User Manual SecureMail

Unit Information Security

As of August 2017

Contents

List of Figures

1 Quick guide

In co-operation with the Centre for Information Services and High Performance Computing (ZIH), the Unit Information Security operates a system for TU Dresden, which is based on the patented SEPPmail product of the Swiss manufacturer of the same name. This solution allows every member of TU Dresden (associate members and students) to communicate with third parties (especially research and co-operation partners) via encrypted e-mail, even if the communication partner does not have the digital key material. This significantly expands the possibilities for encrypted communication via email for our university. The basic procedure is briefly explained schematically below:

- The senders write a confidential e-mail in their default e-mail client and either mark it with the "confidential flag" in the subject line, e.g. "[+securemail]", or they use the free plugin for MS Outlook.
- The recipients receive a standard message with an explanation and an html attachment, which contains the encrypted message in its entirety. In parallel, they receive an initial password via SMS (text message). The mobile phone number is received by the system via query mail from the sender or the sender already provides the number in the subject line.
- The recipients open the html attachment and must enter their initial password.
- Afterwards, the senders have to register once on the system and assign their own password, and optionally set a security question + response for the automated password reset.
- The decrypted email is then visible in the webmail. From the webmail, the user can reply via encrypted email, upload their own keys or change the user settings.

2 Preparation

2.1 Microsoft Outlook

The manufacturer provides a so-called add-in for Microsoft Outlook, which allows the encryption of the email to be sent „at the push of a button“. If the add-in is not yet available in your Microsoft Outlook, please contact your administrator. **Note for administrators:** You can find an up-to-date installation archive (ZIP file) under

https://stura.link/y

2.2 Mozilla Thunderbird and other email programmes

No special preparations are required for Mozilla Thunderbird and other email programmes, such as Apple Mail etc. Please note the following paragraph "Writing encrypted emails".

3 Writing encrypted emails

3.1 Microsoft Outlook

In order to write an encrypted email to an external recipient from whom you do not have digital key material (precise wording: public key of recipient’s certificate), always enable the green "Encrypt" button located at the upper left of the Microsoft Outlook email window (see figure 1). Write your email as usual and send it off.

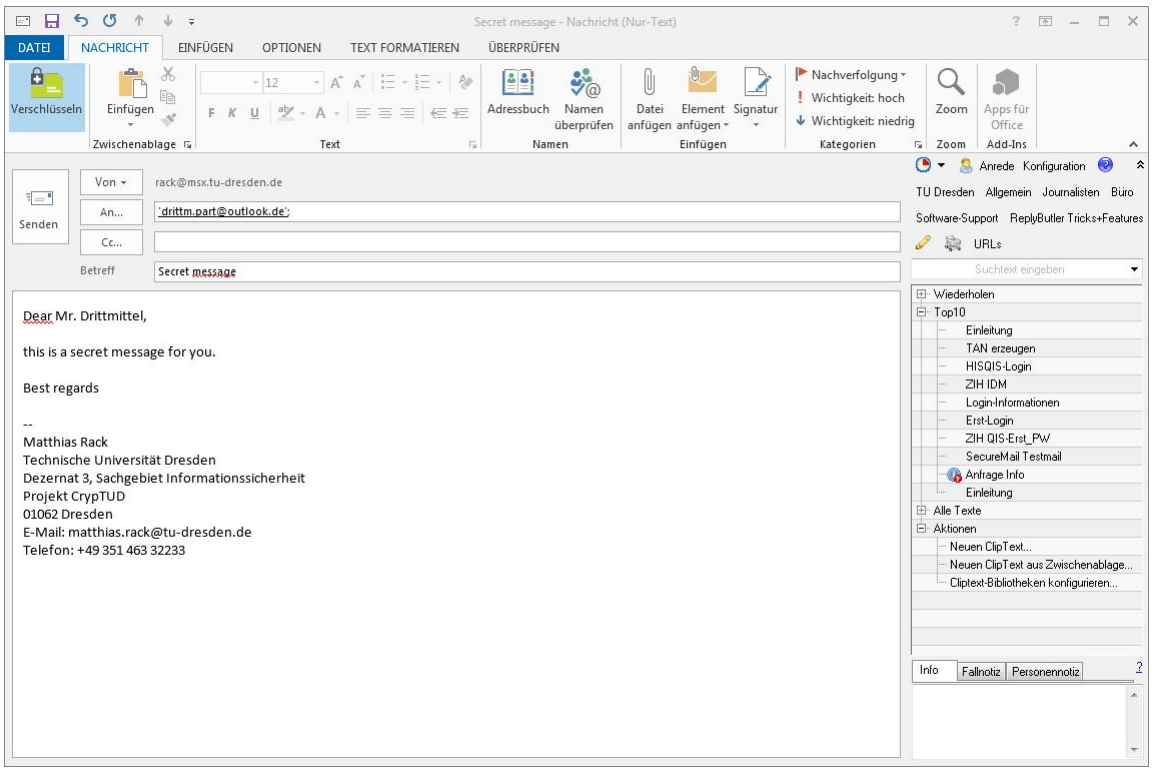

Figure 1: Writing encrypted emails in MS Outlook

3.2 Mozilla Thunderbird and other email programmes

In order to write an encrypted email to an external recipient using a different email programme than MS Outlook (e.g. Mozilla Thunderbird, Apple Mail etc.), type the following string at the beginning of the subject line:

```
[+securemail]
```

In figure 2, you will find an illustration as an example for Mozilla Thunderbird. Please make sure that you observe the square brackets! Then, as usual, write the subject behind the abovementioned string, write your e-mail, and send it off.

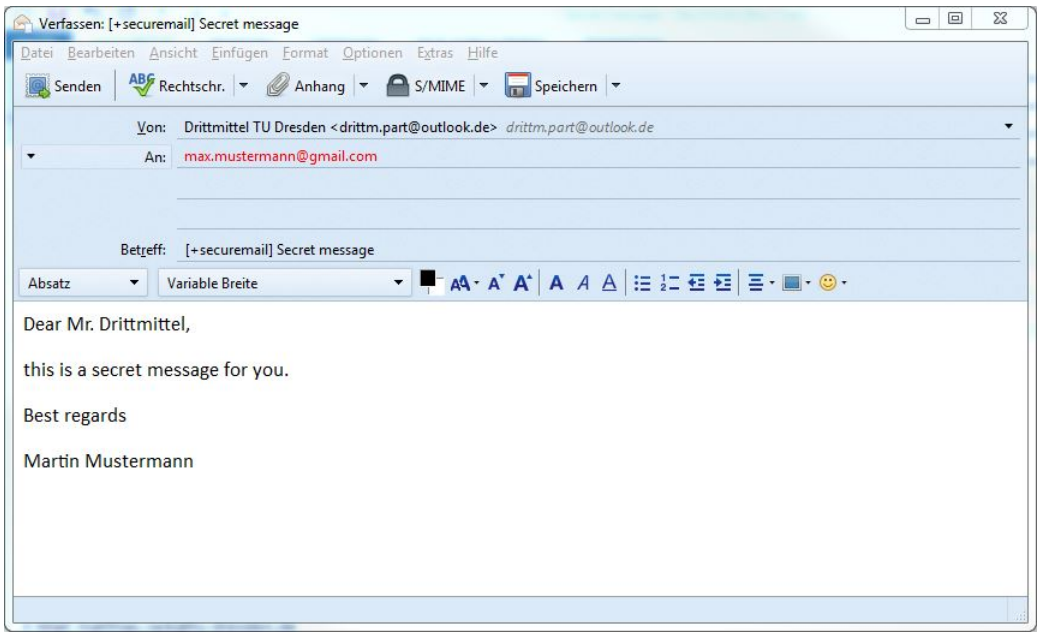

Figure 2: Writing encrypted emails with Mozilla Thunderbird etc.

4 Transmission of initial password

The recipient must visit a web portal that provides the solution in order to read the encrypted email. They require an initial password for the login process. You will receive this password by email after sending an encrypted email to an appropriate external recipient for the first time (see figure 3).

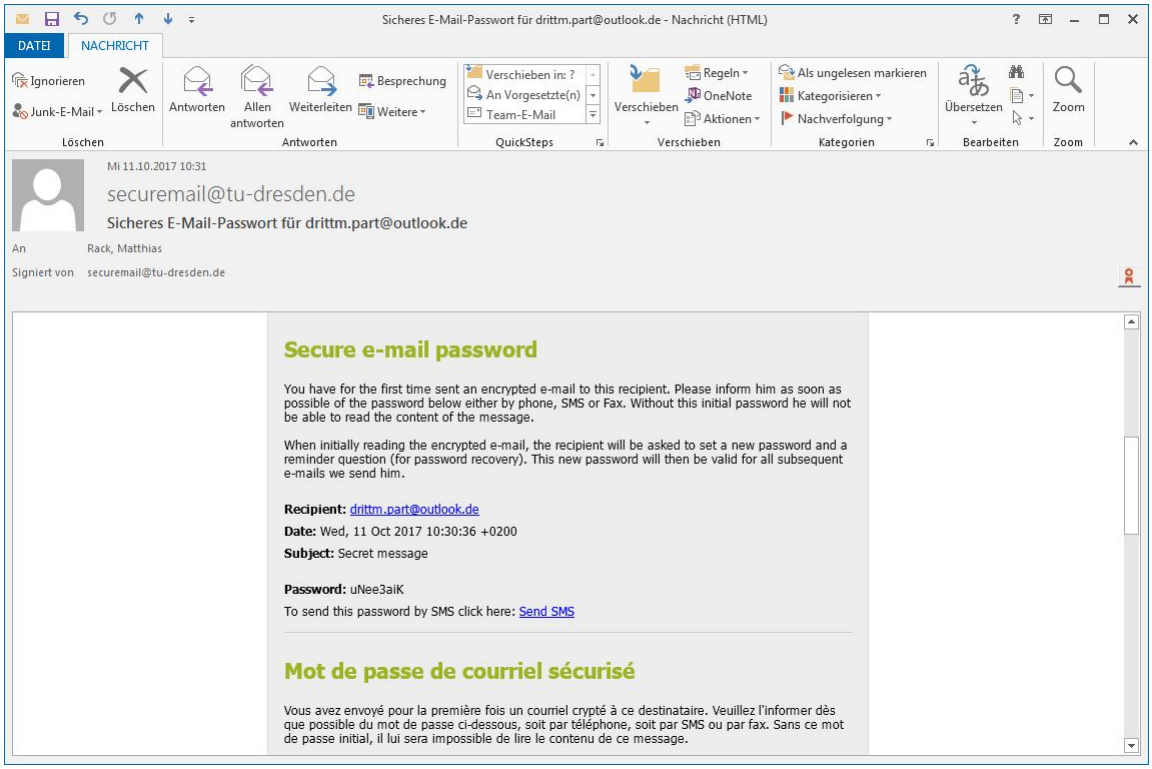

Figure 3: Email with initial password

Please click on the "Send SMS" link in the email. Your standard web browser will open and you will be requested to enter the mobile phone number in international format ‘‘0049 171 22211133”.

(see figure 4).

Figure 4: Website for entering recipient's mobile phone number

After the SMS has been successfully sent with the initial password, you will receive a confirmation (see figure 5).

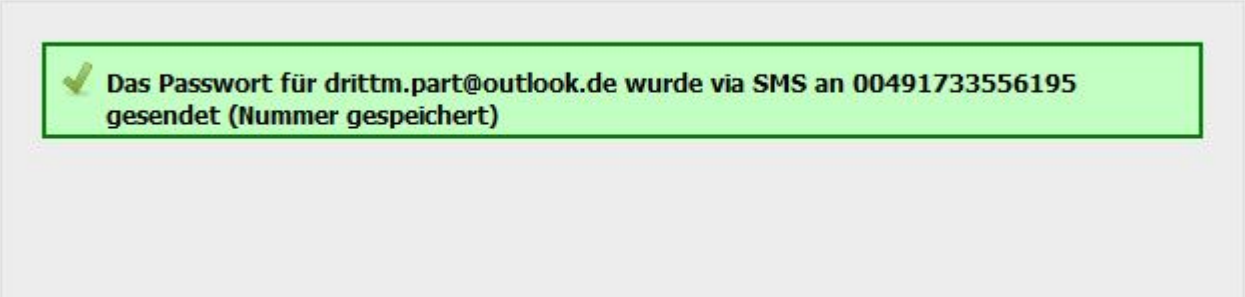

Figure 5: Confirmation of forwarding SMS

If your communication partners do not have an SMS-enabled mobile phone, please give them the initial password in another secure way. This can be ensured by telephone, for example. Please do NOT send the initial password to your communication partners in an unencrypted email!

5 Receiving end

This paragraph is for your information and does not have any impact and effect on the use of the SecureMail solution on the sender's side. The recipient of your encrypted email will receive your mail as an encrypted HTML attachment. This attachment is opened in the web browser, which initiates the forwarding to the SecureMail portal at Technische Universität Dresden (see figure 6).

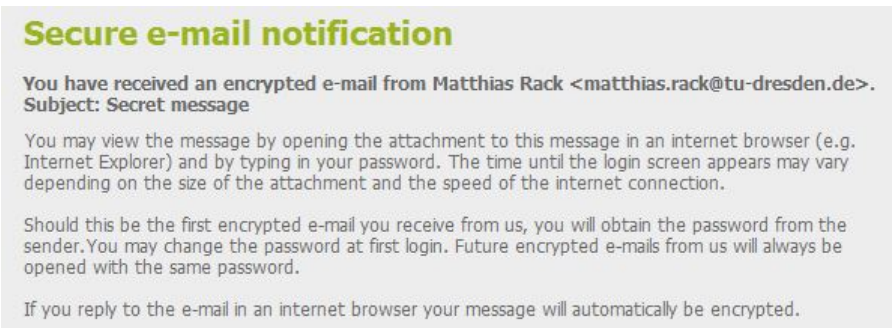

Figure 6: Secure email in the recipient's inbox

Here, the recipients can login with their initial password and must change the password immediately (This is mandatory!) and create an account. This process is only necessary once for the recipient. The recipient can then read the email sent by you (see figure 7).

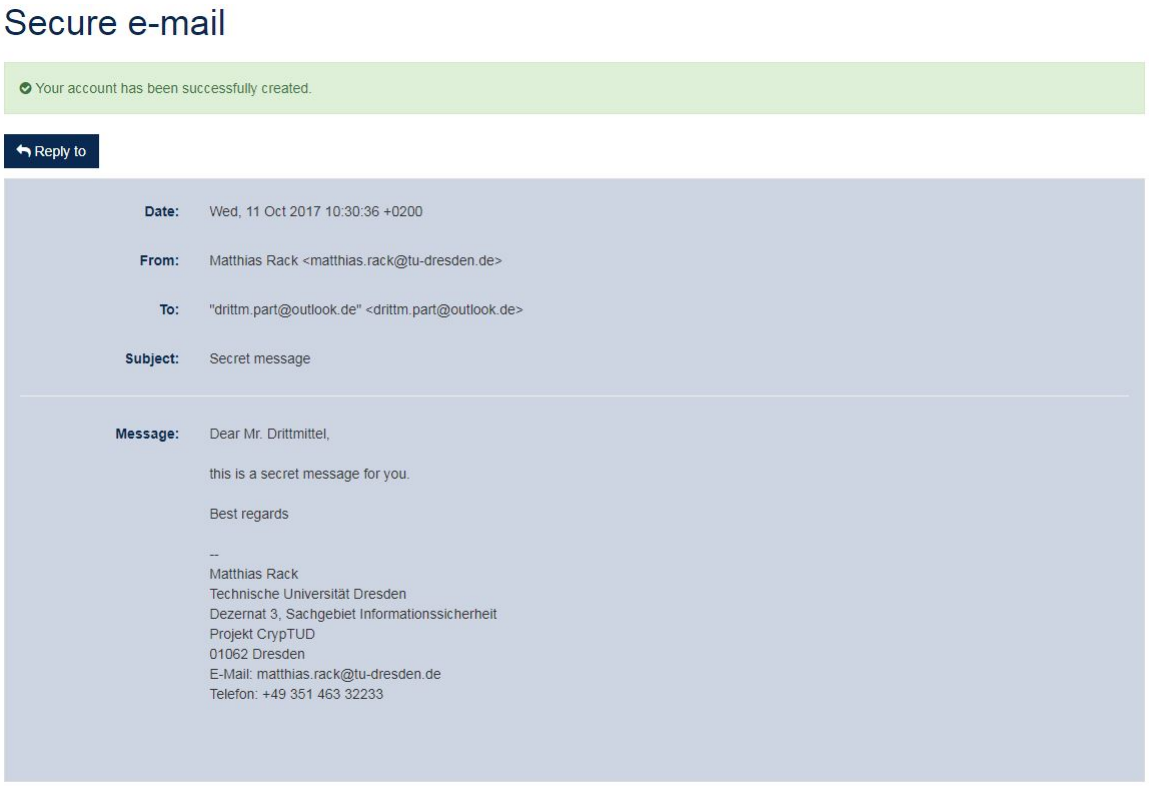

Figure 7: Reading the encrypted mail by the recipient

If an answer is required, the recipient can write the message by clicking on the “Reply” button and send it to you (see figure 8).

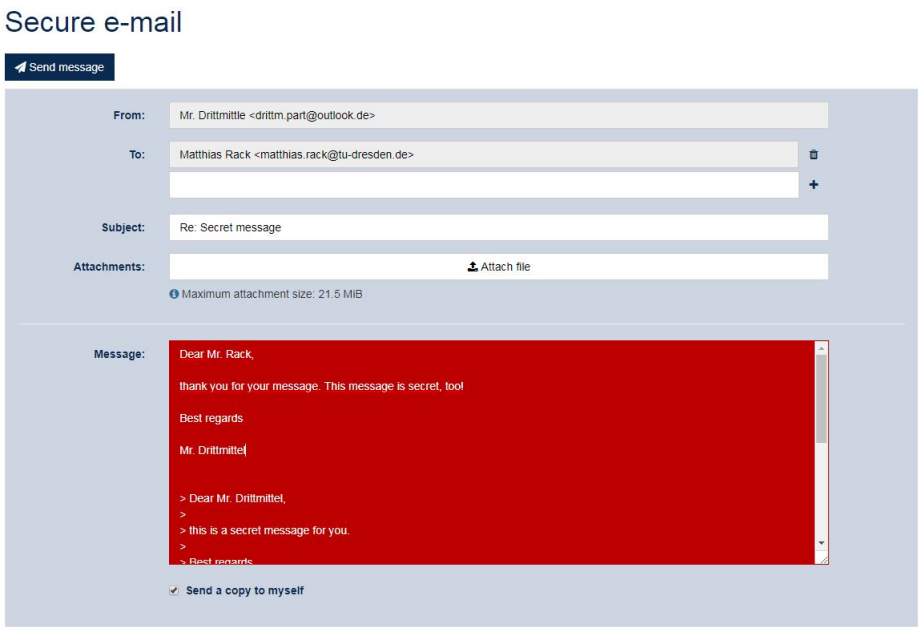

Figure 8: Answer email, written by the recipient

5.1 Mobile devices

The recipient can also open encrypted messages on mobile devices such as smartphones or tablets. The recipient does not need any additional software if using the operating systems Android or iOS (from version 11): the encrypted HTML attachment can be easily opened in the browser and then redirects to the SecureMail portal for decryption. Note for iOS devices up to version 10: an app "SEPPmail iApp" is available for free download in the Apple Appstore. The recipients have to select the encrypted HTML attachment under iOS for security reasons and select the "SEPPmail iApp" app via "Open in". It works as a "Bridge" between the mail programme and browser. After that, the recipient can open, read and, if necessary, answer the encrypted HTML attachment on the SecureMail portal.

6 Receiving read receipts and replies

As soon as the recipient opens your encrypted email in the SecureMail web portal, the system will always send you a read receipt (see figure 9).

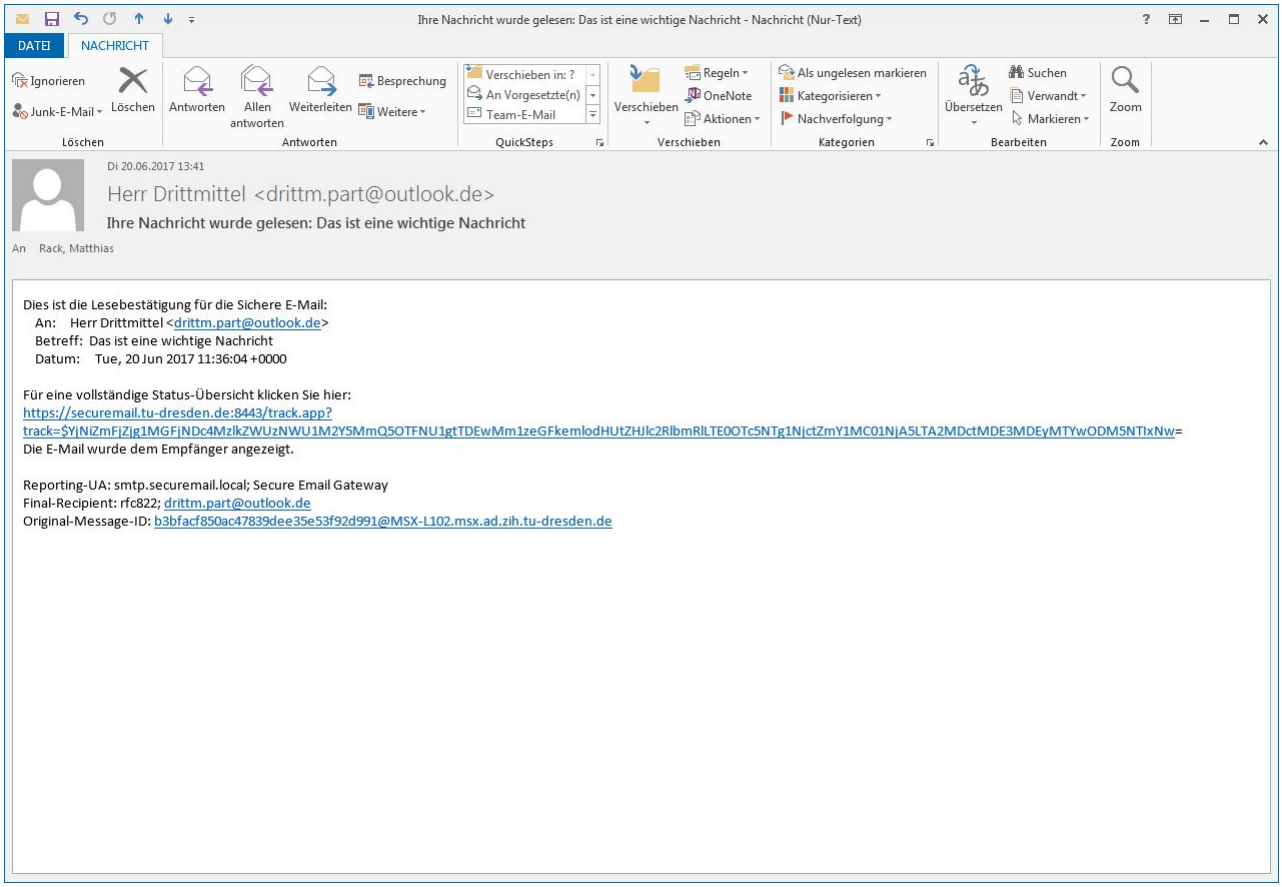

Figure 9: Email with read receipt

In case the recipient replies to your encrypted email, you will receive a corresponding email (see figure 10).

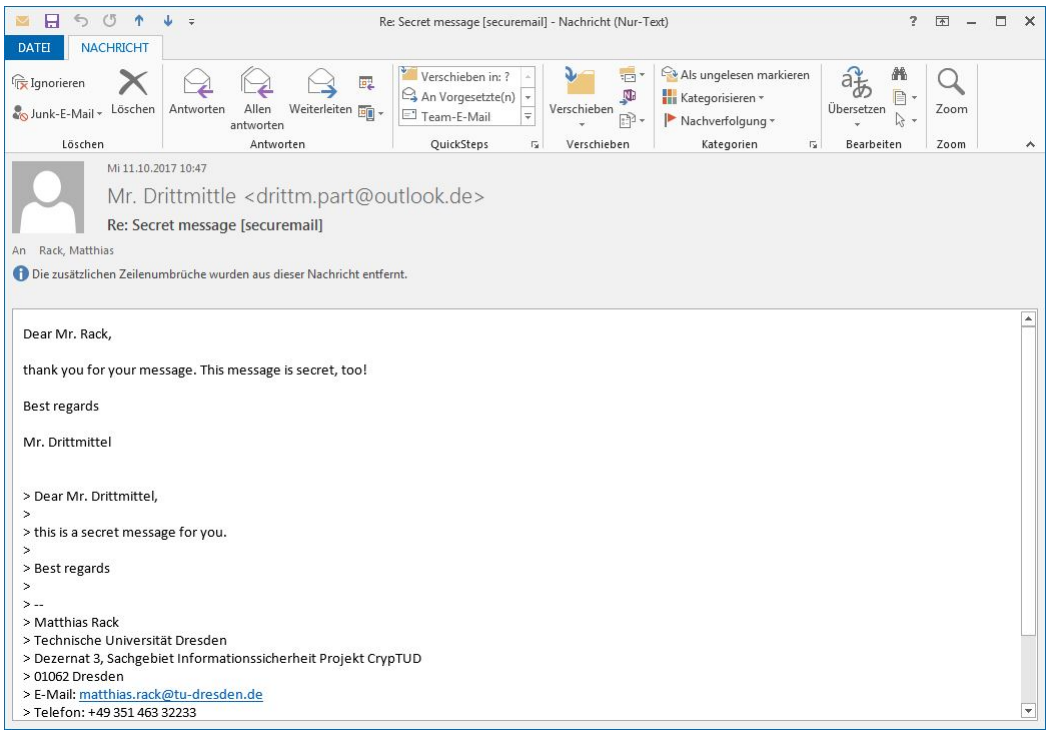

Figure 10: Email with reply

Sie können wie gewohnt ggf. auf die erhaltene E-Mail antworten. You can reply to the received email as usual. If you want an encrypted transmission to the recipient, please proceed as described in paragraph 3 "Writing encrypted email".

7 Spontaneous communication

As an external communication partner at Technische Universität Dresden, you can always send an encrypted message to a member of TU Dresden as a recipient via the SecureMail portal. To do this, the following steps are necessary:

1. Registration: please visit the website `https://securemail.tu-dresden.de`. There, you will find "Registration" in the upper menu bar, which you please click on. Then complete the registration form as shown in figure 11. Please note that you must read and confirm the terms of use before you can continue. After successful registration, an activation mail will be sent to your address. Please click the activation link included. This step completes the registration.

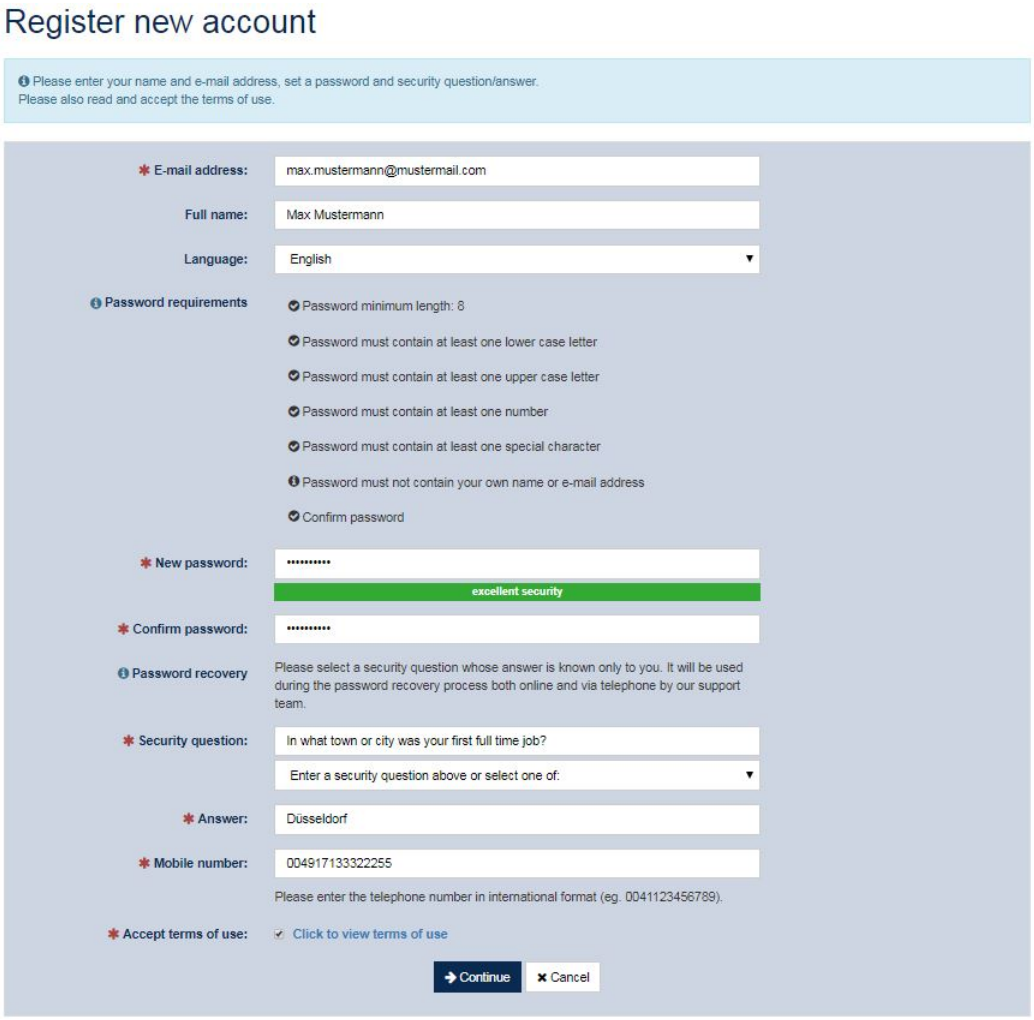

Figure 11: SecureMail registration form

2. Login: you can now log on to the SecureMail portal with your email address and the password you entered during the registration process. After successful login, you have the same options, which can be seen in figure 12: it is possible to edit your profile, change your password and, in particular, write an encrypted email to an associate member of Technische Universität Dresden by clicking on "Write email" in the upper menu bar (see 3).

Figure 12: SecureMail - preferences

3. Writing emails: as shown in figure 13, , you can write an encrypted message in the "Write email" form. Please note that only members of Technische Universität Dresden are eligible

as recipients (...@tu-dresden.de)! Please write your message and, if necessary, add a file attachment by clicking on "Attach file". Please note that the respective active form checkboxes turn red for reasons of accessibility. You have the possibility to send a copy of the message to yourself by activating the “Send copy to myself” checkbox in the bottom part of the form. By clicking the button "Send message", you will send your written email in encrypted form. You can now exit the SecureMail portal via the button "Logout" in the upper menu bar.

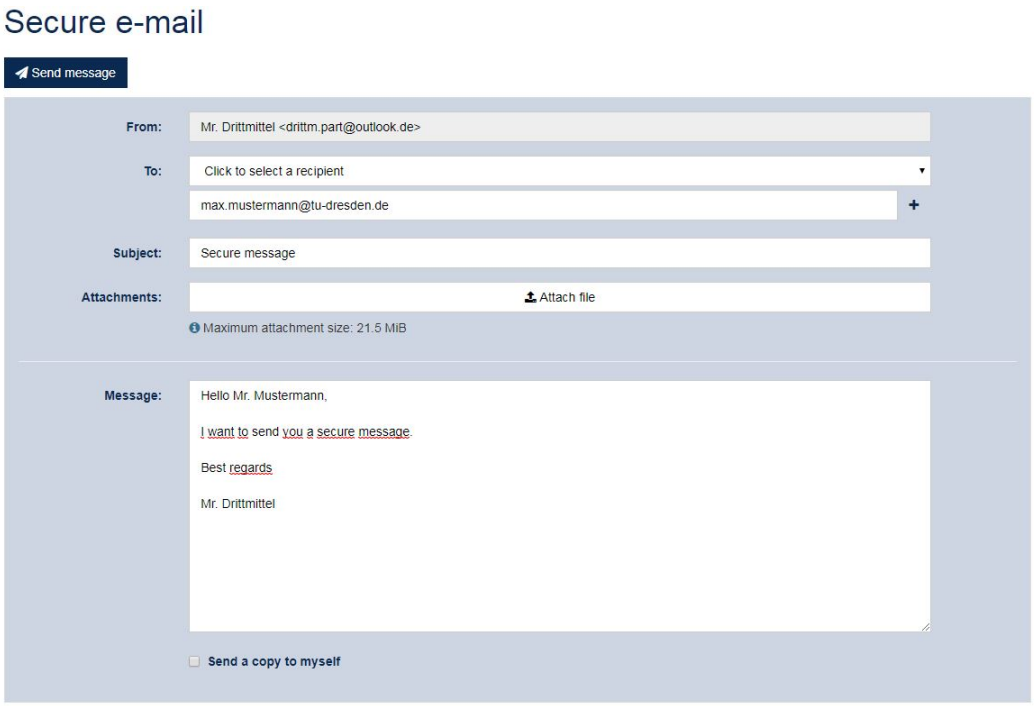

Figure 13: SecureMail – writing emails

8 Contact information

If you have any questions, problems, information or you want to report technical failures or malfunctions, please contact the Service Desk of the Centre for Information Services and High Performance Computing (ZIH) at Technische Universität Dresden:

- Telephone: +49 351 463 40000
- Email: servicedesk@tu-dresden.de