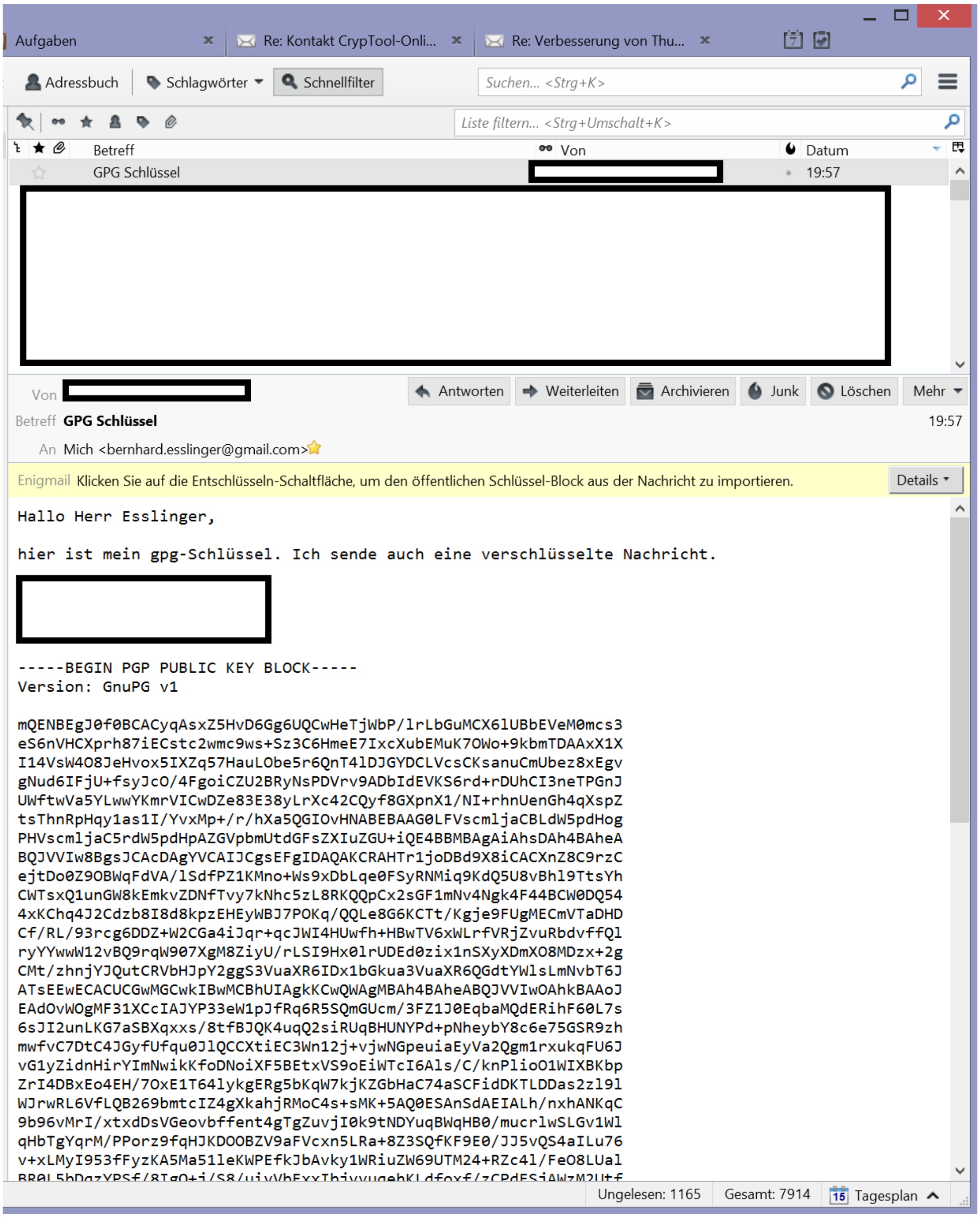
Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:
0xDD47E7967F411E27 (Bernhard Esslinger

[redacted]

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

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

a) I got a pubkey in text form:



GPG Schlüssel [redacted] 19:57

[redacted]

Von [redacted]

Betreff **GPG Schlüssel** 19:57

An Mich <bernhard.esslinger@gmail.com>

Enigmail Klicken Sie auf die Entschlüsseln-Schaltfläche, um den öffentlichen Schlüssel-Block aus der Nachricht zu importieren.

```
Hallo Herr Esslinger,

hier ist mein gpg-Schlüssel. Ich sende auch eine verschlüsselte Nachricht.
```

[redacted]

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBEgJ0f0BCACyqAsxZ5HvD6Gg6UQCwHeTjWbP/lrLbGuMCX6lUBbEVeM0mcs3
eS6nVHCXprh87iECstc2wmc9ws+Sz3C6HmeE7IxcXubEMuK7OWo+9kbmTDAAxX1X
I14VsW4O8JeHvox5IXZq57HauLObe5r6QnT4lDJGYDCLVcsCKsanuCmUbez8xEgv
gNud6IFjU+fsyJcO/4FgoiCZU2BRyNsPDVrv9ADbIdEVKS6rd+rDUhCI3neTPGnJ
UWftwVa5YLwwYKmrVICwDZe83E38yLrXc42CQyf8GXpnX1/NI+rhnUenGh4qXspZ
tsThnRpHqy1as1I/YvxMp+/r/hXa5QGIOvHNABEBAAG0LFVscmljaCBLdW5pdHog
PHVscmljaC5rdW5pdHpAZGVpbmUtdGFsZXIuZGU+iQE4BBMBAgAiAhsDAh4BAheA
BQJVVIw8BgsJCAcDAgYVCAIJCgsEFgIDAQAKCRAHTr1joDBd9X8iCACXnZ8C9rzC
ejtDo0Z9OBWqFdVA/lSdfPZ1KMno+Ws9xDbLqe0FSyRNMiq9KdQ5U8vBhl9TtsYh
CWTsxQ1unGW8kEmkvZDNfTvy7kNhc5zL8RKQQpCx2sGF1mNv4Ngk4F44BCW0DQ54
4xKChq4J2Cdzb8I8d8kpzEHEyWBJ7POKq/QQLe8G6KCTt/Kgje9FUgMECmVTaDHD
Cf/RL/93rcg6DDZ+W2CGa4iJqr+qcJWI4HUwfh+HBwTV6xWLrfVRjZvuRbdvffQl
ryYYwwW12vBQ9rqW907XgM8ZiyU/rLSI9Hx0lrUDEd0zix1nSXyXDmXO8MDzx+2g
CMt/zhnjYJQutCRVbHJpY2ggS3VuaXR6IDx1bGkua3VuaXR6QGdtYWlsLmNvbT6J
ATsEEwECACUCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheABQJVVIwOAhkBAAoJ
EAdOvWOgMF31XCcIAJYP33eW1pJfRq6R5SQmGUcm/3FZ1J0EqbaMQdERihF60L7s
6sJI2unLKG7aSBXqxxs/8tfBJQK4uqQ2siRUqBHUNYPd+pNheybY8c6e75GSR9zh
mwfvC7DtC4JGyfUfqu0JlQCCXtiEC3Wn12j+vjwNGpeuiaEyVa2Qgm1rxukqFU6J
vG1yZidnHirYImNwikKfoDNoiXF5BEtxVS9oEiWTcI6Als/C/knPlioO1WIXBKbp
ZrI4DBxEo4EH/7OxE1T64lykgERg5bKqW7kjKZGbHaC74aSCFidDKTLDDas2zl9l
WJrwRL6VfLQB269bmtcIZ4gXkahjRMoC4s+sMK+5AQ0ESAnSdAEIALh/nxhANKqC
9b96vMrI/xtxdDsVGeovbffent4gTgZuvjI0k9tNDYuqBWqHB0/mucrlwSLGv1Wl
qHbTgYqrM/PPorz9fqHJKDOOBZV9aFVcxn5LRa+8Z3SQfKF9E0/JJ5vQS4aILu76
v+xLMyI953fFyzKA5Ma51leKWPEfkJbAvky1WRiuZW69UTM24+RZc4l/FeO8LUal
```

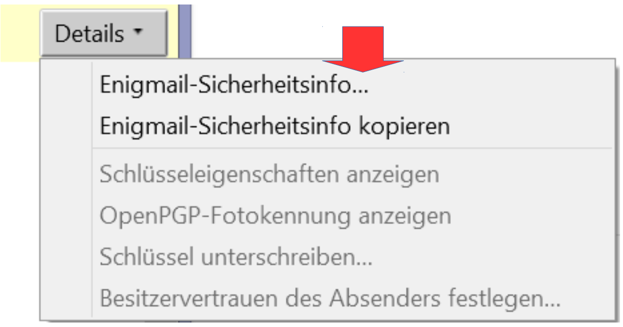
-----BEGIN PGP PUBLIC KEY BLOCK-----

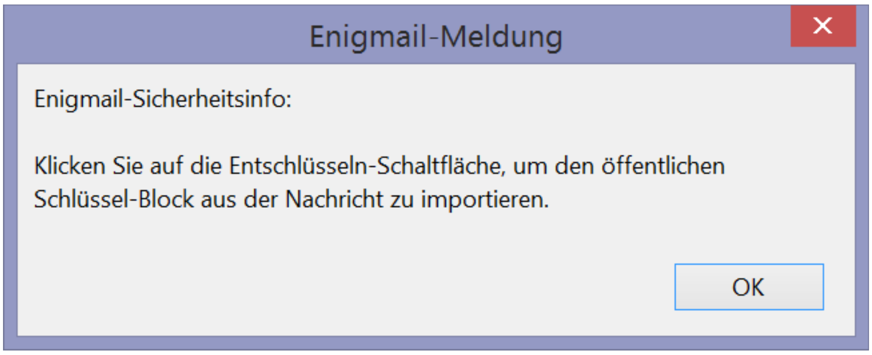
```
Version: GnuPG v1

mQENBEgJ0f0BCACyqAsxZ5HvD6Gg6UQCwHeTjWbP/lrLbGuMCX6lUBbEVeM0mcs3
eS6nVHCXprh87iECstc2wmc9ws+Sz3C6HmeE7IxcXubEMuK7OWo+9kbmTDAAxX1X
I14VsW4O8JeHvox5IXZq57HauLObe5r6QnT4lDJGYDCLVcsCKsanuCmUbez8xEgv
```

```
gNud6IFjU+fsyJcO/4FgoiCZU2BRyNsPDVrv9ADbIdEVKS6rd+rDUhCI3neTPGnJ
UWftwVa5YLwwYKmrVICwDZe83E38yLrXc42CQyf8GXpnX1/NI+rhnUenGh4qXspZ
tsThnRpHqy1as1I/YvxMp+/r/hXa5QGIOvHNABEBAAG0LFVscmljaCBLdW5pdHog
PHVscmljaC5rdW5pdHpAZGVpbmUtdGFsZXIuZGU+iQE4BBMBAgAiAhsDAh4BAheA
BQJVVIw8BgsJCAcDAgYVCAIJCgsEFgIDAQAKCRAHTr1joDBd9X8iCACXnZ8C9rzC
ejtDo0Z9OBWqFdVA/lSdfPZ1KMno+Ws9xDbLqe0FSyRNMiq9KdQ5U8vBhl9TtsYh
CWTsxQ1unGW8kEmkvZDNfTvy7kNhc5zL8RKQQpCx2sGF1mNv4Ngk4F44BCW0DQ54
4xKChq4J2Cdzb8I8d8kpzEHEyWBJ7POKq/QQLe8G6KCTt/Kgje9FUgMECmVTaDHD
Cf/RL/93rcg6DDZ+W2CGa4iJqr+qcJWI4HUwfh+HBwTV6xWLrfVRjZvuRbdvffQl
ryYYwwW12vBQ9rqW907XgM8ZiyU/rLSI9Hx0lrUDEd0zix1nSXyXDmXO8MDzx+2g
CMt/zhnjYJQutCRVbHJpY2ggS3VuaXR6IDx1bGkua3VuaXR6QGdtYWlsLmNvbT6J
ATsEEwECACUCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheABQJVVIwOAhkBAAoJ
EAdOvWOgMF31XCcIAJYP33eW1pJfRq6R5SQmGUcm/3FZ1J0EqbaMQdERihF60L7s
6sJI2unLKG7aSBXqxxs/8tfBJQK4uqQ2siRUqBHUNYPd+pNheybY8c6e75GSR9zh
mwfvC7DtC4JGyfUfqu0JlQCCXtiEC3Wn12j+vjwNGpeuiaEyVa2Qgm1rxukqFU6J
vG1yZidnHirYImNwikKfoDNoiXF5BEtxVS9oEiWTcI6Als/C/knPlioO1WIXBKbp
ZrI4DBxEo4EH/7OxE1T64lykgERg5bKqW7kjKZGbHaC74aSCFidDKTLDDas2zl9l
WJrwRL6VfLQB269bmtcIZ4gXkahjRMoC4s+sMK+5AQ0ESAnSdAEIALh/nxhANKqC
9b96vMrI/xtxdDsVGeovbffent4gTgZuvjI0k9tNDYuqBWqHB0/mucrlwSLGv1Wl
qHbTgYqrM/PPorz9fqHJKDOOBZV9aFVcxn5LRa+8Z3SQfKF9E0/JJ5vQS4aILu76
v+xLMyI953fFyzKA5Ma51leKWPEfkJbAvky1WRiuZW69UTM24+RZc4l/FeO8LUal
BR0L5bDqzYPSf/8IgQ+j/S8/uiyVbExxIbjvyuqehKLdfoxf/zCPdESjAWzM2Utf
iFhbfeolCPJ3zLI5Vxepcv3V6DaKzms+FdFa38YlPmsHhBQNZeoVQnBXLTu4jyuI
40fVKKH7YUMAEQEAAYkBHwQYAQIACQUCSAnSdAIbDAAKCRAHTr1joDBd9WKfB/9C
mBoclAQTztyGkQ9npWZ55RxLI5x64sZSTBlYikflLUdThz3Chm3MvRNTOVAmiqmr
gnAowNftWZezvL+sw3PCQxY4uug+NKy6jn0Kg9ae9DS3jzRMJD6lm8bmCMAsS47h
xh83nvTraZo0aBKyRPxgy120XpXSymANCMBfmygNF7WLrXjZ39P6QzomVXqJ8w96
+akAArmZ1DxC1h085ufc67U2GMOjixf28sdabv963gANDIsTYYYeow/VpNkx+n5S
9MuPeITWS/iZXeilmc2kBxLotUAiLcLJdT2tR3C1lv9C9bfZCCCtPYkGYpxGmrn1
Jn0h4F0UEgkB6j8PJIPR
=lvYx
-----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”:


Details ▾
Enigmail-Sicherheitsinfo...
Enigmail-Sicherheitsinfo kopieren
Schlüsseleigenschaften anzeigen
OpenPGP-Fotokennung anzeigen
Schlüssel unterschreiben...
Besitzervertrauen des Absenders festlegen...



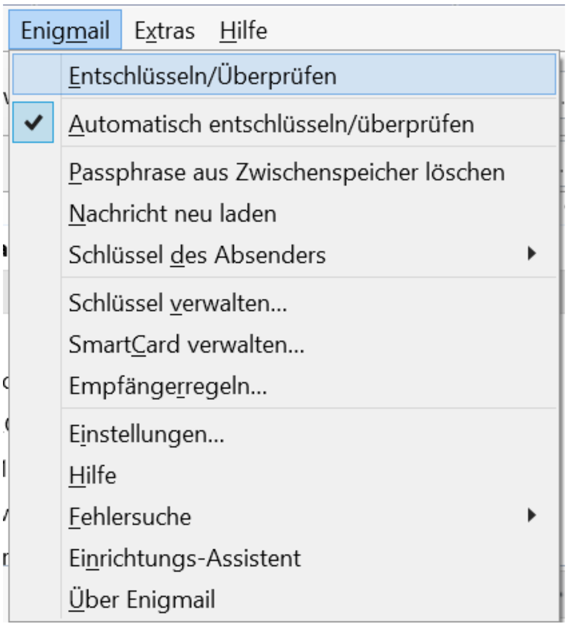
Enigmail-Sicherheitsinfo:

Klicken Sie auf die Entschlüsseln-Schaltfläche, um den öffentlichen Schlüssel-Block aus der Nachricht zu importieren.

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 1st point may be not the developers' fault.
- However, the 2nd 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)

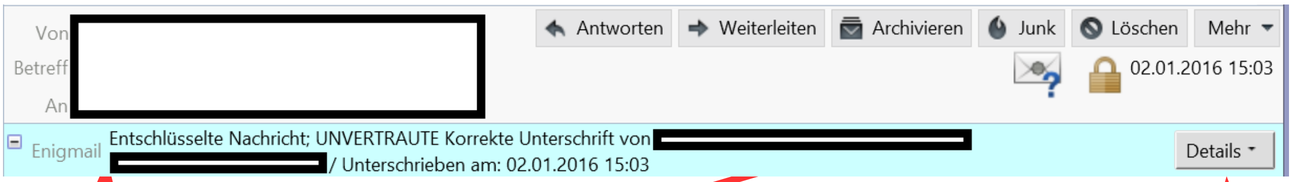
a) Have an option to send PGP signed as default.

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:

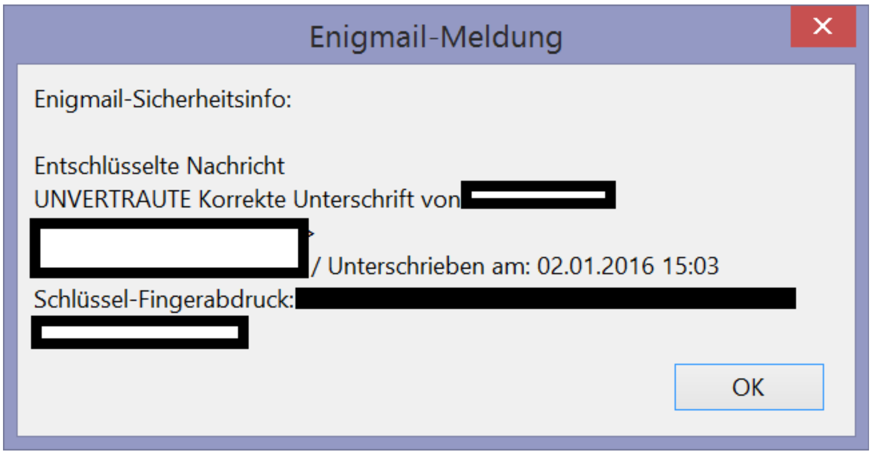


Von [redacted]
Betreff
An

02.01.2016 15:03

Enigmail Entschlüsselte Nachricht; UNVERTRAUTE Korrekte Unterschrift von [redacted] [redacted] / Unterschrieben am: 02.01.2016 15:03

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



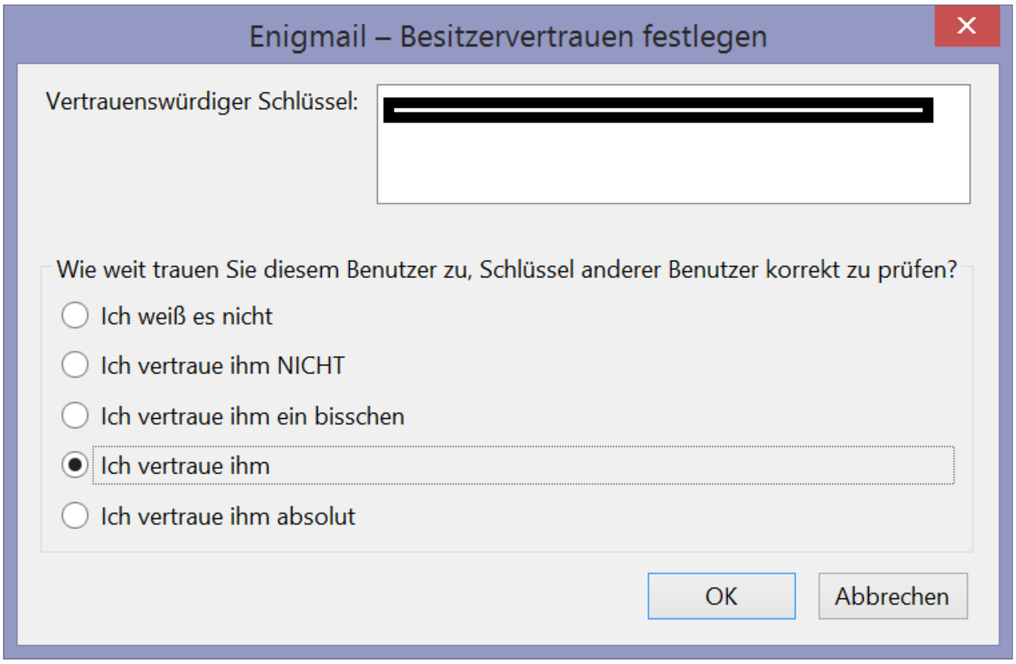
Enigmail-Meldung

Enigmail-Sicherheitsinfo:

Entschlüsselte Nachricht
UNVERTRAUTE Korrekte Unterschrift von [redacted]
[redacted] / Unterschrieben am: 02.01.2016 15:03
Schlüssel-Fingerabdruck: [redacted]
[redacted]

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 2nd line.

If I click on "Details" and request more information, one can see that the "Ich vertraue ihm" (= "I trust him" is active.
Remark: For "user trust" (= "Benutzervertrauen") it should NOT be necessary to sign it in addition):

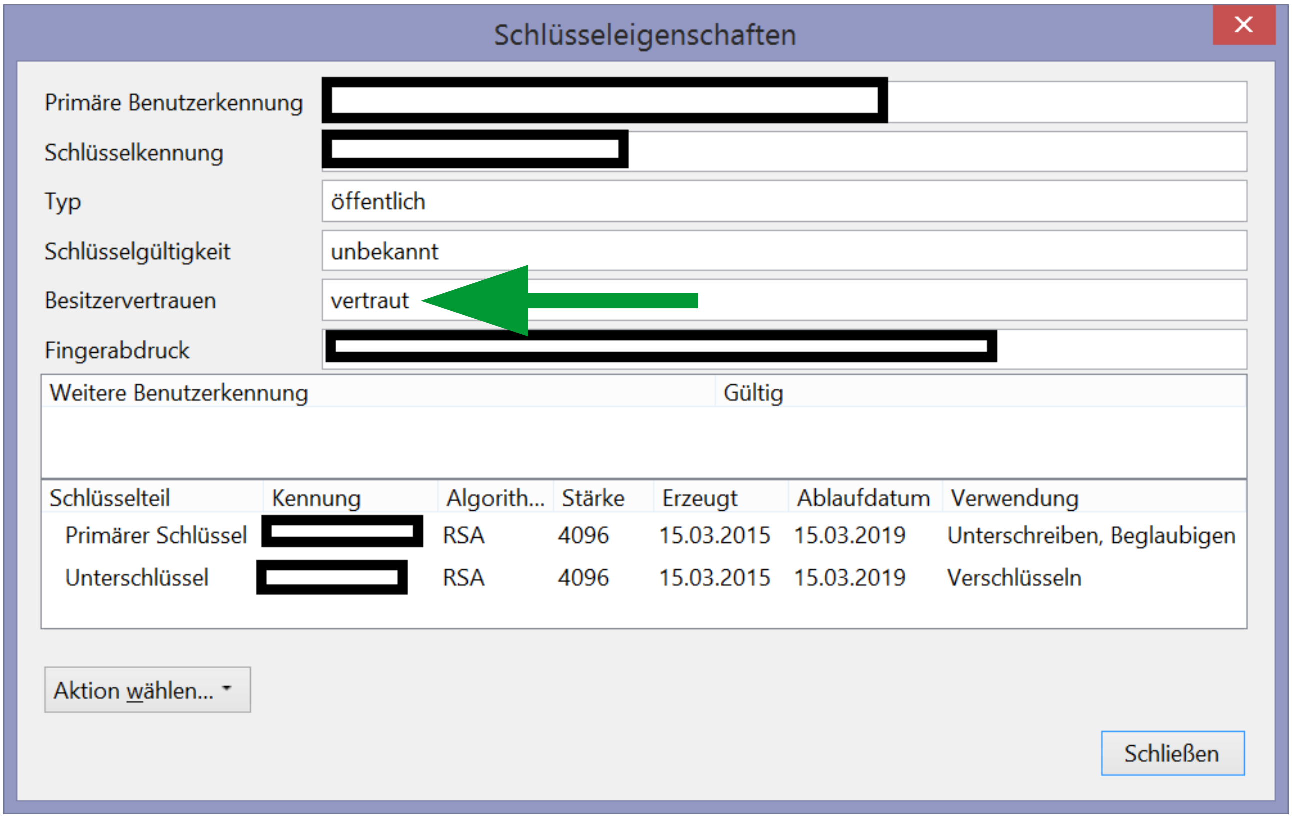


Enigmail – Besitzervertrauen festlegen

Vertrauenswürdiger Schlüssel: [redacted]

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



Schlüsseleigenschaften

Primäre Benutzerkennung	[redacted]
Schlüsselkennung	[redacted]
Typ	öffentlich
Schlüsselgültigkeit	unbekannt
Besitzervertrauen	vertraut
Fingerabdruck	[redacted]

Weitere Benutzerkennung	Gültig

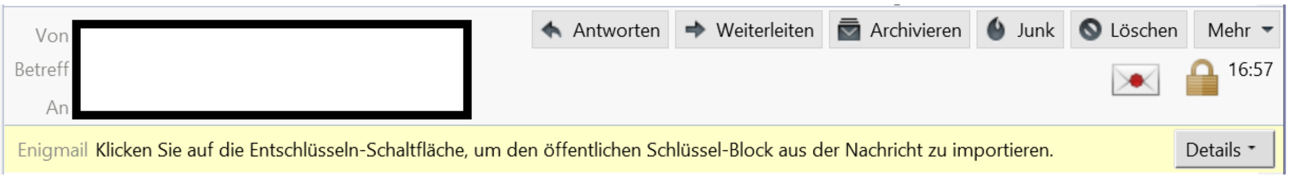
Schlüsselteil	Kennung	Algorith...	Stärke	Erzeugt	Ablaufdatum	Verwendung
Primärer Schlüssel	[redacted]	RSA	4096	15.03.2015	15.03.2019	Unterschreiben, Beglaubigen
Unterschlüssel	[redacted]	RSA	4096	15.03.2015	15.03.2019	Verschlüsseln

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?)

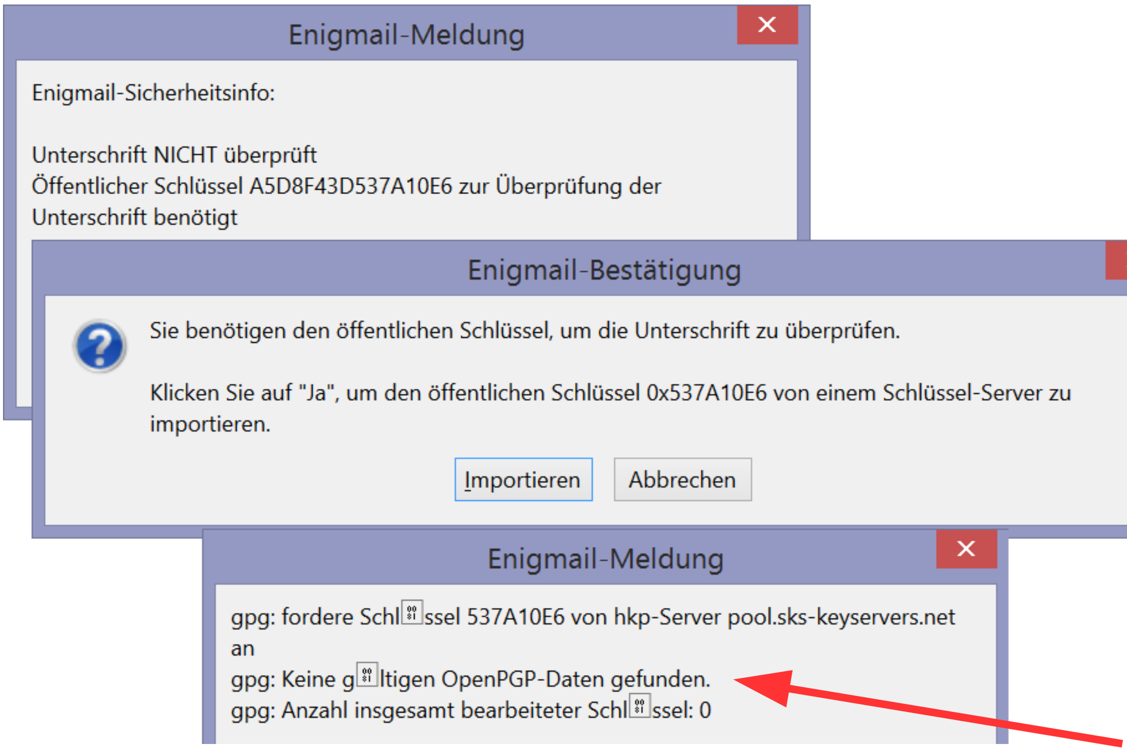


[redacted]

Enigmail Klicken Sie auf die Entschlüsseln-Schaltfläche, um den öffentlichen Schlüssel-Block aus der Nachricht zu importieren.

3.8. Umlaut problems in some Enigmail triggered dialogs

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



Enigmail-Sicherheitsinfo:

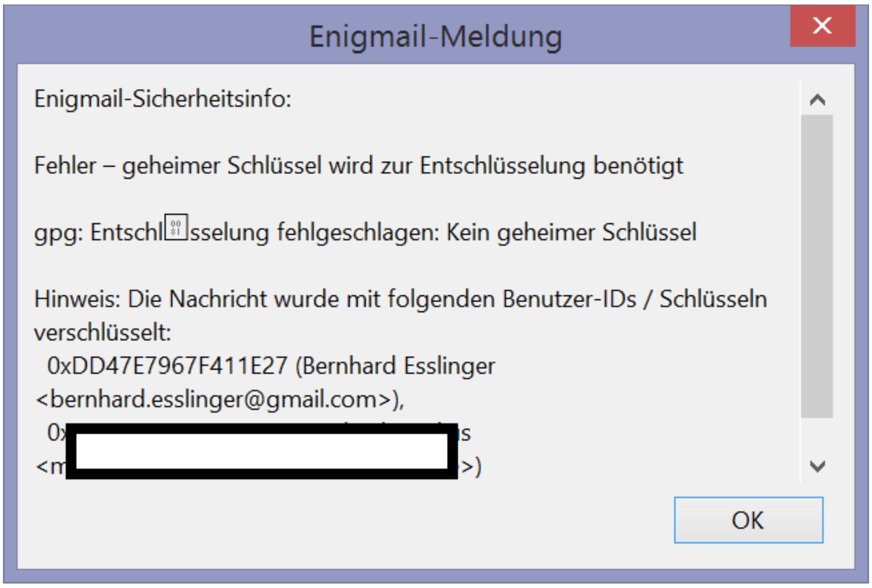
Unterschrift NICHT überprüft
Öffentlicher Schlüssel A5D8F43D537A10E6 zur Überprüfung der Unterschrift benötigt

Sie benötigen den öffentlichen Schlüssel, um die Unterschrift zu überprüfen.

Klicken Sie auf "Ja", um den öffentlichen Schlüssel 0x537A10E6 von einem Schlüssel-Server zu importieren.

```
gpg: fordere Schl□ssel 537A10E6 von hkp-Server pool.sks-keyservers.net
an
gpg: Keine g□ltigen OpenPGP-Daten gefunden.
gpg: Anzahl insgesamt bearbeiteter Schl□ssel: 0
```

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



Enigmail-Sicherheitsinfo:

Fehler – geheimer Schlüssel wird zur Entschlüsselung benötigt

gpg: Entschl□sselung fehlgeschlagen: Kein geheimer Schlüssel

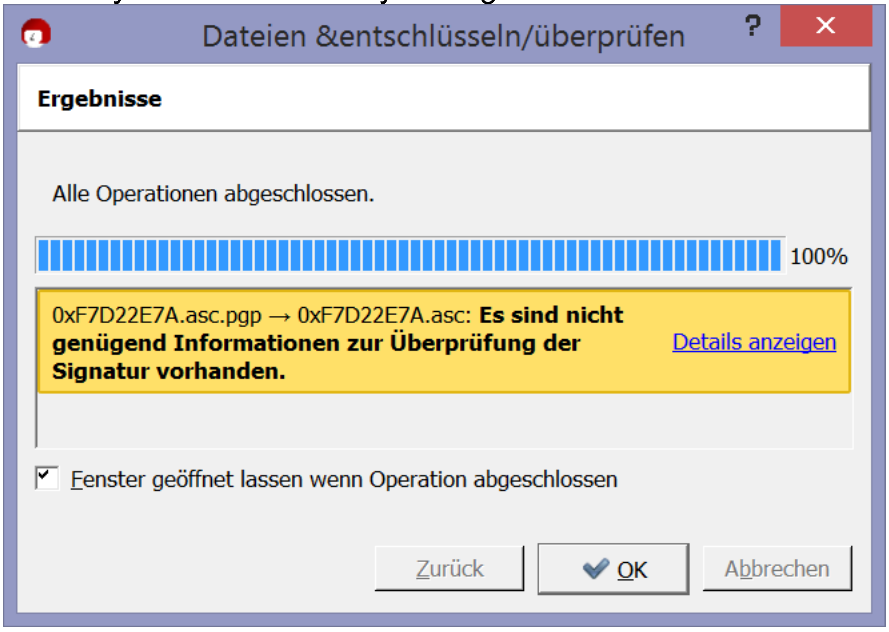
Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:
 0xDD47E7967F411E27 (Bernhard Esslinger <bernhard.esslinger@gmail.com>),
 [redacted]

Fehler – geheimer Schlüssel wird zur Entschlüsselung benötigt
gpg: Entschlsselung 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.


Dateien &entschlüsseln/überprüfen
?
✕
Ergebnisse

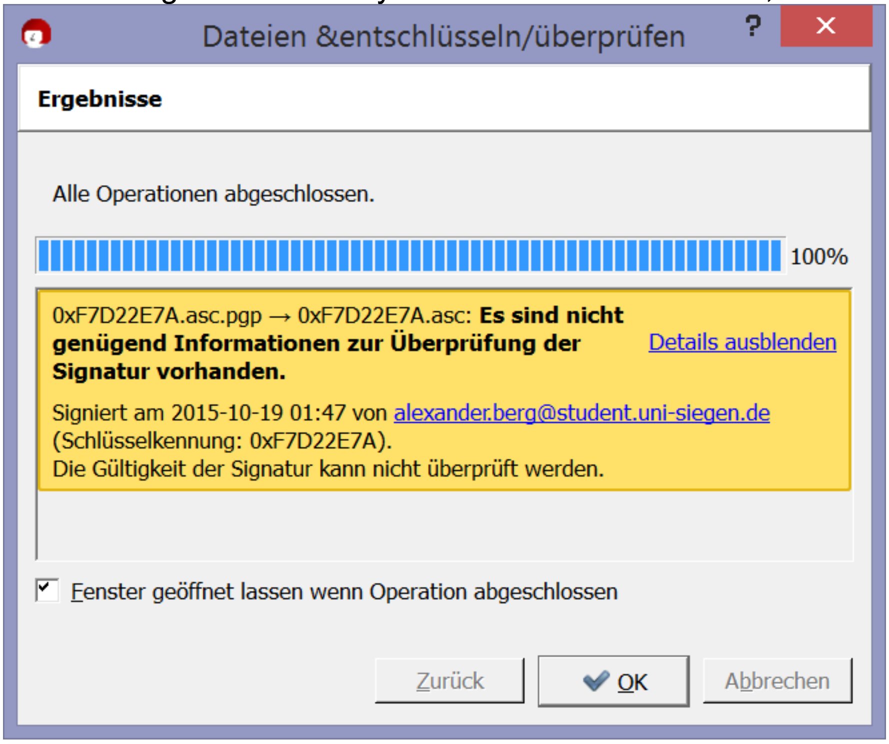
Alle Operationen abgeschlossen.

100%

0xF7D22E7A.asc.pgp → 0xF7D22E7A.asc: **Es sind nicht genügend Informationen zur Überprüfung der Signatur vorhanden.**

Details anzeigen
☑ Fenster geöffnet lassen wenn Operation abgeschlossen
Zurück
✔ OK
Abbrechen

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


Dateien &entschlüsseln/überprüfen
?
✕
Ergebnisse

Alle Operationen abgeschlossen.

100%

0xF7D22E7A.asc.pgp → 0xF7D22E7A.asc: **Es sind nicht genügend Informationen zur Überprüfung der Signatur vorhanden.**

Signiert am 2015-10-19 01:47 von alexander.berg@student.uni-siegen.de (Schlüsselkennung: 0xF7D22E7A).
Die Gültigkeit der Signatur kann nicht überprüft werden.

Details ausblenden
☑ Fenster geöffnet lassen wenn Operation abgeschlossen
Zurück
✔ OK
Abbrechen